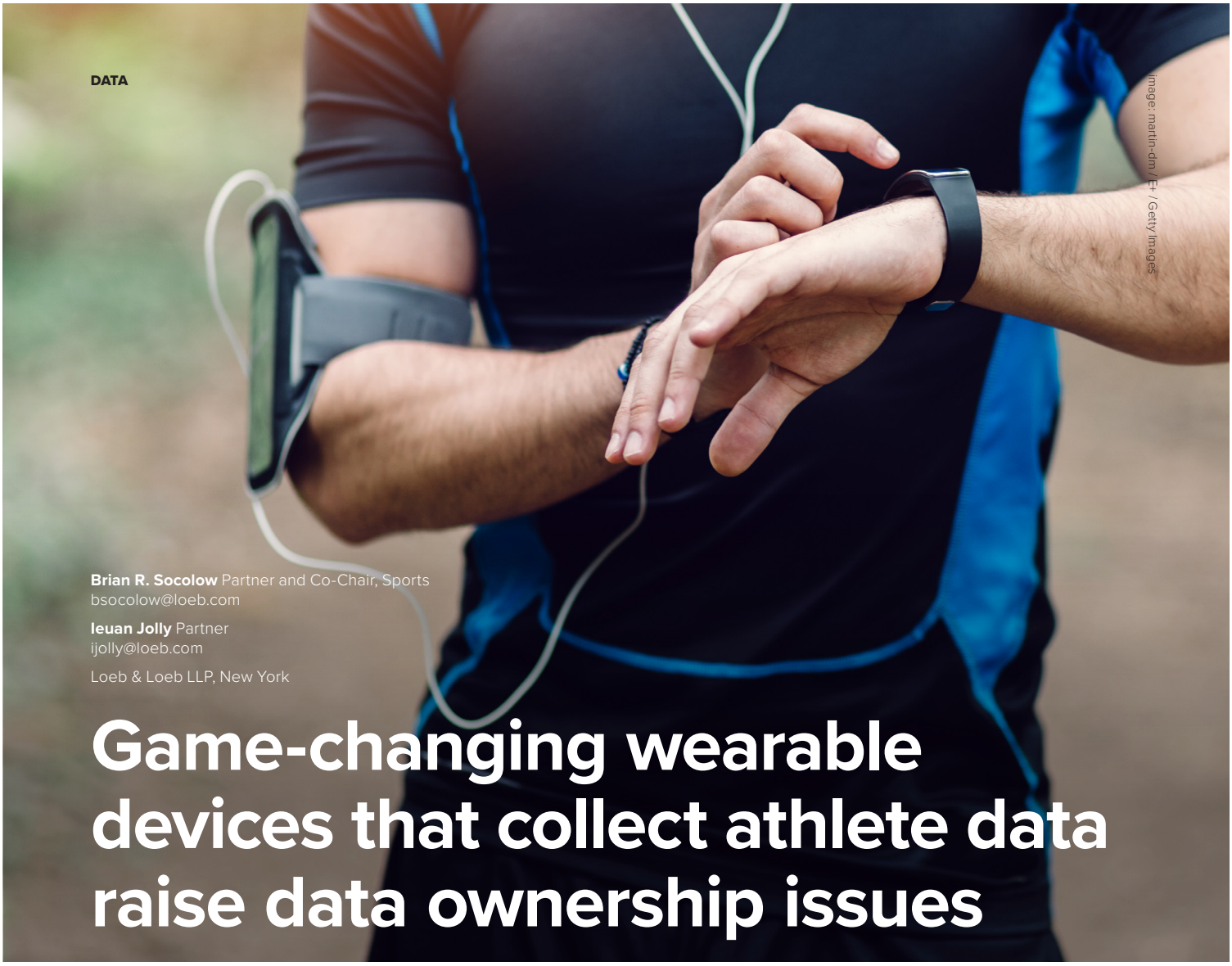

image: martin-dm / E+ / Getty Images

Brian R. Socolow Partner and Co-Chair, Sports
bsocolow@loeb.com

Ieuan Jolly Partner
ijolly@loeb.com

Loeb & Loeb LLP, New York

Game-changing wearable devices that collect athlete data raise data ownership issues

Technology is becoming an increasingly integral part of sport. From betting to performance analysis, injury prevention and coaching, innovations in wearable technology have allowed a huge amount of new data to be gathered about athletes. This new ground is yet to be clearly regulated, however. Brian Socolow and Ieuan Jolly, of Loeb & Loeb LLP, study how sports bodies are utilising sports data and the data privacy risks that come with exploiting it.

Data is a huge asset to sports organisations. The nearly insatiable appetite that fans have for information about their favourite players and teams has led sports organisations to try to maximise and monetise the opportunity this demand creates across as many channels as possible - their own channels and those owned by others, including broadcast partners, the media, video gaming and sports betting, to name a few.

Major sports teams and leagues in the US and abroad are collecting real time player performance data before, during and after practices and games to improve performance, training, injury prevention and coaching. Teams and organisations want to know how much athletes sleep, what they eat and how they work out to ultimately improve athletes' performance and protect their considerable investments in those athletes.

More than just fans are clamouring for this data. Leagues, teams, players, agents and the media now demand a constant supply of detailed performance information, driving the development and use of new, improved or simply different wearable technology. This technology is evolving faster than the law, compelling sports organisations to grapple with the sensitive ownership, intellectual property, privacy and security issues involved in collecting and using an enormous amount of athletes' personal data. In the US, the National Football League ('NFL') is blazing the trail by confronting practical and legal issues head on, even as its unique venture generates even more questions.

NFL partnership - a case study

The NFL is leading the way into this uncharted territory through a partnership between its players union and a fitness tracker manufacturer that will give players access to and ownership of their own health and performance data, as well as the option to commercialise such data. In April, the National Football League Players Association ('NFLPA') named fitness tracker maker WHOOP its official licensed recovery wearable, marking the first time a professional sports players association has partnered with a wearable technology company, according to a joint statement by the NFLPA and WHOOP.

Under the partnership, the NFLPA and WHOOP will study the effects of travel, sleep, scheduling, injuries and other

continued

factors on recovery and will generate reports to advance player safety and maximise athletic performance. Under the partnership, NFL players will own and control their individual data collected by the WHOOP Strap 2.0 fitness tracker, and will be able to commercialise their own data through the NFLPA's group licensing program. The partnership gives the NFLPA exclusive group licensing rights and WHOOP access to approximately 2,000 current NFL players.

Also on board with the partnership is OneTeam Collective, an athlete-centric accelerator launched in December by seven partners, including the NFLPA. OneTeam Collective connects businesses with the sports industry and provides rights to sports related intellectual property in areas including data analytics, wearables, consumer products and content.

The NFL began laying the groundwork for collecting player performance data back in 2011, when players agreed to wear tracking devices as part of their collective bargaining agreement. They started gathering player performance data, known as 'Next Gen Stats,' during the 2015 season and gave team general managers access to the data in 2016. The tracking devices capture real time information on every player's movements during a game through radio frequency identification signals technology installed at every stadium, which collects data from sensors on players' shoulder pads. The 'Next Gen Stats' initiative also gives broadcasters real time visualisations and replays, and makes detailed player performance data available to fans.

Other US sports leagues

The other three major US professional sports leagues - the National Basketball Association ('NBA'), Major League Baseball ('MLB') and the National Hockey League ('NHL') - are also collecting and analysing large amounts of player performance data for a variety of purposes. Wearable technology is being deployed to monitor player form and fitness, prevent injury, train officials and, of course, feed fans' seemingly unlimited demand for player and game stats.

The NBA works with Sportradar US, a sports data and integrity service provider, to distribute league statistics to fans, teams, media and other data users all over the world. The NBA also uses data collected through wearable technology during training to improve performance and avoid injury. More than 20 NBA teams collect and analyse players' biomedical data, including impact forces, turn rates and orientation, from wearable technology on player jerseys. The technology, including Catapult's OptimEye monitoring devices, can also provide teams with two dimensional animations of play in real time or post practice.

MLB has been tracking players' pitch speed and home run distances, among other performance measurements, since 2015. The league's data collection initiative, known as Statcast, offers fans a gold mine of player stats on the league's website while giving teams the ability to assess players on a new level. At the same time, the majority of MLB teams are using the Motus mThrow smart throwing sleeve, which houses a small sensor, to track pitchers' arm movements to guard against injury. Motion sensor devices made by companies including Zepp Baseball, Diamond Kinetics and Blast Motion are also used to analyse players' batting form.

So far, the NHL is trailing the other three professional leagues in the use of data analytics. However, the league is working with Catapult on wearable technology that collects information including player speed and force sustained in collisions to help address the sport's high rate of player injuries.

Myriad questions

A key challenge for these sports organisations in collecting players' performance data is navigating data ownership questions. Of particular concern is the fact that technology has evolved far more quickly than the law in this area, leaving teams, leagues, players and third parties struggling with both practical and legal issues involved in the data collection. Questions about who owns the data, how it can be used and who has access to it raise myriad issues involving player privacy, data security and ethical considerations, to name but a few. Certainly, the partnership between the NFLPA and WHOOP attempts to head off legal issues involving player privacy and data ownership before they arise, but that venture is still very much in its infancy and has yet to be tested.

The NFLPA-WHOOP venture is also unique in US sports. While the NFLPA is a full partner in the league's data collection initiative, the NBA, for example, has banned the use of wearable device data in contract negotiations and player transactions. Although the NBA's current collective bargaining agreement with its players allows teams to use data gathered from wearable devices to monitor player health and performance for training purposes, making use of the data in any other decision making process is prohibited.

Other questions raised by data collection do not have clear answers at this time. For example, are players able to opt out of data collection or limit the type of data collected? At what point is a player's privacy considered to be violated? Does a player have any reasonable expectation of confidentiality regarding any personal information that the team or the league collects?

Another privacy issue is third party access to analytical data on individual athletes. To what extent will this data be shared with broadcast partners, sports commentators and analysts? Then there are video games and fantasy sports leagues. Do players have control over the data given to game manufacturers or fantasy sports platforms? And how will player privacy be addressed in the event their data is requested by insurers or lawyers during discovery in litigation?

The security of data collected on individual players already poses an ongoing problem. In an MLB example, Christopher Correa, a former Scouting Director of the St. Louis Cardinals, was sentenced in July 2016 to nearly four years in prison for hacking the Houston Astros' player personnel database and email system. In 2013, Correa improperly accessed and downloaded the Astros' scouting list of every eligible player for that year's draft and viewed proprietary documents including notes on trade discussions, potential bonus details, and prospects' recent performances and injuries.

There are also ethical issues to consider. An article published in the *American Journal of Bioethics* in December 2016 titled 'Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies' identifies a range of ethical

Another privacy issue is third party access to analytical data on individual athletes. To what extent will this data be shared with broadcast partners, sports commentators and analysts?

considerations, including the accuracy of wearable devices. While the makers of wearable biometric measurement devices claim to offer objective data collection, it should not be assumed that the technology delivers uniformly accurate results or that the technology is being used correctly and the data interpreted and analysed competently. The article also points out that team executives may have a vested interest in the wearable devices used and that potential conflicts of interest should be examined. For example, Mark Cuban, the owner of the NBA's Dallas Mavericks, is also an investor and customer of SportVU, the maker of a player tracking system used by the NBA.

Legal limitations in the US and abroad

As technology develops, the law lags behind. In the US, a patchwork of legal and regulatory schemes may have an indirect impact on privacy and security issues involved in the collection of an athlete's biometric data from wearable technology devices. Data ownership impacts employment, player contract and collective bargaining issues, but no professional sports industry standards or general privacy and employment laws currently exist to assist the parties involved.

The US Privacy Act of 1974 governs the collection, maintenance, use and dissemination of information about individuals, but applies only to data maintained in federal agencies' databases. The Americans with Disabilities Act limits employers' access to employees' medical information, and the Genetic Information Nondiscrimination Act of 2008 prohibits the use of genetic information to make health insurance and employment decisions, but neither specifically addresses biometric data. The Health Insurance Portability and Accountability Act ('HIPAA'), a US law covering medical information, does not directly apply to biometric data either.

A number of states have enacted laws restricting the collection and use of biometric data. While some apply only to specific populations (California is among the states that restrict the collection and use of the biometric data of students) or to collection by governmental agencies for uses unrelated to law enforcement, both Illinois and Texas restrict the collection and use of this data by businesses. The Illinois Biometric Information Privacy Act ('BIPA'), for example, regulates companies collecting biometric data and grants Illinois residents a private right of action if their biometric data is collected or used in violation of BIPA. Among other rules, BIPA requires informed consent for collection, allows only a narrow set of circumstances under which companies can disclose the data, and mandates specific data protection obligations and retention guidelines. Notably, BIPA prohibits companies from selling or 'otherwise profiting' from biometric data. What the statute includes in this vague description remains undefined at this point.

Legislatures in at least four more states have proposed BIPA-like laws restricting the collection and use of biometric data. Some states also have existing data security and breach laws that specifically include biometric information in their definitions of covered personal information, and many other state data breach laws could sweep biometric data into the broader category of 'personal information' without specific mentions. Professional athletes are protected by federal and state employment regulations, their player contracts, and collective bargaining agreements. Led by the NFLPA's partnership with WHOOP, it's likely that teams and leagues will address outstanding issues on their own long before lawmakers do.

Outside the US, changes to privacy laws in the European Union will likely have some bearing on the increasingly globalised US sports industry. In 2016, the European Parliament and the Council of the European Union passed the General Data Protection Regulation, a wide ranging protection and privacy law that will take effect in May 2018. The Regulation applies primarily to businesses established in the EU but also to businesses based outside the EU that offer goods and services to, or monitor individuals in, the EU.

More specifically, but still in a non-sports context, employers in the Netherlands that use wearable devices to track employee health as part of wellness programs have been subject to litigation barring the use of the devices in these programs. The Netherlands' Data Protection Authority investigated two companies with wearable technology programs and ruled that employees are financially dependent on their employers and therefore don't have the power to give consent when it comes to revealing sensitive personal health data.

On the horizon

Access to athlete health and performance information could also have an impact on betting on sports. In the US, betting on sports is currently illegal in 46 states under the Professional and Amateur Sports Protection Act, enacted in 1992. Sports betting is currently legal in Delaware, Montana, Nevada and Oregon, which met the Law's grandfathering requirements by demonstrating a history of legal gambling. Of course, betting on sports remains a thriving underground operation.

Efforts are underway in various states to legalise sports betting, most notably in New Jersey. In June, the US Supreme Court agreed to hear arguments this fall on whether wagering on sports should be legalised. If that happens, a whole new set of privacy and security concerns about collecting health data from athletes could arise.

Sports betting is much more prevalent outside the US. In the EU, sports betting is a big business and growing bigger, with online gambling reportedly driving significant growth. Regulation of sports betting is not centralised in the EU; regulation and licensing are handled on a national or local level in each Member State. At the end of 2015, the gambling regulatory authorities of the European Economic Area Member States (EU Member States and Iceland, Liechtenstein and Norway) signed a cooperation arrangement focused on enhancing cross border cooperation on the challenges of online gambling, including sports betting.

Meanwhile, data collection technology continues to rapidly evolve. Injectable, ingestible and implantable technologies are being hailed as the next big development in collecting health and performance data from athletes. With the legal framework for addressing the privacy, data security, ownership and employment issues already lagging behind, it may be up to the sports industry to take the lead and set its own standards.