THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

Athlete Surveillance and Data Privacy: A Scoping Review of Privacy Concerns Related to Wearable Technologies in Collegiate Sports

DAVID RICHARDS
SPRING 2026

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Enterprise Technology Integration
with honors in Enterprise Technology Integration

Reviewed and approved* by the following:

Kelley Cotter
Assistant Professor of Human-Centered Computing and Social Informatics
Thesis Supervisor

Carleen Maitland
Professor and Associate Dean for Research and Graduate Affairs
Thesis Honors Adviser

* Electronic approvals are on file.

ABSTRACT

This thesis presents a scoping review of privacy concerns surrounding the use of wearable technologies in collegiate athletics in the United States. As wearable devices such as GPS trackers, smart bands, heart monitors, and other biometric monitoring tools become more ubiquitous in the domain of U.S. college sports, they offer potential benefits for performance optimization, enhanced recovery, and injury prevention. However, these wearable technologies and their associated data practices also raise significant questions pertaining to privacy, consent, data ownership, and institutional control. In order to examine how these issues have been previously addressed in scholarship, the present study reviewed fifteen sources and analyzed the privacy concerns identified within them according to Daniel Solove's taxonomy of privacy. The findings show the existing literature most commonly emphasizes privacy concerns related to surveillance (n = 14), exclusion (n = 12), secondary use (n = 10), increased accessibility (n = 9), decisional interference (n = 8), disclosure (n = 7), and intrusion (n = 6). These concerns underscore a consistent tension between performance optimization and athlete autonomy. This review also shows that this field remains limited in methodological diversity and sampling breadth. For instance, there are relatively few existing empirical studies, and those studies primarily employ qualitative approaches and focus on small participant pools. By consolidating and systematically organizing a fragmented body of literature and the privacy concerns found within it, this thesis provides a clearer foundation for future research and contributes to broader discussions surrounding governance, ethics, and athlete rights in the rapidly evolving landscape of wearable technology in U.S. collegiate athletics.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

First and foremost, I want to thank God for presenting me with opportunities and providing me with the tools and support I need to succeed in those moments. I firmly believe that He has a plan for me, and His plan is best, and I am thankful that He continues to remind me just how true that is.

Second, I want to thank my fiancé, Ella, for standing by my side and listening to me talk about my thesis more than anyone. Through the good and bad moments, you have remained in my corner cheering me on. You amaze me every day and push me to be better in every way, and I truly appreciate that. You're my everything, I love you!

Third, I want to thank my entire family for all they have done to help me reach this point. Mom and Dad, thank you for always believing in me and pushing me to excel in everything I do. Thank you also for reminding me that God has a plan even when I can't see it. Mom, thank you for helping me navigate tough moments and see the light at the end of the tunnel. Dad, thank you for teaching me to do the little things well and let the big things come naturally—this advice has guided me through life in every way. To my siblings and sisters-in-law, thank you so much for providing me with incredible examples and shoes that I can never fill—you inspire me to be great, and you share your own life lessons with me so that I might not have to learn them the hard way myself. To my nieces and nephews, thank you for brightening my day every single time I see you; you never fail to make me smile and remind me what is most important in life.

I would also like to thank my late-grandmother, Gram, for being my first teacher back in the days of Grandma School. You taught me how to count banana slices and read picture books—the foundation of my academic career. Much more than that, you taught me so much about life and faith. I will never forget you or the lessons you taught me. Thank you for continuing to watch over me and our family, I love you!

Next, I want to thank my thesis supervisor, Dr. Kelley Cotter, and my mentor, Hong, for guiding me through this process every step of the way and helping me pivot when things didn't go my way. You made this possible for me and taught me so much along the way, and I am eternally grateful for that.

Also, thank you to the Schreyer Honors College and Presidential Leadership Academy for offering me grants in support of my research. More than that, thank you for setting me up for success in every way and providing me with the best experience I could have imagined for myself at Penn State, both professionally and socially.

Finally, thank you to my entire village at Penn State—all my friends, organizations, mentors, and peers. You know who you are, and I appreciate you more than words can say.

Chapter 1

Introduction

Wearable technologies, or wearables, have become ubiquitous in the domain of collegiate athletics in the United States. GPS trackers, smart bands, and other biometric monitoring devices are used for the intended purposes of improving performance, enhancing recovery, and reducing the risk of injury for athletes (Arnold & Sade, 2017; Waśkiewicz et al., 2020). However, the use of these wearables raises many concerns as well, such as privacy, consent, data ownership, institutional control, and more (Brown & Brown, 2021). As the use of these technologies becomes more widespread, athletes are often subjected to monitoring that extends beyond the scope of traditional performance evaluation, which creates novel ethical and governance concerns that have yet to be synthesized across scholarly literature in this context. This thesis aims to address that gap by exploring how existing literature has addressed privacy concerns in relation to wearable technologies in U.S. collegiate athletics and by classifying those identified privacy concerns according to an established framework. By categorizing these issues, this review can offer human-computer interaction (HCI) scholars, particularly those focusing on privacy, a clearer view of how wearable technologies in collegiate athletics both reflect and further complicate larger debates regarding personal data, privacy, and user agency. Additionally, this study informs further research by summarizing the extent to which this field has been studied in regard to methods, sampling patterns, and data collected.

In order to accomplish those goals and make these issues easier to understand and interpret, the present study employs a scoping review design and leverages Solove's taxonomy of privacy to identify and analyze the types of privacy concerns that are apparent throughout the existing human-computer interaction research in this field (Solove, 2006). This study first provides a background on the use of wearable technologies in sports, briefly highlighting perceived benefits and general concerns associated with the technologies, as well as why it is appropriate to use Solove's taxonomy for this research. The

study then breaks down the methodological approach to the scoping review that was used to synthesize these findings, including the searching, screening, and coding processes.

Following that, this thesis presents those aggregated findings., which primarily focus on mapping privacy concerns identified in the reviewed articles against Solove's major categories of privacy harms to describe the nature of privacy concerns within this domain at a more granular level. The review additionally summarizes how this field has been researched in terms of methods and sampling strategies. Across those findings, the most prominent privacy concerns were surveillance, exclusion, secondary use, increased accessibility, decisional interference, disclosure, and intrusion, and the literature was shown to be limited in methodological diversity and sampling breadth. The findings are then interpreted, highlighting a fundamental, overarching tension between performance optimization and athlete autonomy. The discussion also points out particularly significant and persistent issues like surveillance, exclusion, weak consent integrity, and institutional control. Finally, the discussion emphasizes aforementioned methodological and sampling-related limitations that constrain the findings of the reviewed literature.

The broader value of this thesis lies in the fact that it consolidates a fragmented area of research and enhances clarity regarding which privacy concerns are most prominent, how this area has been studied, and why these issues matter on a variety of levels. In addition, by implementing Solove's taxonomy of privacy in the analysis of these privacy concerns, this thesis offers a clearer basis for future research and enables deeper discussions pertaining to privacy, governance, ethics, and athlete rights surrounding the use of wearable technologies in U.S. collegiate athletics. Ultimately, the present study lays the groundwork for further exploration in this field by identifying key issues for consideration and highlighting specific areas of opportunity for future research within this context.

Chapter 2

Background & Related Work

Overview

The integration of wearable technologies, or wearables, in professional, collegiate, and even amateur sports has advanced rapidly over the past two decades. These technologies collect biometric data, which enable the tracking of physical and physiological information for assessment of performance and recovery in sports (Arnold & Sade, 2017). Biometric data from wearables is widely considered medical information and should be treated as such (Dietrick, 2021). That data includes a range of physiological parameters such as heart rate, speed, distance, force output, and other biometric variables (Malleswari et al., 2024). This allows coaches, scouts, trainers, and players to move beyond traditional, subjective assessments of athletic performance (Toner, 2023). Athletic organizations use this data to provide insights for optimizing their training regimens and overall performance at the individual and aggregate levels. That said, this increasing reliance on wearable technologies and their associated data analyses brings forth significant ethical and privacy concerns that warrant careful consideration. Namely, the constant data monitoring can "increase pressure on athletes…leading to anxiety, stress, feeling overwhelmed and confusion" (Postma et al., 2024, p. 4). Also, there is speculation on how effectively this data can be translated into actionable insights due to the complexity of certain metrics (Postma et al., 2024).

Benefits of Wearable Technologies

Key benefits of wearable technologies in athletics include improved recovery outcomes and injury prevention, as well as training optimization. Postma et al. (2024) summarize the utility of these wearable technologies in the sports industry, saying "Beyond simply tracking, sports technology enables athletes to plan their training, pace their effort during training, and review their performance afterwards…

Sport data can even help athletes better understand their training load and recovery, providing in-depth insights into its underlying factors, like sleep quality" (p. 1). James Franklin, former head coach of the Penn State football team, credited the use of wearable health tracking bracelets known as WHOOP bands with improvements in the team's athletic training programming. Franklin explained that he would post players' sleep results so they could see that data and adjust their lifestyle accordingly (Corr et al., 2025).

The application of wearables in injury prevention also involves monitoring specific biomechanical information to identify potential risk factors. Many teams use data from wearable technologies to benchmark certain variables for individual athletes for reference in preventing or recovering from injuries (Toner, 2023, p.13). These benchmarks serve as baseline data that illustrate athletes' typical physiological conditions or performance levels, which help training staff identify deviations from their normal state of being. While the promise of early detection and intervention is significant, the effectiveness of these technologies in accurately predicting and preventing injuries requires further validation. This is illustrated by Düking et al. (2024)'s disclaimer, "there is a pressing need to evaluate the scientific evidence on whether and how wearable technologies can improve aspects of individual training procedures such as…reducing the likelihood of injuries" (p. 4).

Training optimization is facilitated by the continuous collection of a variety of physiological data, such as heart rate variability for example, allowing for the individualization of training programs based on an athlete's recovery and adaptation (Düking et al., 2024). Athletes also noted these technologies add an element of competition and motivation to their training, which leads to self-improvement (Postma et al., 2024). One of the most ubiquitously used wearable technologies in college sports is the Catapult vest, known as the Vector. This device includes a GPS, accelerometer, and magnetometer, which are able to cumulatively capture over one thousand data points per second. Key metrics include total distance traveled, top speed, number of sprints, sprint distance, power, load, intensity, and more (Catapult One, n.d.). One strength and conditioning coach explained the impact of this technology, claiming the device

"is to strength and conditioning what the barbell was 40 or 50 years ago" (Corr et al., 2025, p. 179). This underscores the perceptions of utility and positive impact that are associated with these technologies.

Concerns & Challenges Surrounding Wearables

Despite these benefits, the pervasive use of wearable technologies carries with it some crucial ethical and privacy concerns. Corr et al. (2025) interviewed collegiate athletes regarding data surveillance in college athletics and discovered respondents felt that "while implementation of wearable technology within training programs was instrumental in improving performance, such increasing biometric monitoring was detrimental to individual development and occasionally fostered dissension among teammates" (p. 175) The collection and usage of sensitive biometric data, especially in the college athletics environment, raises questions about data ownership, informed consent, and the potential for misuse (Arnold & Sade, 2017).

Due to the nature of relationships between student athletes and their coaches, there are power imbalances at play that may compromise the integrity of true willing consent (DeShane, 2024). Corr et al. (2025) explain this dynamic, saying "Such willful consent may be the manifestation of the paternalistic relationship between coaches and athletes prevalent in many collegiate athletics programs" (p. 188). One Division I football player spoke on the matter, adding "you grow up with the assumption [coaches] know what's best. They're using science to make you better" (Corr et al., 2025, p. 188). Moreover, the "cult of measurement" fostered by excessive and incessant data collection can lead to anxiety and undue pressure on athletes (Toner, 2023, p.139). Transparency in data management and the potential for algorithmic bias are also critical ethical considerations (DeShane, 2024). Even major sports technology platforms like Catapult Sports, the producer of the aforementioned Vector device, have garnered attention regarding data privacy issues (Mohamed et al., 2024). During the 2023 football season, there were allegations that an unnamed team accessed film of other programs through Catapult's platform, without authorization

(Rittenberg & VanHaaren, 2023). The claim was not substantiated, but the allegations were enough for notable NCAA Division I football teams to forego using Catapult's video analysis system for the remainder of the season, which illustrates the significance of data governance concerns in this industry.

A particularly significant concern surrounding wearable technologies and the collection of college athletes' data is the sharing of that data with third parties, especially in the current college sports landscape that is dominated by athlete compensation considerations, including name, image, and likeness (NIL) deals and revenue sharing. For example, Nike has recently signed deals with numerous colleges, like the University of Michigan, negotiating for student athletes' biometric data. Holt (2025) elaborates on this, saying:

> The data is de-identified, but some schools have not placed any parameters on how Nike can use the data, or what data they can collect from the wearable technology. Further, some schools do not require Nike to comply with FERPA or HIPAA. Some schools also do not require player consent and sign the deal on behalf of the athletes without any discussion concerning their rights. (p. 220)

Arnold and Sade (2017) recommend the establishment of a designated governing body that would overlook the issue of creating a protocol for data governance in collegiate athletics. In the meantime, it is also their recommendation that external distribution and usage of student athletes' biometric data should be discouraged and only permitted when accompanied by explicit consent from the associated athletes. Holt (2025) makes the claim college athletes should have a particularly significant say in how their data is used due to their lack of bargaining power and representation. Finally, with high school athletic teams starting to use wearable technologies, Holt (2025) warns that the sharing of data from high schools to universities may affect recruiting by allowing university coaches to use this data to determine which athletes receive scholarships.

The Solove Taxonomy

This thesis draws on Daniel Solove's (2006) taxonomy of privacy to provide a clear conceptual framework for the analysis of the privacy concerns identified in the literature. Solove developed his taxonomy to add nuance to the concept of privacy, arguing that it was too vague to function as a single, unitary concept. His aim was to identify and understand "the different kinds of socially recognized privacy violations" in a more concrete and useful way (Solove, 2006, p. 483).

Solove organizes privacy concerns into four primary categories: information collection, information processing, information dissemination, and invasion. The categories are structured around the data subject, covering the entire data life cycle from collection to processing to dissemination, and then forms of invasion which focus on the progressions toward the subject, rather than away, and do not always involve information (Solove, 2006). A visual depiction of the relationships between these categories is illustrated in Figure 1 below. Solove argues that, as information moves further away from the subject, from collection to processing to dissemination, the subject's control over said information decreases (Solove, 2006).

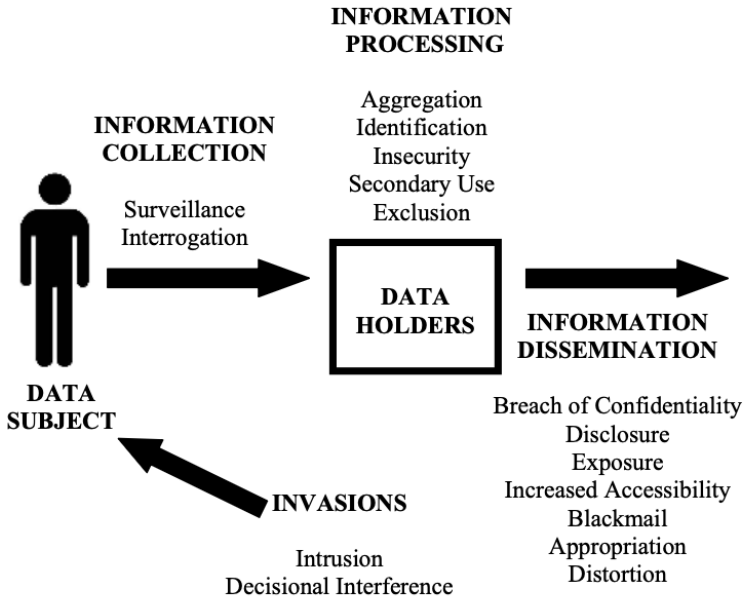

Figure 1. Solove Taxonomy Category Relationships (Solove, 2006)

The first category, information collection, includes surveillance and interrogation. Surveillance is "the watching, listening to, or recording of an individual's activities," while interrogation includes various forms of questioning or probing for information (Solove, 2006, p. 490).

The second category, information processing, pertains to the way information is stored, manipulated, and used (Solove, 2006, p. 490). The privacy concerns in this category are aggregation, identification, insecurity, secondary use, and exclusion. Aggregation deals with combining various pieces of data about a person. Identification refers to linking information to specific individuals. Insecurity focuses on carelessness in the protection of stored information that may increase risk of leaks or improper access. Secondary use occurs when collected information is used in any manner other than that which was originally specified to the data subject, without the data subject's consent. Exclusion addresses the failure to allow the data subject to know about the data that concerns them and the prevention of the data subject's involvement in its handling and use (Solove, 2006, p. 490).

Solove's third category, information dissemination, includes privacy concerns such as breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion. These activities all pertain to the spreading of information or transfer of personal data. Breach of confidentiality means the breaking of a promise to keep a data subject's information private. Disclosure involves revealing true information about a data subject that may impact the way others judge their character. Exposure pertains to the revealing of a data subject's nudity, grief, or bodily functions. Increased accessibility refers to the act of making a data subject's information more accessible. Blackmail refers to the threat to divulge personal information. Appropriation entails using a data subject's identity to benefit the aims or interests of another. Distortion relates to the dissemination of inaccurate or misleading information about data subjects (Solove, 2006, p. 491).

The fourth category, invasion, pertains to breaches or invasions into individual's private affairs. Unlike the other categories, privacy concerns under the invasion designation do not need to involve personal information, though they often do (Solove, 2006, p. 491). Intrusion consists of invasive acts that

disrupt an individual's tranquility or solitude. Decisional interference pertains to the government's intrusion into a data subject's decisions regarding private affairs (Solove, 2006, p. 491).

This framework is well suited for this thesis as it allows for greater precision in the analysis of privacy concerns associated with wearable technologies in college athletics. Moreover, Solove's taxonomy of privacy is a framework that is widely used in human-computer interaction literature, which will make it familiar to scholars interested in this research and allow them to more easily connect past scholarship on privacy concerns with the domain of wearables in collegiate athletics (Kumar et al., 2023; Lee et al., 2024; Wang & Pea, 2026). Ultimately, leveraging this framework makes it possible to distinguish whether a specific concern stems from the collection of athlete data, the way it is used, the way it is shared, or the way those practices may infringe on athletes' autonomy and private affairs.

Research Gap

Although existing literature has identified important privacy, governance, and ethical concerns surrounding wearable technologies in sports, this body of work remains limited in multiple ways. First, scholarship on privacy concerns in relation to wearables in U.S. collegiate athletics—the scope of the present study—is still relatively miniscule and fragmented. Prior work has raised numerous concerns about athlete surveillance, data ownership, governance, informed consent, and broader consequences of datafication, but the issues are dispersed across legal, ethical, and sport-related discussions rather than synthesized into a unified, comprehensive body of literature. Toner (2023) emphasizes the significance of understanding athletes' own perceptions of the data collection practices that they are subjected to, the usefulness of the data that is collected, and the associated privacy risks within these systems. Similarly, Deshane (2024) highlights the necessity for increased attention on power balances, consent, and ethical implications of biometric data collection in U.S. intercollegiate athletics.

Furthermore, the existing literature has not yet been effectively consolidated in a manner that distinguishes the specific types of privacy concerns being raised in this particular context. Most existing studies refer to issues of privacy, ethics, or governance in a broad fashion rather than classifying these concerns systematically. A more systematic approach would make it easier to identify patterns across this field and determine which dimensions of privacy are the most prominent. In addition, while existing literature suggests the need for more qualitative research and focus on stakeholder perceptions, which would be worthwhile in itself, the present study underscores the broader need to map the field and synthesize existing findings to identify the areas that most crucially require further exploration (DeShane, 2024).

When taken together, this thesis is justified by these gaps and prior recommendations. Through a scoping review of literature on privacy concerns surrounding collegiate sports in the U.S., the present study seeks to consolidate and organize existing scholarship and ultimately identify whose perspectives have been studied, what methods have been used, and which privacy concerns have been covered. This will provide a clear, organized foundation for future research and enable more informed discussion of privacy, governance, and athlete rights in the context of wearable technologies monitoring in U.S. collegiate athletics.

Chapter 3

Methods

Overview of the Methodological Approach

Since this thesis aims to synthesize and organize an emerging body of existing literature, a scoping review was selected as the most applicable design. The following subsections provide insight on the scoping review design, the inclusion and exclusion criteria, the database search strategy, the screening process, and the data coding process. Altogether, the methods outlined hereafter were decided upon in an effort to provide a systematic and transparent review of the existing body of scholarship on privacy concerns surrounding wearable technologies in U.S. collegiate athletics.

Scoping Review Design

A scoping review is a method of synthesizing knowledge of a particular field or context in a systematic and iterative way (Mak & Thomas, 2022). Scoping studies are generally performed to examine the extent and nature of research, to determine need for a comprehensive systematic review, to summarize existing findings, or to identify research gaps that still exist in a given field based on existing scholarship (Arksey & O'Malley, 2005). Scoping reviews are known to be better suited for providing a comprehensive overview to address a broader question than systematic reviews, especially since they are able to draw on evidence from any research methodology as well as non-research sources like policy (Peters et al., 2020).

The scoping review format was deemed appropriate and chosen for this thesis for multiple reasons. First, the topic of privacy and wearable technology in U.S. collegiate athletics is still emerging and does not seem to consist of a large, standardized catalog of empirical research yet. Second, the existing literature spans across several domains, including sport sociology, sport management, law,

communication, human-computer interaction, and ethics. Third, the technologies and the overarching setting of collegiate sports in the U.S. are ever changing, and the industry is currently in an era that is particularly marked by major evolution given the recent additions to the landscape, NIL and revenue sharing. Finally, the purpose of this thesis is not to test a single causal relationship, but rather to explore the extent to which privacy concerns have been discussed, what types of concerns have been highlighted, and how researchers have studied this issue. Therefore, the purpose and methodology of the present study align with the general purpose and methodology of scoping reviews, which is to map evidence on a specific topic and identify primary concepts, sources, and any existing knowledge gaps (Tricco et al., 2018).

Inclusion & Exclusion Criteria Overview

For this study, sources were included if they focused on privacy, surveillance, data ownership, governance, data rights, or related ethical concerns associated with wearable technologies in the context of collegiate athletics in the United States. In order to fall within the scope of this project, sources had to clearly satisfy four primary criteria 1) discussion of a data privacy-related concern, 2) focus on the use of wearable technologies, 3) emphasis on a people-centered approach rather than a technical approach seeking to develop or improve wearable technologies in this context, and 3) scoped within the context of U.S. collegiate athletics. The geographical limitation of just the United States was added for the sake of consistency, as data privacy laws and social norms differ between countries. Sources that failed to clearly meet all four criteria were excluded. For example, studies that focused solely on sports-related performance measurement, biomechanics, injury prediction, or technical system development without discussing privacy-related issues and a people-centered approach were excluded.

These inclusion and exclusion criteria were put in place to ensure this review focused on the institutional and human dimensions of wearable technologies and their related privacy concerns in U.S.

collegiate athletics. This was important because much of the literature on wearables in sports is oriented toward performance optimization or injury prevention rather than privacy, governance, and the related issues that are explored in this study. For the sake of this study, this means some technical studies were excluded if they did not meaningfully address the privacy concerns associated with the technologies and the athlete data that come from them.

Database Search & Data Cleaning

The first element of the search strategy for the present study entailed deciding which databases would be used for gathering literature. The chosen databases were SPORTDiscus, Web of Science, ACM Digital Library, and PubMed. These databases were selected because the topic covered in this study sits at the intersection of sport, technology, health, and data ethics. SPORTDiscus provides a sport-focused lens, Web of Science covers broader interdisciplinary coverage, ACM Digital Library adds computing and wearable technology elements, and PubMed focuses on health and biometrics. Together, they combine to capture most relevant studies across the multiple domains in which this topic exists.

The search process began with structured database queries using a Boolean search string centered on three concept groups: collegiate athletics, privacy/data governance, and wearable technologies. The search string used for each database included terms such as “college athletes,” “student-athletes,”, and “NCAA” as well as privacy-related terms like “privacy”, “surveillance,” “data ownership,” and wearable-related terms such as “wearables,” “wearable technology,” “WHOOP,” “Catapult,” “GPS,” “performance monitoring,” and more. Words and phrases *within* a given concept group were connected using the “OR” Boolean operator and concepts were combined using “AND” Boolean operators. The exact search string is the following:

("College athletes" OR "collegiate athletes" OR "student-athletes" OR "student athletes" OR "college athletics" OR "collegiate athletics" OR "college sports" OR "collegiate sports" OR

NCAA) AND (privacy OR private OR surveillance OR monitoring OR tracking OR datafication OR "data collection" OR "data ownership" OR "data rights" OR "biometric rights") AND (wearables OR "wearable technology" OR "wearable technologies" OR WHOOP OR Catapult OR "fitness trackers" OR biometric OR "smart devices" OR "player tracking" OR "performance monitoring" OR GPS OR "sports analytics" OR "predictive analytics")

When provided with that same query string, Web of Science returned 65 results, SPORTDiscus returned 72 results, ACM Digital Library returned 156 results, and PubMed returned 113 results. Those queries were further limited by filtering for articles—as opposed to books, extended abstracts, etc.—and limiting the time frame to the past ten years for relevancy—decisions that were made to enforce maximum relevancy and focus scope. After those filters were applied, Web of Science provided 61 results, SPORTDiscus provided 62 results, ACM Digital Library provided 67, and PubMed provided 90 results. Those filtered query results were downloaded from their respective databases and uploaded into Zotero. Duplicates were manually removed using Zotero's built-in duplicate-screening function. Further, the de-duplicated results were then imported into Excel and screened once more for duplicates in case any remained after the Zotero screening. After combining all results and removing duplicates, there were 212 results remaining for the screening process.

Screening Process

The screening process consisted of two primary stages: a preliminary relevance check followed by a second pass to confirm inclusion criteria were satisfied. The initial screening entailed searching each article's title and abstract for indications of inclusion criteria and checking off each of the four primary criteria one by one. If all four criteria—a data privacy-related concern, the use of wearable technologies, a people-centered approach, and the context of U.S. collegiate athletics—were apparent in the title or

abstract, the source was given preliminary approval. Once all sources were screened once, each source that was preliminarily approved was re-evaluated to confirm the validity of its inclusion.

Ultimately, 10 articles were included in the study based on the inclusion criteria. Connected sources—backward citations, or articles cited in the included sources, and forward citations, or articles that cited those sources—associated with those 10 selected sources were then gathered using Google Scholar. The 10 originally approved sources provided 109 more connected articles for review, which then were reduced to 76 articles once duplicates (n = 28) and inaccessible articles (n = 5) were removed. The inaccessible articles were not available through the existing library subscriptions and were therefore omitted due to time constraints. Once screened for relevance, 5 of those connected sources were added to the list of sources that would be included, bringing the total number of sources included in the present scoping review to 15 (See full list of articles in Appendix). Both the database search and screening process are illustrated in Figure 2 below.

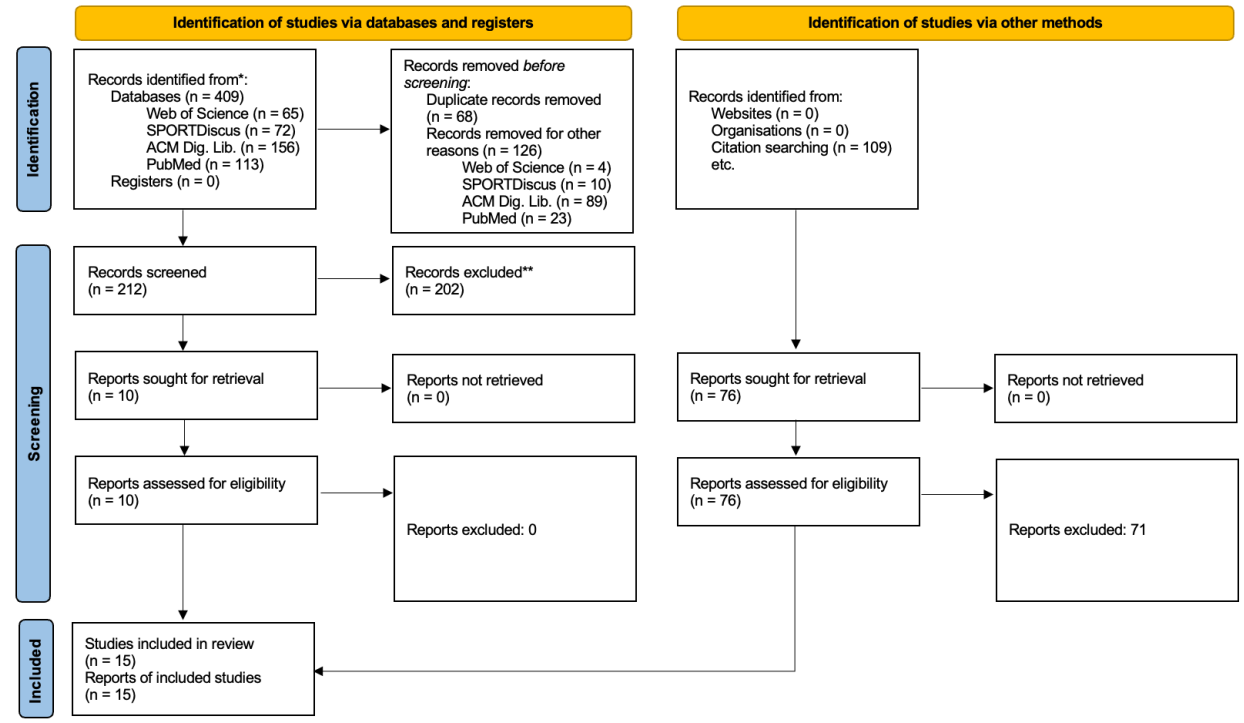

Figure 2. PRISMA Chart Detailing Database Search, Screening, and Citation-Chaining Processes

Data Extraction & Coding

After screening concluded, the 15 included sources were coded in a structured spreadsheet. The primary researcher coded the sources in collaboration with a research assistant. The coding framework documented each article's privacy concerns, methods, and participant sample information (if applicable), with notable quotes for each section.

The identified privacy concerns were documented, described in lay terms, and then coded based on Solove's taxonomy of privacy. Contextual information pertaining to each privacy concern, including notable quotes, was documented in another column of the coding spreadsheet. Concerns were identified in the source text through keyword searches of the documents; relevant search terms included "priva," "ownership," "surveil," "tracking," "monitor," and "right." The taxonomy-based coding entailed classifying each privacy concern under Solove's framework, such as "Exclusion" or "Disclosure." The privacy concern types are not mutually exclusive, meaning one privacy concern can constitute multiple types of privacy-related harm. So, one concern can be labeled as "Surveillance," "Secondary Use," "Breach of Confidentiality," "Exposure," and "Intrusion" if all those concern types seem to manifest in the identified privacy violation. It is important to note that this process was deductive, as it used Solove's taxonomy to map the findings of the literature to existing privacy concerns rather than creating privacy concerns inductively based on the articles included in the review. This enables comparison through precedent, ensures consistency, and provides a stable foundation for reasoning. Moreover, this approach is appropriate for the present study since the aim of this study was to synthesize existing knowledge on this topic, not to create a new taxonomy of privacy concerns.

Information pertaining to the methodological approaches of each source, including study type, the data being collected, and notable contextual information, was also collected. This information is especially important for identifying how researchers have studied this topic. Further, sample information is documented in another section of the spreadsheet, which notes the populations that each study explored. This is significant, as it shows which stakeholders within this topic have been given the chance

to shed light on their own experiences and perceptions. Details for these sections were found through keyword searches or the examination of common sections such as “Methods,” “Methodology,” “Participants,” “Sample”, or other similar headings. Both sections—methods and samples information—shed light on the extent and range of the existing empirical scholarship on privacy concerns surrounding wearable technologies in U.S. collegiate athletics. This provides critical insight on opportunities for future empirical research exploring this issue.

Chapter 4

Findings

Overview

The 15 articles that comprised the final list of included sources examined privacy-related issues pertaining to wearable technologies used for monitoring and athlete-tracking in U.S. collegiate athletics. Across this body of literature, a variety of privacy concerns were identified that altogether covered all major categories of Solove's taxonomy of privacy—information collection, information processing, information dissemination, and invasion. The most common concerns identified were surveillance (n = 14), exclusion (n = 12), secondary use (n = 10), increased accessibility (n = 9), decisional interference (n = 8), disclosure (n = 7), and intrusion (n = 6). Breach of confidentiality (n = 4), insecurity (n = 3), and exposure (n = 2) appeared less frequently, while interrogation, aggregation, identification, blackmail, appropriation, and distortion concerns were not discussed in any of the sources.

The sources addressed a variety of issues, including athlete surveillance, institutional power discrepancies, information flows, coaching staff data practices, legal and ethical concerns, athlete data literacy, explainable health-monitoring systems, and speculative futures for athlete tracking. When analyzed together, the body of knowledge in this scoping review showed data practices concerning wearable technologies in U.S. collegiate athletics are influenced by two main factors that are at odds with one another: performance optimization and athlete autonomy, which includes privacy, consent, control over data, and other elements.

Methods

As far as methods, the analyzed literature was predominantly qualitative and interpretive in nature. Ten sources were empirical and primarily qualitative, using interviews, focus groups, or

speculative design. The five remaining studies were legal, policy-oriented, conceptual, or review-based. As a result, the literature provides rich insight into privacy concerns pertaining to wearables in collegiate athletics but also exhibits limitations as far as diversity of methods across the field. These methodological findings indicate the topic is yet emerging and still requires extensive quantitative measurement.

Sampling

Sampling patterns varied across the catalog, with some sources focusing on athletes, some on coaching staff, some on support staff, and several on mixed combinations of stakeholders. Most common sampling techniques included purposive, convenience, snowball, or network-based, and most studies fielded their participants from only one or two institutions. These sampling decisions led to strong insights within their given contexts, but limited representativeness for the greater population of wearable technology users in U.S. collegiate sports. Overall, sampling in this field remains exploratory in both design and scope based on these findings.

Types of Privacy Concerns Identified in the Literature

As mentioned previously, apparent privacy concerns from each included article were coded deductively using Solove's taxonomy of privacy. The following subsections break down the reviewed literature in accordance with that framework.

Information Collection

Surveillance

The most prevalent type of privacy concern in this scoping review was surveillance (n = 14). Across the body of literature, surveillance pertained not only to the existence and use of wearables, but also to the normalization of ongoing or continuous monitoring of biometric, behavioral, and locational data within collegiate athletics. Corr et al. (2025) provided one of the clearest examples that shows how athletes understood their use of wearables as a way for coaches to constantly observe them beyond just training contexts. One participant from that study explained their understanding, saying, “Every move you make is under surveillance, on and off the field” (p. 186). In that same study, Corr et al. (2025) concluded wearable technologies, particularly those that track location and sleep patterns, are invasive and even psychologically damaging to college athletes.

Surveillance was also a prominent issue in works that focused on continuous monitoring via wearables and athlete tracking infrastructures. For example, Childs et al. (2025) pointed out how continuous monitoring devices create automatic flows of information from athletes’ bodies to coaches and staff, and that flow persists in many cases beyond formal spaces designated for sport. Brewer et al. (2025a) found that coaches and staff were aware of these concerns pertaining to continuous monitoring, particularly when tracking athletes outside of practice or competition. This was significant as it showed that not only do athletes feel the effects of surveillance, but the practitioners also recognize the risks. Kolovson et al. (2024) and Kolovson et al. (2020) also explained that surveillance is bolstered through sports tracking tools automatically connecting and transmitting athlete data to coaches in ways that athletes have limited ability to resist.

Multiple conceptual and legal analyses reinforced the empirical findings outlined above. Rush (2022) showed biometric tracking systems in collegiate athletics allow coaches to collect high volumes of data pertaining to sleep, heart rate, hydration, and other physiological metrics, at rates of up to 1,000 data

points per second, to constantly monitor athletes while providing the data subjects with little control over this process. Brown & Brown (2021) emphasized the "24/7" surveillance structure that athletes experience while having little say in the matter (p. 99). Brown & Brown (2020) also specifically highlights one wearable technology provider, WHOOP and their primary technology, the WHOOP strap. WHOOP is widely used in many professional sports leagues, as well as college, including institutions such as Duke University, Harvard University, Penn State University, and Conference USA. Brown & Brown (2020) estimate thousands of college athletes wear the WHOOP strap, which collects data on five metrics—heart rate variability, resting heart rate, body temperature, sleep latency, and skin conductivity (sweat)—at a rate of about 100 times per second.

Jessop & Baker (2019) also framed biometric tracking outside of sport as potentially unreasonable and negatively impactful to athletes because they are subjected to extensive monitoring without meaningful bargaining power over how or when it is collected. Greene et al. (2023) and Clegg et al. (2023) broadened this point by sharing how surveillance is engrained into the organizational culture within college sports, with Greene et al. (2023) saying college athletes are "constantly measured, weighed, pinched, tracked, recorded, monitored, and reviewed" (p. 1). Waśkiewicz et al. (2025) also declared biometric surveillance to be one of the clearest ethical problems in AI-driven injury monitoring because monitoring through wearable technologies such as smart mouthguards, real-time biosensors, and wearable ECG monitors has blurred the lines between voluntary participation and institutional compliance, particularly in high-performance environments such as collegiate athletics.

Information Processing

Exclusion

The most common information-processing-related type of privacy concern was exclusion (*n* = 12). In the context of the reviewed articles, exclusion referred to athletes being left out of decision-making processes related to their biometric data, including what data are collected, how those data are interpreted, who has access to those data, and how insights derived from those data are made actionable. Across each of these articles, exclusion was not just about data access, it was about the broader removal or omission of athlete agency from institutional data governance in U.S. collegiate athletics. Several studies in this scoping review assert exclusion is a foundational feature of collegiate athletics data practices instead of an occasional failure. This issue manifests in multiple ways, from a lack of athlete access to data and poor data literacy practices to decisions being made for athletes by non-athletes based on the athletes' biometric data.

The simplest manifestation of this privacy concern is athletes having inadequate data literacy, often due to lack of support or teaching. Childs et al. (2025) notes athletes are seldom aware of the purpose for which information is collected from them. One student-athlete who participated in the study admitted, "I don't really know what [they] need it for," when talking about sharing heart rate data with coaches (Childs et al., 2025, p, 6). Similarly, Clegg et al. (2020) points out data-driven decision-making processes are not made readily apparent to athletes. This latter point also relates to another form of exclusion in this context, where athletes are simply not given adequate access to their data. Kolovson et al. (2020) explains multiple participants reported not having access to their collected biometric data. Not only did they not have access to the data itself, but they were also unable to see the trends and other insights derived from the data, which prevented them from understanding how it was used. This effectively made staff the gatekeepers of the information, deciding when and what to share with the athletes (Kolovson et al., 2020). Finally, Jessop & Baker (2019) shed light on the fact that there is no

evidence that NCAA athletes are adequately informed of the risks associated with opting-in to the collection of biometric data before they make the decision to consent.

On a similar note, exclusion appeared in studies that focused on coaching practices and conceptual information flows. Brewer et al. (2025a) pointed out how coaches and staff frequently simplified or filtered the data that they shared with their athletes, commonly justifying these actions as a method for reducing stress or trying to prevent misinterpretation. Brewer et al. (2025b) outlined a similar commonly held hesitation toward giving athletes unlimited access to metrics traditionally managed by the coaching staff. Stenger and Feng (2024) posited team-centric data systems placed coaches at the center of the information flow and limit athletes to receive only what their coaches decide to share. Brown & Brown (2021), Jessop and Baker (2019), and Waśkiewicz et al. (2025) extended this notion, highlighting the weakness of athlete consent in this context, as it is affected by contingent worries such as team membership and playing time, which make participation practically mandatory.

In other cases, athletes are subject to decisions based on their own biometric data despite effectively having no say in the matter. Clegg et al. (2020) illustrated this fact in the form of a case about a study participant referred to as Ben, in which the authors explained, “The coach’s interpretation was established as authoritative, and Ben understood his data was to be interpreted for him, not by him” (p. 6). Another athlete from the same study faced backlash from her coach for ignoring metrics in favor of improving technique, and the authors asserted that athletes generally did not report open conversations where they could discuss their data-derived training plans with coaches (Clegg et al., 2020). Furthermore, Clegg et al. (2020) discovered athletes’ agency in regard to data collection and analysis was inversely proportional to the resources available to their athletic team, meaning athletes participating in lower-revenue sports with less technology had more freedom to dictate what was measured, and how, compared to their peers in higher-revenue sports. Therefore, in a high-revenue sport like football, athletes had minimal choices as far as how their data would be collected or used (Clegg et al., 2020). Greene et al.

(2023) summarizes these notions and adds some additional nuance through the additional lenses of informational asymmetry and race, stating:

> The information asymmetry at the core of athletics data presented differently for different sports with different levels of investment and different divisions of race and gender: Capital-intensive sports such as basketball and football, where Black men were overrepresented relative to the campus population, collected more and different data and gave players fewer options to avoid, dispute, or understand their data, relative to Olympic sports with lower levels of investment and majority-white teams. (p. 5)

Secondary Use

Another type of privacy concern found in many (n = 10) of the included articles, and one of the most common information processing concerns, was secondary use. In this body of knowledge, secondary use referred to athlete data being used beyond the scope of purposes for which the athletes may have understood the data to be collected, such as commercial partnerships, team selection, disciplinary actions, or gambling. Corr et al. (2025) highlighted this issue by noting biometric data from university-issued devices are "permitted to be sold to sport wagering companies to assist in establishing more informed betting lines" (p. 189). The authors further explain this point by saying college athletes essentially forgo control of their personal biometric data in the hyper-commercialized setting of NCAA athletics (Corr et al., 2025). This underscores how athletes' biometric data can be used outside the environment and beyond the purposes for which it was gathered. Brown & Brown (2021) also notes that universities, such as the University of Michigan and at least ten other universities, have included their athletes' biometric data in sponsorship agreements with commercial partners like NIKE. Moreover, Brown & Brown (2021) explains that the selling, sharing, and other alternative use of athletes' biometric data has occurred without bringing the athletes into the conversation or obtaining their consent. Jessop & Baker (2019)

similarly explain how athletes are absent from the bargaining table when it comes to negotiations between their respective NCAA institutions and biometric collection device companies or other external entities. The authors go on to point out that this arrangement leaves athletes in a disadvantageous position as their biometric data is sold without their input (Jessop & Baker, 2019).

Kolovson et al. (2020) sheds light on how athletes' wearable-derived data can be leveraged in organizational contexts for purposes other than performance monitoring that can be detrimental to the athletes themselves. The authors explain that athletes feel anxiety over their wearable-derived information possibly affecting their status on the team, limiting how they train, or determining whether they compete on a given day. Moreover, the authors note that wellness data that reveals violations or team rules or expectations may lead to punitive actions for associated individuals or the team altogether (Kolovson et al., 2020). Brown & Brown (2021) share one particularly poignant instance of this issue. In 2020, the head coach and coaching staff of Texas Tech Women's Basketball mandated the use of wearable monitors in every practice, game, and workout, and used the results to "chastise and bully their players" (Brown & Brown, 2021, p. 100). In this same case, the authors noted this abusive use of wearables and biometric data drove some players to refrain from using over-the-counter painkillers so they could use the pain to keep their heart rates spiked, as heightened heart rate was one of their coach's primary metrics (Brown & Brown, 2021).

Jessop & Baker (2019) also outline the potential risks faced by athletes when their biometric data is used beyond performance optimization or injury prevention within their athletic organization. Primarily, athletes can be subjected to consequential decisions based on the use of invalid or improperly interpreted data, such as cutting an athlete from a team or any other decision that could negatively impact an athlete's career aspirations or well-being (Jessop & Baker, 2019). On a similar note, Waśkiewicz et al. (2025) argues the use of biometric data in relation to AI and injury-prediction systems can be detrimental to the athletes involved, as data-informed designations such as "high risk" can impact

playing time and follow them into the future, negatively influencing future opportunities and career prospects (p. 15-20).

Two particularly significant issues related to this privacy concern are the ambiguity surrounding data ownership in this context and the power imbalances at play between athletes and their respective coaches and institutions (Brown & Brown, 2021). Data ownership ambiguity not only limits athletes' agency in controlling the use of their biometric data, but it also has negative implications for their business interest as it prevents them from using their biometric data as a commercialized commodity (Brown & Brown, 2021). Lack of clear ownership and institutional power imbalances combine to limit athletes' autonomy regarding how and for what purposes their data are shared, sold, or otherwise used (Brown & Brown, 2019; Waśkiewicz et al., 2025).

Insecurity

Another privacy concern type related to information processing that was less common (n = 3) was insecurity. In this context, insecurity referred to the vulnerability of athlete biometric data to be misused or leaked due to weak safeguards or insufficient governance protections. Jessop & Baker (2019) declared insecurity as a significant and largely unmitigated risk to athletes, pointing out the substantial risks of data breaches and misuse regarding biometric data that can identify athletes. The authors went on to advise athletes against consenting to the collection of their biometric data until their institutions display better protection and insurance protocols to defend against breaches and misuse (Jessop & Baker, 2019).

Stenger & Feng (2024) also discussed insecurity-related concerns pertaining to the flow of athletes' biometric data. First and foremost, the authors explained how commercial products are the primary safeguards for protecting athletes' biometric data and their privacy. In other words, many institutions outsource data security to the companies that provide their wearable technologies or storage platforms. Moreover, the authors point out that these external partners collect signed waiver forms for

privacy policy agreements, and many teams pay limited attention to these agreements. According to their analysis, coaches are often thankful to pass off responsibility for athlete privacy to vendors (Stenger & Feng, 2024).

Waśkiewicz et al. (2025) provided insight on another insecurity concern in the use of athlete biometric data that is especially pertinent to use cases involving AI. The authors explain how athletes' data used in the AI context are typically retained and processed within black-box infrastructures that do not provide much clarity or assurance to athletes regarding how securely their information is stored, reused, or shared (Waśkiewicz et al., 2025). When combined, these insecurity risks raised awareness for the insufficient security and protection infrastructures surrounding athletes' biometric data in U.S. collegiate athletics. Furthermore, insecurity issues magnify every other privacy concern outlined in this scoping review, as they magnify the risk of athletes' data being used for inappropriate and potentially damaging purposes.

Information Dissemination

Increased Accessibility

The most prominent (n = 9) privacy concern in the information dissemination category was increased accessibility. In the context of this scoping review, increased accessibility referred to the way wearable technologies and organizational data practices expanded the number of people, systems, and institutions that could more-easily access athlete information. Bae et al. (2025) touched on the problematic manner in which detailed athlete data is made accessible to other people, such as coaches, while athletes themselves do not have adequate access to or control over that same data. Childs et al. (2025) similarly explained how continuous monitoring through wearables facilitates automatic

information flows to coaches and other recipients, which expands access to the data and bypasses athlete oversight.

Kolovson et al. (2024), Rush (2022), Brown & Brown (2021), and Clegg et al. (2023) all suggest the same overarching problem related to increased accessibility: once athletes' biometric data are collected and integrated into a given institution's systems, they inherently become more available across organizational and commercial information networks. Waśkiewicz et al. (2025) sheds light on the way this issue is affected by the ambiguous nature of data ownership in this field. The authors point out that athletes seldom have formal ownership of their biometric data, which enables teams, institutions, and commercial vendors to use these data "indefinitely and for profit" (Waśkiewicz et al., 2025, p. 15). Stenger & Feng (2024) highlighted this by explaining how data flows in collegiate athletics are team-centric, with coaches and staff being the primary recipients by default and commercial vendors holding major roles by providing storage and management solutions. Therefore, increased accessibility reflects a recurring theme in the literature: wearable devices and the data-driven analytic systems that they feed have made athlete information wholly easier for recipients to access, share, but not easier for the data subjects—the athletes—to govern.

Disclosure

In the context of the present study, disclosure (n = 7) referred to athlete information being revealed, shared, or otherwise communicated to others in ways athletes did not fully control or necessarily consent to. Stenger & Feng (2024) described this sort of inappropriate flow of information as occurring when coaches use player data to highlight inadequate effort without the athlete permission or transparency. In several cases, this privacy concern was tied to team-based hierarchies and related to team dynamics. Brown & Brown (2021) and Jessop & Baker (2019) both showcase how coaches use biometric

data in ways that disclose athlete performance or compliance data to others, including public and semi-public evaluations within team settings.

Clegg et al. (2020) highlighted how the disclosure of athletes' biometric and performance data, often derived from wearable devices, leads to excessive competition and disrupts team chemistry. Athletes admit it is difficult and uncomfortable for them to discuss their data with their teammates since they are competing with one another for spots in the lineup (Clegg et al., 2020). Greene et al. (2023) bolsters this notion by reiterating athletes' discomfort with sharing their data with their teammates and those closest to them. In one testimony from their study, an athlete described the way their coaching staff would share entire performance data spreadsheets with the whole team so that everybody could see athletes' scores for workouts, which the athlete seemed uncomfortable with (Greene et al., 2023).

Clegg et al. (2023) also contributed insights on this privacy concern by explaining how athletes' data were accessible to their coaches, athletic departments, and even corporate partners in manners that athletes did not govern or desire. One example of this issue is apparent in the testimony of one interview participant, an athlete referred to as Lei. Regarding this issue, Lei explained how she did not want to join a new data collection and visualization platform implemented by the team because they started using it while she was hurt. She claimed she did not want to join because the platform, Training Peaks, allowed her coaches to see "everything" and she wanted to come back from her injury on her own pace because she knew that she would likely over-exert herself and risk her own health if she knew her coaches could see all of her performance data through her recovery (Clegg et al., 2023, p. 1800).

Waśkiewicz et al. (2025) added more nuance to this concern, explaining its application in the context of AI prediction systems. The authors posited these systems can negatively impact athletes' career prospects and job security, in the athletic sense, through injury-risk outputs and other related interpretations. For instance, high-risk labels on athletes can be self-fulfilling prophecies as the disclosure of these assessments may result in tagged athletes receiving fewer future career opportunities, which will reinforce the notion that the model's prediction was accurate. Ultimately, disclosure in this context

matters not only in the case of data moving outside the organization, but also within unequal institutional relationships and between peers.

Breach of Confidentiality

This privacy concern (n = 4) referred to the failure to keep athletes' private information within the expected boundaries of trust. Childs et al. (2025) and Brewer et al. (2025a) suggested that biometric data can move beyond limited coaching or performance-related contexts that athletes might assume, especially when continuous monitoring systems enable broader surveillance. However, Brewer et al. (2025a) also provides counterexamples that highlight how certain data is constrained to certain designated viewers, such as athletic training department practitioners and team physicians, and may even exclude coaching staff when appropriate.

Kolovson et al. (2024) framed biometric data tracking as capable of violating expectations of confidentiality pertaining to who should know what about a given athlete's body, health, and habits. Rush (2022) approaches this concern in legal and governance terms, warning that biometric data monitoring creates substantial confidentiality risks based on the sheer volume and sensitivity of data collected, especially when clear guardrails are not made apparent. Overall, confidentiality in this context was not compromised by a single dramatic instance of a breach, but by the common expansion of access within athletic organizations and their partnerships.

Exposure

Exposure, though rarely identified (n = 2) in the literature, warrants meaningful consideration as a serious information-dissemination-related concern. In the present study, exposure referred to revealing athletes' bodily and behavioral information. Corr et al. (2025) and Jessop & Baker (2019) posited that

wearable devices and biometric monitoring can expose athletes to negative impacts, as they can make intimate bodily or behavioral information readily available to coaching staff, institutions, peers, and external actors. In Corr et al. (2025), exposure was affiliated with the unwarranted visibility into athletes' lives outside of sport, which was brought on by continuous monitoring beyond the competition and training settings. Participating athletes described this monitoring, and the dissemination of the associated data, as invasive and psychologically damaging (Corr et al., 2025). In Jessop & Baker (2019), exposure was tied to the chance of detailed biometric data being revealed in ways that make the athletes more vulnerable while offering them little say in the matter.

One of the most acute, stand-out examples of exposure was provided by Jessop & Baker (2019). In 2015, fifteen athletes on the University of Tennessee Swimming and Diving team used WHOOP wearable devices, and their data was displayed on a central team dashboard. Viewers, both coaches and players alike, could see when each athlete went to sleep and how much sleep they got, as well as much more intrusive information, "including how many alcoholic drinks they consumed on a Friday night, and if and how long someone had sex" (Jessop & Baker, 2019, p. 97). The authors described this real scenario as "Big Brother on a level that no one, including [Head Coach Matt] Kredich, could have anticipated" (Jessop & Baker, 2019, p. 97).

Invasion

Decisional Interference

Appearing in over half of the reviewed articles (*n* = 8), decisional interference was another prominent privacy concern. In this context, decisional interference referred to privacy violations and data practices that constrain or influence the ways athletes make decisions pertaining to their bodies, behavior, or participation. One primary manifestation of this privacy concern is the process and environment surrounding athletes' consent to be monitored. Kolovson et al. (2024) and Kolovson et al. (2020) both argue that fundamental power asymmetries within collegiate athletic organizations make it so college athletes do not have a position of power and therefore cannot refuse the exchange of their data without jeopardizing their standing on their team. Kolovson et al. (2024) showcase a specific example of data sharing being involuntary even when it is supposedly voluntary, as one interviewed athlete explained how coaches say they will not penalize athletes for not participating, but then favor the athletes who do participate. The athlete added that they have witnessed this phenomenon numerous times where participation is "optional but it's not optional" (Kolovson et al., 2024, p. 15).

Brown and Brown (2021) echo this point and assert that this "inherent imbalance of power" likely forces athletes to allow access to "intimate personal data" (p. 98). The authors also note coercion is a notable concern in this context and recommend student-athletes be informed on these practices so they can be empowered to make educated decisions pertaining to the collection and use of their biometric data (Brown & Brown, 2021). Further, Childs et al. (2025) posits that "automatic and continuous data sharing can effectively lock athletes into a decision that becomes socially difficult to reverse" (p. 11). On a similar note, Waśkiewicz et al. (2025) notes that one-time consent agreements are often leveraged indefinitely without identifying any clear withdrawal mechanisms. Moreover, Jessop & Baker (2019)

argue that the "informal nature" of the opt-in agreements that athletes are given, and the fact that they are not given meaningful opportunities to opt-out, threaten the integrity of athletes' consent and could "undermine the assertion that NCAA athletes have consented to the risks associated with their use of [biometric data] collection devices" (p. 103).

Kolovson et al. (2020) also point out that automatic, continuous collection of athlete data "diminishes an athlete's ability to control what they share and how they present themselves" (p. 20). Moreover, the authors found that automatic sensing through wearable devices limits behavioral discretion, interferes with existing routines, and reduces athletes' ability to distort data and defy rules with limited consequences. Therefore, the use of wearables for automatic data collection "diminishes athlete agency and increases staff control over athletes" (Kolovson et al., 2020, p. 22-23). When analyzed in aggregate, the reviewed body of knowledge suggests institutional pressure shapes the range of choices that athletes can realistically make without negatively impacting themselves.

Intrusion

Intrusion (n = 6) referred to the extent to which data practices invaded athletes' private lives or disturbed the athletes' tranquility or routines. Despite the average level of prominence in terms of how many articles this concern appeared in, the manifestations of this issue were some of the most poignant out of all the concerns highlighted in this review. Corr et al. (2025) explains directly that continuous monitoring devices are invasive and detrimental to athletes' mental health. Childs et al. (2025) highlights this issue through athlete testimony, as one athlete explained how the information gathering supported by WHOOP felt "intrusive" and argued that coaches should not know how much sleep athletes get every night because they may judge the athletes and doubt their level of dedication (p. 8).

Kolovson et al. (2024) also showcased athlete perspectives on this matter, with one participating athlete saying they do not mind monitoring during training because they recognize that "practice time is

practice time," but it becomes uncomfortable when they are being monitored outside of the game (p. 14). That participant also went on to directly state they "don't agree with tracking anything outside of the workouts" because that is "an invasion of personal space" (p. 14). Clegg et al. (2020) highlighted another type of non-wearable-based surveillance in the form of paying for meals with a team-issued debit card. Testimony from a softball player referred to as Nicole explained that the purchases are monitored by athletics staff, namely the nutritionist, so "if you go and say, hey, she'll be like 'Lay off the french fries' something" (p. 6).

The aforementioned instance of invasive monitoring involving the University of Tennessee Swimming and Diving team also constitutes a significant intrusion incident, especially considering the "Big Brother" element of invasiveness. With that said, it is important to note Brewer et al. (2025a) showed that this is not necessarily a universal experience, as a participant—an assistant coach—in that study stated, "our head coach is very sensitive to the [student-athletes] feeling 'big brothered' because they wear it all the time" (p. 6). Nonetheless, this extreme case involving the University of Tennessee Swimming and Diving team, and the other more ordinary instances of intrusion, captured the tangible encroachment of surveillance, primarily through wearables, into athletes' private lives. In all these studies, the problem was not only that data was collected, but that the data collection persisted into spaces that would be reasonably viewed as personal or off-limits.

Chapter 5

Discussion

This scoping review was conducted with the intent to examine how privacy concerns surrounding wearable technologies in U.S. collegiate athletics have been explored in existing literature, as far as the types of concerns, methods used for exploration, and the populations studied. Overall, the findings show that the literature identifies a variety of privacy-related issues that span all four major categories of Solove's privacy taxonomy. To be specific, surveillance (n = 14), exclusion (n = 12), secondary use (n = 10), increased accessibility (n = 9), decisional interference (n = 8), disclosure (n = 7), intrusion (n = 6), breach of confidentiality (n = 4), insecurity (n = 3), and exposure (n = 2) were identified across the body of knowledge. The central theme across the fifteen reviewed sources is that athlete data are not only collected, but that the data practices surrounding the use of wearable technologies often reduce athletes' agency over the collection, management, and use of their biometric data. Altogether, the findings suggest that the use of wearable technologies in U.S. collegiate athletics operates under a significant degree of tension between performance optimization and athlete autonomy.

The findings generated by the present study are important and valuable to the field because the data in question—athletes' biometric and behavioral data—are not trivial performance metrics. These data are personal and identifiable in nature, and their manipulation has real effects on the data subjects they are extracted from. Athletes' biometric and behavioral data that are derived from wearable technologies are utilized to influence their training and recovery regimens, their performance evaluations, and their coaches' decisions regarding their standing on their respective teams. However, the reviewed literature indicates those data subjects, the athletes, have minimal control and bargaining power, inadequate understanding, and a limited ability to object to the data practices that they are subjected to without facing real or perceived consequences. This, in turn, means the use of wearables in collegiate athletics is more than just a sport performance innovation, it is also the source of many issues including,

but not limited to, governance, ethics, consent, and athlete rights. These privacy-related issues warrant attention from all stakeholders because the affected parties, the athletes, are in a particularly vulnerable position and their fate in this context often depends on the staff at their given institution. Athletes are expected to comply with institutional demands in exchange for their continued participatory role on their athletic team, even when those demands bear the personal consequences of intrusive monitoring, secondary use of their information, and unexplained data flows, all of which are beyond their control.

The importance of these findings is also amplified because the privacy concerns outlined in this review were not isolated or hypothetical. The body of knowledge consistently identifies organizational environments where continuous monitoring is the norm, athlete consent is weak due to power asymmetries, and data are unnecessarily and overly accessible to broad networks of actors including staff, vendors, and commercial partners. More than that, most of the privacy concerns identified are backed by testimony from real athletes or coaches who have experienced these harms firsthand and feel strongly enough about those experiences to share them with researchers, often in hopes of improving the system they came from. A particularly crucial point to stress is that exclusion, secondary use, and decisional interference emerged alongside surveillance and intrusion. This implies that this issue runs deeper than the fact that athletes are constantly being monitored and their privacy is being invaded. It means athletes are subject to these realities while being wholly omitted from any meaningful participation in the governance and management of the data that is derived from their own bodies. Ultimately, this reflects the fact that the privacy concerns in this field are just as much tied to power and institutional control as they are related to the information itself.

The findings also reinforce the value of using Solove's taxonomy of privacy in this context. The present study represents the first time that the range of privacy concerns discussed in the existing literature are systematically classified according to a predetermined framework, allowing for enhanced analysis and clear takeaways regarding which privacy concerns are most prominent in the body of knowledge. Importantly, it provides a clearer basis for future research by identifying the most pressing

issues based on which privacy issues within the taxonomy appeared the most in the reviewed literature. For instance, based on the findings, the major concerns are related to institutional practices that influence the continuous monitoring of athletes' biometric data and reduce athletes' agency rather than isolated incidents like data breaches.

The findings also explain how this context has been studied in the past. A key takeaway from that information is that the existing literature is limited in methodological diversity and sampling scope. Of the reviewed articles, ten are empirical studies, and all of those are qualitative, utilizing interviews, focus groups, or speculative design. The remaining five sources are legal, conceptual, policy-focused, or review-based. The qualitative works have been very valuable, providing rich insights into athlete experiences that highlight institutional practices and ethical tensions. With that said, the limited variety of research methods illustrates how the field is still emerging and warrants further exploration. With little large-scale empirical evidence, limited work that compares institutions or sports, and a lack of quantitative or mixed-methods sources that explore how widespread these perceptions are, there are many worthy avenues for future research in this field.

Sampling patterns are another source of limitation in this field. Most of the reviewed studies drew on insights from only one or two institutions. Moreover, empirical studies in this body of knowledge relied on purposive, convenience, snowball, or network-based samples. While these sampling approaches provided rich contextual insights, they simultaneously limited the range to which these findings can be generalized across the expansive landscape of collegiate athletics in the United States. Furthermore, while athletes and their experience were the central focus of this review, the reviewed literature was inconsistent with its sampling, as some studies focused on athletes, others focused on coaches and support staff, and multiple touched on a mix of both. Additionally, the field does not yet offer a comprehensive understanding of how privacy concerns may differ across NCAA divisions or other subgroupings, nor does it take into account revenue versus non-revenue sports, gendered sport implications, or racialized institutional contexts. In short, the findings derived from the reviewed literature were successful in

showing that privacy concerns exist and identifying which of those are most prominent, but they also show that the body of knowledge has yet to address these issues in a manner that fully explains how they manifest across collegiate sport based on a variety of factors.

Recommendations for Future Research

Future research in this field should aim to build upon the exploratory qualitative work that currently dominates the body of knowledge by incorporating more diverse methods and study designs. While interviews and focus groups have provided valuable contextual insights, especially regarding athlete perceptions, and should continue to be done, the field would greatly benefit from studies that compare these issues across multiple universities, conferences, divisions, and sports. In addition, researchers should continue to explore the way these privacy concerns appear in high-revenue sports versus lower-revenue sports considering the findings of this review indicate that access, autonomy, and surveillance may be unevenly distributed across this dimension. Similarly, future research should examine how race, gender, scholarship status, injury status, team role, and other athlete differentiators shape athletes' experiences with and exposure to privacy harms. Finally, there are not many, if any, sources that evaluate certain policies, consent processes, or institutional practices that may actually improve athlete protections in the scope of wearable technology use and biometric data management. Therefore, some longitudinal and policy-oriented studies would be beneficial in helping the field identify effective solutions.

With that said, it is also important to acknowledge that such research efforts may be difficult to conduct in the context of collegiate athletics. Based on the experience of this research team during the development of this thesis, gaining institutional access to athletes, coaches, staff, or other internal organizational practices can be quite difficult. Institutional power dynamics and financial interests tied to athlete performance, competitive advantage, and biometric data management may restrict opportunities

for approval, transparency, and stakeholder engagement. Therefore, this challenge is not only a practical barrier but also a meaningful feature of the research environment in this field, as limited accessibility may reflect the opacity and control structures that underscore many of the existing privacy issues in this domain. Future scholars should still pursue diverse methods for researching this topic, but with the understanding that direct access for empirical studies may be rather difficult to secure.

Chapter 6

Limitations

The present study was subject to multiple limitations. First and foremost, this scoping review examines a rather small, niche body of literature. Despite the fact that the initial database search process returned hundreds of records, only fifteen sources satisfied all inclusion criteria outlined in this review. This illustrates the narrow scope of this study and the emerging nature of the body of literature surrounding this issue. Moreover, as described in the Discussion section, the reviewed literature was limited in scope in terms of research methods and sampling strategies. Subsequently, this review should be interpreted as a mapping of an emerging field rather than a basis for broad generalization across this context.

Another limitation is the study's restricted time frame, which constrained database results to only those published within the last ten years. This decision was made for the sake of manageability and relevance, as it helps keep contemporary developments at the center of the research, but it may have also excluded earlier sources that could have provided pertinent historical context.

On a similar note, the knowledge within this field lives in a constant state of change as both primary industries that comprise the field, technology and collegiate athletics, are extremely dynamic in terms of innovation and policy adjustments. For instance, the findings of this review indicate a need for more standardized oversight, with at least three reviewed sources—Brewer et al. (2025b), Brown & Brown (2021), and Jessop & Baker (2019)—specifically pointing out a lack of institutional guidance as a major issue. However, these points are not necessarily sustained anymore, even though one of the sources is not even one year old yet, because the landscape has already changed since then. In December 2025, the NCAA Committee on Competitive Safeguards and Medical Aspects of Sports approved guidance on the responsible use of performance technologies, which the NCAA began disseminating in January 2026 (Johnson, 2025).

This guidance touches on the potential unintended impacts of performance technologies which may affect student-athlete health, safety, performance, and mental health. The guidance also recommends NCAA member schools establish written plans that address the responsible use of these technologies, outline how relevant groups will be educated, explain how the school will manage and secure athletes' data, articulate how the school will go about purchasing and implementing new technologies, and define how the school intends to continuously improve (Johnson, 2025). This example of recent development illustrates how some findings from this review may only be snapshots of an evolving environment rather than stable, longstanding facts, considering how quickly governance and policy are frequently changing in this context.

Chapter 7

Conclusion

This thesis set out to evaluate how privacy concerns pertaining to the use of wearable technologies in U.S. collegiate athletics have been studied and to organize those findings according to Solove's taxonomy of privacy. Through a scoping review of fifteen existing studies, this thesis showcases the range of privacy concerns identified in this context. The most notable of these concerns were surveillance, exclusion, secondary use, increased accessibility, decisional interference, disclosure, and intrusion.

When considered in aggregate, these findings suggest wearable technologies in collegiate athletics raise questions of privacy, governance, consent, athlete autonomy, and institutional control. Across the body of knowledge in this scope, athletes were commonly subjected to systems and data practices that collected and used sensitive biometric data while depriving them of adequate control, a proper understanding, or any other form of meaningful participation in the process. This highlights the tension between the perceived benefits of wearable technologies and the rights of the athletes being monitored by them.

This study provides a clearer foundation for future research and discussion in this field by consolidating the fragmented catalog of literature that currently makes up the body of knowledge and simultaneously organizing the privacy concerns identified within it according to an established framework. The review also shows how the body of research in this field remains limited in methodological range and sampling breadth, leaving considerable room for further inquiry across a variety of dimensions. Overall, this thesis demonstrates how the study of privacy concerns surrounding wearable technologies in U.S. collegiate athletics warrants continued scholarly and institutional attention, especially as these technologies and the policies that govern them rapidly evolve.

Appendix

Privacy Concerns Covered in Each Included Source

Included Source Citation	Privacy Concerns Covered in Source			
	Collection	*Info Processing*	*Info Dissemination*	*Invasion*
Corr, C., Stokowski, S., Staurowsky, E. J., Paule-Koba, A. L., & Southall, R. M. (2025). The modernization of monitorization: Technological adaption and innovation as mechanisms for college athlete surveillance. Journal of Sport and Social Issues, 49(2–3), 175–195.	Surveillance	Exclusion; Secondary use; Insecurity	Exposure	Intrusion
Bae, S. W., Laccetti, A., Ozolcer, M., & Zhang, T. (2025). PXAI-Coach: Designing and evaluating a person-centric explainable AI dashboard for athlete health monitoring and coaching. In 2025 International Conference on Activity and Behavior Computing (ABC) (pp. 1–13). IEEE. https://doi.org/10.1109/ABC64332.2025.11118561	Surveillance	Secondary use	Increased Accessibility	N/A
Childs, K., Brewer, M., Thomas, S., Wilkins, C., Nichols, J. A., Boyer, K. E., & Butler, K. R. B. (2025). Mapping the flow of information from continuous wearables: Insights from elite collegiate athletes in the United States. In Proceedings of the First Annual Conference on Human-Computer Interaction and Sports (Article 8, pp. 1–15). Association for Computing Machinery. https://doi.org/10.1145/3749385.3749387	Surveillance	Exclusion; Secondary use	Breach of confidentiality	Decisional interference; Intrusion
Brewer, M., Childs, K., Thomas, S., Wilkins, C., Boyer, K. E., Nichols, J. A., Butler, K. R. B., Beatty, G. F., & Ferris, D. P. (2025a). Coach, data analyst, and protector: Exploring data practices of collegiate coaching staff. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (Article 990, pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3706598.3714026	Surveillance	Exclusion; Secondary use	Breach of confidentiality	Decisional interference; Intrusion
Kolovson, S., So, S., & Munson, S. A. (2024). Using speculative design to understand preferred futures for the design and use of tracking data in U.S. college sport teams. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1), Article 189, 1–35. https://doi.org/10.1145/3641028	Surveillance	Exclusion; Secondary use	Increased accessibility; Breach of confidentiality	Decisional interference; Intrusion
Rush, C., & Osborne, B. (2022). Benefits and concerns abound, regulations lack in collegiate athlete biometric data collection. Journal of Legal Aspects of Sport, 32(1), 62–94.	Surveillance	Secondary use	Increased accessibility; Breach of confidentiality	N/A
Brown, S. M., & Brown, K. M. (2021). Should your wearables be shareable? The ethics of wearable technology in collegiate athletics. Marquette Sports Law Review, 32(1), 97–116.	Surveillance	Exclusion; Secondary use	Increased accessibility; Disclosure	N/A
Clegg, T., Greene, D. M., Beard, N., & Brunson, J. (2020). Data everyday: Data literacy practices in a Division I college sports context. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376153	Surveillance	Exclusion	Increased accessibility; Disclosure	Decisional interference; Intrusion
Kolovson, S., Liang, C., Munson, S. A., & Starbird, K. (2020). Personal data and power asymmetries in U.S. collegiate sports teams. Proceedings of the ACM on Human-Computer Interaction, 4(GROUP), Article 5, 1–27. https://doi.org/10.1145/3375185	Surveillance	Exclusion; Secondary use	N/A	Decisional interference
Jessop, A., & Baker, T. A., III. (2019). Big data bust: Evaluating the risks of tracking NCAA athletes' biometric data. Texas Review of Entertainment & Sports Law, 20(1), 81–112.	Surveillance	Exclusion; Secondary use; Insecurity	Increased accessibility; Disclosure; Exposure	Decisional interference; Intrusion
Greene, D., Beard, N., Clegg, T., & Weight, E. (2023). The visible body and the invisible organization: Information asymmetry and college athletics data. Big Data & Society, 10(1). https://doi.org/10.1177/20539517231179197	Surveillance	Exclusion	Disclosure	N/A
Brewer, M., Childs, K., Wilkins, C., Smith, Z. R., Thomas, S., Boyer, K. E., Nichols, J. A., Beatty, G. F., & Ferris, D. P. (2025b). A qualitative examination of the evolving role of sports technology in collegiate coaching. Frontiers in Sports and Active Living, 7, Article 1644099. https://doi.org/10.3389/fspor.2025.1644099	Surveillance	Exclusion	N/A	N/A
Stenger, B., & Feng, Y. (2024). Information flows for athletes' health and performance data [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2412.05055	n/a	Exclusion; Insecurity	Increased accessibility; Disclosure	N/A
Waśkiewicz, Z., Słomka, K. J., Grzywacz, T., & Juras, G. (2025). Ethical bias in AI-driven injury prediction in sport: A narrative review of athlete health data, autonomy and governance. AI, 6(11), Article 283. https://doi.org/10.3390/ai6110283	Surveillance	Exclusion; Secondary use; Insecurity	Increased accessibility; Disclosure	Decisional interference
Clegg, T., Cleveland, K., Weight, E., Greene, D., & Elmqvist, N. (2023). Data everyday as community driven science: Athletes' critical data literacy practices in collegiate sports contexts. Journal of Research in Science Teaching, 60(8), 1786–1816. https://doi.org/10.1002/tea.21842	Surveillance	Exclusion; Secondary use	Increased accessibility; Disclosure	N/A

References

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19–32.

Arnold, J. F., & Sade, R. M. (2017). Wearable technologies in collegiate sports: The ethics of collecting biometric data from student-athletes. The American Journal of Bioethics, 17(1), 67–70. https://doi.org/10.1080/15265161.2016.1251648

Bae, S. W., Laccetti, A., Ozolcer, M., & Zhang, T. (2025). PXAI-Coach: Designing and evaluating a person-centric explainable AI dashboard for athlete health monitoring and coaching. In 2025 International Conference on Activity and Behavior Computing (ABC) (pp. 1–13). IEEE. https://doi.org/10.1109/ABC64332.2025.11118561

Brewer, M., Childs, K., Thomas, S., Wilkins, C., Boyer, K. E., Nichols, J. A., Butler, K. R. B., Beatty, G. F., & Ferris, D. P. (2025a). Coach, data analyst, and protector: Exploring data practices of collegiate coaching staff. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (Article 990, pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3706598.3714026

Brewer, M., Childs, K., Wilkins, C., Smith, Z. R., Thomas, S., Boyer, K. E., Nichols, J. A., Beatty, G. F., & Ferris, D. P. (2025b). A qualitative examination of the evolving role of sports technology in collegiate coaching. Frontiers in Sports and Active Living, 7, Article 1644099. https://doi.org/10.3389/fspor.2025.1644099

Brown, S. M., & Brown, K. M. (2021). Should your wearables be shareable? The ethics of wearable technology in collegiate athletics. Marquette Sports Law Review, 32(1), 97–116.

Catapult One. (n.d.). Why do football players wear GPS vests? https://one.catapultsports.com/blog/why-do-soccer-players-wear-gps-vests/

Childs, K., Brewer, M., Thomas, S., Wilkins, C., Nichols, J. A., Boyer, K. E., & Butler, K. R. B. (2025). Mapping the flow of information from continuous wearables: Insights from elite collegiate athletes in the United States. In Proceedings of the First Annual Conference on Human-Computer Interaction and Sports (Article 8, pp. 1–15). Association for Computing Machinery. https://doi.org/10.1145/3749385.3749387

Clegg, T., Cleveland, K., Weight, E., Greene, D., & Elmqvist, N. (2023). Data everyday as community driven science: Athletes' critical data literacy practices in collegiate sports contexts. Journal of Research in Science Teaching, 60(8), 1786–1816. https://doi.org/10.1002/tea.21842

Clegg, T., Greene, D. M., Beard, N., & Brunson, J. (2020). Data everyday: Data literacy practices in a Division I college sports context. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376153

Corr, C., Stokowski, S., Staurowsky, E. J., Paule-Koba, A. L., & Southall, R. M. (2025). The modernization of monitorization: Technological adaption and innovation as mechanisms for college athlete surveillance. Journal of Sport and Social Issues, 49(2–3), 175–195.

DeShane, T. (2024). Wearable technology in intercollegiate sport: Ethical and legal considerations of collecting student-athlete biometric data (Honors thesis, Western Michigan University). ScholarWorks. https://scholarworks.wmich.edu/honors_theses/3888

Dietrick, T. A. (2021). Biometric monitoring devices: Modern solutions to protecting athletes' data privacy. Journal of Technology Law & Policy, 21. https://doi.org/10.5195/tlp.2021.245

Düking, P., & Sperlich, B. (2024). Individualizing training procedures with wearable technology (1st ed.). Springer International Publishing. https://doi.org/10.1007/978-3-031-45113-3

Greene, D., Beard, N., Clegg, T., & Weight, E. (2023). The visible body and the invisible organization: Information asymmetry and college athletics data. Big Data & Society, 10(1). https://doi.org/10.1177/20539517231179197

Holt, Matthew. (2025). From trackers to tacklers: the fine line between performance data and personal privacy in sports wearables. Arizona State University Sports and Entertainment Law Journal, 14(2), 213-226.

Jessop, A., & Baker, T. A., III. (2019). Big data bust: Evaluating the risks of tracking NCAA athletes' biometric data. Texas Review of Entertainment & Sports Law, 20(1), 81–112.

Johnson, G. (2025, December 11). Performance technology guidance approved by CSMAS. NCAA. https://www.ncaa.org/news/2025/12/11/media-center-performance-technology-guidance-approved-by-csmas.aspx

Kolovson, S., Liang, C., Munson, S. A., & Starbird, K. (2020). Personal data and power asymmetries in U.S. collegiate sports teams. Proceedings of the ACM on Human-Computer Interaction, 4(GROUP), Article 5, 1–27. https://doi.org/10.1145/3375185

Kolovson, S., So, S., & Munson, S. A. (2024). Using speculative design to understand preferred futures for the design and use of tracking data in U.S. college sport teams. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1), Article 189, 1–35. https://doi.org/10.1145/3641028

Kumar, P. C., O'Connell, F., Li, L., Byrne, V. L., Chetty, M., Clegg, T. L., & Vitak, J. (2023). Understanding research related to designing for children's privacy and security: A document analysis. In Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (pp. 335–354). Association for Computing Machinery. https://doi.org/10.1145/3585088.3589375

L. Malleswari, N. Dheeraj, R.Joshna, P Sujatha, & B . Vaishnavi. (2024). Smart Movement Science Using Smart Kinetics Wearable Tech to Quantify Human Performance. Journal of Computing in Education, Sports and Health (JCESH, ISSN: 3049-4273), 1(1), 14-26. https://doi.org/10.69996/jcesh.2024002

Lee, H.-P. (Hank), Yang, Y.-J., Von Davier, T. S., Forlizzi, J., & Das, S. (2024). Deepfakes, phrenology, surveillance, and more! A taxonomy of AI privacy risks. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (Article 775, pp. 1–19). Association for Computing Machinery. https://doi.org/10.1145/3613904.3642116

Mak, S., & Thomas, A. (2022). Steps for conducting a scoping review. Journal of Graduate Medical Education, 14(5), 565–567. https://doi.org/10.4300/JGME-D-22-00621.1

Mohamed, Z., Ngali, M. Z., Sudin, S., Ibrahim, M. F., & Casson, A. (2024). Proceedings of the 2nd International Conference on Innovation and Technology in Sports, ICITS 2023 (1st ed.). Springer Nature Singapore.

Peters, M. D. J., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., McInerney, P., Godfrey, C. M., & Khalil, H. (2020). Updated methodological guidance for the conduct of scoping reviews. JBI Evidence Synthesis, 18(10), 2119–2126. https://doi.org/10.11124/JBIES-20-00167

Postma, D., Reidsma, D., van Delden, R., & Karahanoğlu, A. (2024). From metrics to experiences: Investigating how sport data shapes the social context, self-determination and motivation of athletes. Interacting with Computers, 1–15. https://doi.org/10.1093/iwc/iwae012

Rittenberg, A., & VanHaaren, T. (2023, December 29). Catapult: NCAA investigating unauthorized access, denies breach. ESPN. https://www.espn.com/college-football/story/_/id/39206250/ncaa-investigating-unauthorized-access-denies-breach

Rush, C., & Osborne, B. (2022). Benefits and concerns abound, regulations lack in collegiate athlete biometric data collection. Journal of Legal Aspects of Sport, 32(1), 62–94.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564.

Stenger, B., & Feng, Y. (2024). Information flows for athletes' health and performance data [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2412.05055

Toner, J. (2023). Wearable technology in elite sport. Routledge. https://doi.org/10.4324/9781003184409

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., Lewin, S., … Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. Annals of Internal Medicine, 169(7), 467–473. https://doi.org/10.7326/M18-0850

Waśkiewicz, Z., Słomka, K. J., Grzywacz, T., & Juras, G. (2025). Ethical bias in AI-driven injury prediction in sport: A narrative review of athlete health data, autonomy and governance. AI, 6(11), Article 283. https://doi.org/10.3390/ai6110283

Wang, G., & Pea, R. (2026). Algorithmic autonomy in data-driven AI. Communications of the ACM, 69(3), 74–81. https://doi.org/10.1145/3765704