The Sport of Cybersecurity: How Professional Sport Leagues Can Better Protect the Competitive Integrity of Their Games

Nathaniel Grow
*Indiana University, grown@iu.edu*

Scott J. Shackelford
*Indiana University, sjshacke@indiana.edu*

Follow this and additional works at: [https://lawdigitalcommons.bc.edu/bclr](https://lawdigitalcommons.bc.edu/bclr)

Part of the Computer Law Commons, Intellectual Property Law Commons, and the Internet Law Commons

**Recommended Citation**


This Article is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.
# THE SPORT OF CYBERSECURITY: HOW PROFESSIONAL SPORTS LEAGUES CAN BETTER PROTECT THE COMPETITIVE INTEGRITY OF THEIR GAMES

NATHANIEL GROW  
SCOTT J. SHACKELFORD

## INTRODUCTION

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>474</td>
</tr>
</tbody>
</table>

## I. INTRODUCING THE MULTIFACETED CYBER THREAT

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>476</td>
</tr>
</tbody>
</table>

### A. Exploring the Internet of Everything

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>477</td>
</tr>
</tbody>
</table>

### B. Public Facilities and Critical Infrastructure Protection

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>479</td>
</tr>
</tbody>
</table>

## II. ANALYZING THE APPLICABLE LEGAL REGIMES PROTECTING THE INTEGRITY OF PROFESSIONAL SPORTS TEAMS, FACILITIES, AND INTELLECTUAL PROPERTY

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>481</td>
</tr>
</tbody>
</table>

### A. The Computer Fraud and Abuse Act

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>481</td>
</tr>
</tbody>
</table>

### B. The Law of Trade Secrecy

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>483</td>
</tr>
</tbody>
</table>

#### 1. Uniform Trade Secrets Act

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>485</td>
</tr>
</tbody>
</table>

#### 2. Economic Espionage Act

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>487</td>
</tr>
</tbody>
</table>

#### 3. Defend Trade Secrets Act

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>488</td>
</tr>
</tbody>
</table>

## III. POTENTIAL CYBER THREATS TO THE U.S. PROFESSIONAL TEAM SPORTS INDUSTRY

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>489</td>
</tr>
</tbody>
</table>

### A. Security of In-Game Technology

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>490</td>
</tr>
</tbody>
</table>

### B. Security of Shared Data

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>492</td>
</tr>
</tbody>
</table>

### C. Security of Proprietary Databases

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>495</td>
</tr>
</tbody>
</table>

### D. Security of Biometric Tracking Devices

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>496</td>
</tr>
</tbody>
</table>

### E. Gambling-Related Concerns

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>497</td>
</tr>
</tbody>
</table>

## IV. LEAGUES’ CURRENT FRAMEWORK FOR CYBER-RISK MANAGEMENT

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>499</td>
</tr>
</tbody>
</table>

### A. Existing Applicable League Rules

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
</tr>
</tbody>
</table>

#### 1. Major League Baseball

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
</tr>
</tbody>
</table>

#### 2. National Football League

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>501</td>
</tr>
</tbody>
</table>

#### 3. National Basketball Association

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>503</td>
</tr>
</tbody>
</table>

#### 4. National Hockey League

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>504</td>
</tr>
</tbody>
</table>

### B. League Disciplinary Precedents

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>505</td>
</tr>
</tbody>
</table>

#### 1. Major League Baseball

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>505</td>
</tr>
</tbody>
</table>

#### 2. National Football League

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>508</td>
</tr>
</tbody>
</table>

## V. POLICY IMPLICATIONS

<table>
<thead>
<tr>
<th>Subsection</th>
</tr>
</thead>
<tbody>
<tr>
<td>510</td>
</tr>
</tbody>
</table>

### A. What We Can Learn from Using the Lens of Norm Entrepreneurs and Polycentric Governance

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>510</td>
</tr>
</tbody>
</table>

### B. Proposing an Updated Cybersecurity Policy for U.S. Professional Sports Leagues

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
</tr>
</tbody>
</table>

### C. A Potential Government Solution for U.S. Professional Sports Leagues’ Cybersecurity Risks

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>515</td>
</tr>
</tbody>
</table>

## CONCLUSION

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>521</td>
</tr>
</tbody>
</table>
THE SPORT OF CYBERSECURITY: HOW PROFESSIONAL SPORTS LEAGUES CAN BETTER PROTECT THE COMPETITIVE INTEGRITY OF THEIR GAMES

NATHANIEL GROW*  
SCOTT J. SHACKELFORD**

Abstract: From a Major League Baseball scouting director using a cyberattack to break into a competitor’s records, to an NBA franchise being compromised in a phishing scheme, U.S. professional sports leagues are waking up to the fact that cybersecurity is no longer just a problem for the government or tech firms—it has now reached into the playing field, locker room, and boardroom. This Article breaks new ground by examining how the four major U.S. professional sports leagues—Major League Baseball, the National Football League, the National Basketball Association, and the National Hockey League—are protecting themselves from these cyber risks that threaten the competitive integrity of their games, and proposes ways in which the leagues could do more to proactively mitigate their cyber risk.

INTRODUCTION

Consider the following scenario—there is less than a minute left in Super Bowl LV, and the New England Patriots are leading the Dallas Cowboys 24-20. The Cowboys are making a final drive that could win them the game, but face a fourth-down play needing to gain eight yards to score the go-ahead touchdown. During their final timeout, the Cowboys coaching staff use their league-sanctioned tablet computers to access the team playbook, and select a...
The Patriots are well prepared for the play, though, resulting in a quick sack of the quarterback. As a result, New England once again wins the Super Bowl championship.

Controversy ensues during a subsequent investigation when the National Football League (NFL) discovers that an insider threat from the Cowboys’ staff gave the Patriots access to the teams’ internal systems, and allowed the Patriots to monitor Dallas’ tablet computers in order to discover which play the Cowboys would be calling. Perhaps most surprisingly of all, the public is shocked to discover that such blatantly anticompetitive conduct is not directly regulated under any current NFL rule.

From the scouting director for a Major League Baseball (MLB) team using a cyberattack to break into a competitor’s records, to a National Basketball Association (NBA) franchise being compromised in a phishing scheme, U.S. professional sports leagues are waking up to the fact that cybersecurity is no longer just a problem for governments or tech firms—it has now reached into the playing field, locker room, and boardroom. Unfortunately, the leagues’ efforts to safeguard the competitive integrity of their sporting competition from these threats have been relatively slow to develop. Rather than formulate league-wide cybersecurity standards, U.S. leagues appear to largely defer to their teams to protect themselves from cyber intrusions. Meanwhile, the leagues have also failed to enact specific rules to deter their teams from targeting one another in cyberattacks. At the same time, the existing academic literature has completely overlooked the industry, and failed to analyze the unique cyber risks that these high-visibility leagues and franchises face.


2 See infra notes 179–187 and accompanying text (discussing the hacking of the Houston Astros by a former employee of the St. Louis Cardinals).

3 See Jon Fingas, The Milwaukee Bucks Fell Prey to a Phishing Email Scam, ENGADGET (May 21, 2016), https://www.engadget.com/2016/05/21/milwaukee-bucks-fall-to-phishing-scam/ [https://perma.cc/6K43-ZRGN] (reporting that the NBA’s Milwaukee Bucks “fell victim to a phishing scam that compromised the basketball team’s financial data”).

4 See, e.g., Chris Bing, There’s Now a Cybersecurity Organization Dedicated to U.S. Sports, FEDSCOOP (Sept. 22, 2016), https://www.fedscoop.com/sports-safo-cybersecurity-2016/ [https://perma.cc/YZ7U-Z5UB] (discussing the formation of an information sharing and analysis organization (ISAO) focused on “sports-related digital assets”).

5 See Bill Shaikin, Angels, Dodgers Are Responsible for Their Own Cyber Security, L.A. TIMES (June 16, 2015), http://www.latimes.com/sports/la-sp-baseball-security-20150617-story.html [https://perma.cc/H2V6-6THJ] (reporting that in MLB, “each team is responsible for its own cyber security, but MLB employs experts and makes them available to consult with teams”); see also infra note 143 and accompanying text.

6 See infra notes 94–141 and accompanying text (noting the relative dearth of cybersecurity-related rules and regulations promulgated by the four major U.S. professional sports leagues). That said, the Cyber Resilience Institute recently established a Sports ISAO to attempt to address cybersecurity risks in this area. See Bing, supra note 4 (discussing the initiative).
This Article breaks new ground by both identifying the numerous potential competition-related cybersecurity risks the four major U.S. professional sports leagues—MLB, the NFL, the NBA, and the National Hockey League (NHL)—currently face, and assessing the current steps that the leagues are taking to safeguard themselves from these dangers. Ultimately, this Article proposes ways in which the leagues can better protect the competitive integrity of their games in order to proactively ward off worst-case scenarios along the lines of the hypothetical offered above.

The Article is structured as follows. Part I introduces the range of cyber threats pertinent to U.S. professional sports leagues with a focus on Internet of Things (IoT) security and critical infrastructure protection. Part II surveys the existing U.S. legal regime regulating cybersecurity, including most prominently the law of trade secrecy. Part III examines potential competition-related cyber risks already manifest in the U.S. professional team sports industry, including the manipulation of in-game technology, shared data, proprietary databases, and biometric-tracking devices, along with gambling-related concerns. Part IV summarizes the leagues’ existing frameworks to help mitigate these cyber risks. Part V identifies potential shortcomings in the leagues’ current approach to cybersecurity issues and proposes measures the leagues could adopt to better protect the competitive integrity of their competitions from future cyberattack.

I. INTRODUCING THE MULTIFACETED CYBER THREAT

It is no secret that the cost of cyberattacks on both the public and private sectors is mounting. According to a 2018 National Bureau of Economic Research report, for example, large companies that are victims of a cyberattack in which customers’ personal data are compromised realize an approximately 1.1 percent loss in market value and a 3.4 percentage point drop in sales growth. These statistics are sobering, given the prevalence of cyberattackers successfully penetrating even the most guarded corporate networks. One recent example of this all too familiar phenomenon was the alleged Chinese government hacking of a U.S. Navy contractor charged with developing a top-secret super-
sonic missile. In fact, one leading cybersecurity scholar has reported that “ninety-seven percent of Fortune 500 companies have been hacked . . . and likely the other [three] percent have too, they just don’t know it.” Three trends in particular are making it much more difficult for organizations of all sizes to mitigate the array of cyber risks they face: (1) the evolution of the “Internet of Everything”; (2) the difficulty of protecting trade secrets in such an interconnected digital ecosystem; and (3) the proliferation of threats to critical infrastructure, including public facilities. Each of these trends is analyzed in turn to provide context for these debates before focusing in on the specific issues confronting the U.S. professional sports industry.

A. Exploring the Internet of Everything

In late 2016, a distributed denial of service (DDoS) attack, later known as the Mirai botnet, curtailed internet servers run by a tech firm called Dyn. That, in and of itself, might not have been newsworthy; in fact, botnet-enabled DDoS attacks are now commonplace. Nevertheless, the Mirai botnet was noteworthy, given the havoc it wrought by slowing, and in some cases stopping, internet services for much of the eastern United States. The Mirai botnet...
net was so successful, and noteworthy, because it took advantage of security vulnerabilities in the IoT.20 Initially, some thought that the attack was politically motivated, but investigators determined that it was not, in fact, a shadowy group or nation state behind the botnet—instead it was college students, trying to get an edge on the video game Minecraft.21 According to one observer, the students “didn’t realize the power they were unleashing” and compared their actions to the Manhattan Project.22

Although accounts differ as to the origin of the “Internet of Things,” many point to the pivotal role played by Kevin Ashton in popularizing the term during a 1999 presentation he gave to Proctor & Gamble.23 But the global push to make our businesses, homes, toasters, and even our bodies smarter through technology in fact dates back decades.24 For example, in the 1980s, researchers at Carnegie-Mellon University installed sensors and switches in a vending machine to count the number of bottles present and check their temperature.25 By the 1990s, despite the rapid scaling of the internet infrastructure, dial-up internet connectivity with relatively slow connection speeds continued to hold back the growth of IoT applications, a hurdle that has only been overcome since 2010 with the advent of faster computers.26 Still, IoT issues are not well under-

20 See Garrett M. Graff, How a Dorm Room Minecraft Scam Brought Down the Internet, WIRED (Dec. 13, 2017), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/ [https://perma.cc/5NUF-8J7H] (noting the botnet was “powered by unsecured internet-of-things devices like security cameras and wireless routers”); see also Lawrence J. Trautman, Cybersecurity: What About U.S. Policy?, 2015 U. ILL. J.L. TECH. & POL’Y 341, 348 (discussing changes brought on by IoT applications); Brendan Alan Melander, Note, Smart Stadiums: An Illustration of How the “Internet of Things” Is Revolutionizing the World, 6 ARIZ. ST. U. SPORTS & ENT. L.J. 349, 350–51 (2017) (“IoT is a broad array of interconnected devices that use sensors to gather data, share that data between devices, and store or evaluate that data. This machine-to-machine (M2M) communication, in combination with the sensors, allows for devices that traditionally had no use for the Internet (e.g., such as coffee makers, alarm clocks, and refrigerators) to become ‘smart.’”).

21 Graff, supra note 20.

22 Id.


25 See John A. Rothchild, Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else), 66 CLEV. ST. L. REV. 559, 572 n.61 (2018) (noting one of the first IoT devices may have been a Coca-Cola vending machine that was connected to Carnegie Mellon University’s computer network in 1982 in order to allow users to check whether the machine was stocked and the temperature of the soda bottles).

stood or appreciated. One 2014 survey, for example, found that eighty-seven percent of respondents had never even heard of the “Internet of Things.” This apathy, though, does not mask the real vulnerabilities that the explosion in smart devices creates, which by some estimates could reach 200 billion devices by 2020.

IoT vulnerabilities can cause widespread disruptions, such as when they are utilized to spread ransomware attacks. This occurred during the WannaCry and later NotPetya attacks, which impacted more than 7,000 firms globally and cost the shipping giant Maersk more than $200 million. These IoT vulnerabilities can, in turn, help fuel the theft of invaluable trade secrets, which are the lifeblood of major Fortune 500 firms as well as the professional sports industry. Indeed, sports teams are increasingly relying on IoT applications to track their players’ movements, training, and dietary regimens.

B. Public Facilities and Critical Infrastructure Protection

The phrase “critical infrastructure” can conjure the most important aspects of national life and includes the services on which all of us ultimately rely from electricity and water to finance and healthcare. As has been argued, “[c]ontaminated water sanitation systems may injure thousands before any issue is detected; vulnerable electrical grids may blackout cities; and disrupted financial systems may destabilize economies.” The United States, and na-

---


30 See infra notes 127–133 and accompanying text.


32 Scott Shackelford et al., Making Democracy Harder to Hack, 50 U. MICH. J.L. REFORM 629, 634 (2017). An assault on critical infrastructure through cyberattacks has already been dramatized in film:

The 2007 blockbuster [Live Free or Die Hard] dramatized the prospect of a large-scale cyber assault: in it, a frustrated former Pentagon insider and a team of hackers interrupted U.S. air traffic control, power, telecommunications, and financial services. According to Richard Clarke, such a scenario is feasible under certain circumstances.
tions around the world, have long grappled with the appropriate mix of laws and policies to help safeguard vital industries, which the Department of Homeland Security has defined in the U.S. context to encompass sixteen sectors. These sectors are not fixed. For example, elections were included under the public facilities sector in January 2017. Professional sports are, in fact, part of U.S. critical infrastructure under the “Commercial Facilities Sector,” which includes “professional sports leagues and federations” along with operations that “draw large crowds” including stadiums and arenas. Indeed, there is now even an information sharing and analysis organization (ISAO) to help professional sports leagues pool cybersecurity expertise more effectively, an organization that mirrors the Information Sharing and Analysis Center (ISAC) system prevalent across industries from retail to automobiles.

Many critical infrastructure sectors in the U.S. boast an array of federal and state regulations, given their vital status to national life—examples range from the North American Electric Reliability Corporation standards to the

---


36 See Bing, supra note 4 (discussing the formation of the Sports ISAO).

37 See Chris Laughlin, Note, Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations Are Effective, 14 COLO. TECH. L.J. 345, 355 (2016) (observing that “‘under current law . . . many [federal agencies] have sector-specific cybersecurity responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector’” (quoting ERIC A. FISCHER, CONG. RESEARCH SERV. R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 4 (2013))).

38 See Mandatory Standards Subject to Enforcement, NORTH AM. ELECTRIC RELIABILITY CORP., http://www.nerc.net/standardsreports/standardssummary.aspx [https://perma.cc/6EC8-BZJA].
Health Insurance Portability and Accountability Act (HIPAA)\textsuperscript{39}—but, as we will see below, professional sports leagues have long enjoyed a special status in which policymakers have allowed leeway to self-regulate. The question going forward is whether this should continue in light of the serious cyber risks facing these organizations, their players, staffs, and fans.

II. ANALYZING THE APPLICABLE LEGAL REGIMES PROTECTING THE INTEGRITY OF PROFESSIONAL SPORTS TEAMS, FACILITIES, AND INTELLECTUAL PROPERTY

Any potential cyber intrusion against a professional sports team operating in the United States would potentially run afoul of several existing laws. In some cases—such as the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act (EEA)—these laws impose potential criminal liability against the wrongdoer, while in other cases—including the Uniform Trade Secrets Act (UTSA) and the Defend Trade Secrets Act (DTSA)—the victim must instead seek civil remedies\textsuperscript{40}.

A. The Computer Fraud and Abuse Act

Perhaps most significantly, attempts to engage in unauthorized cyber intrusions could run afoul of the CFAA.\textsuperscript{41} The story of the CFAA begins, strangely enough, with a blockbuster movie. In 1983, the movie \textit{WarGames} illustrated the potential of hackers to break into the nation’s nuclear arsenal.\textsuperscript{42} Reagan Administration officials took the threat seriously enough that they worked with Congress to pass the 1986 CFAA.\textsuperscript{43} Among other things, the CFAA criminalizes “unauthorized access” to a computer or the unauthorized “transmission” of malware (malicious software).\textsuperscript{44}


\textsuperscript{40} See infra notes 41–93 and accompanying text.


\textsuperscript{42} See \textit{WarGames} (United Artists 1983).


On its face, then, the CFAA would seem to deter hackers from targeting professional sports teams, their networks, and their trade secrets. Disagreement persists about the bounds of the CFAA, however, including its treatment of active defense.\textsuperscript{45} For example, could a team that has been hacked supposedly by a competitor engage in active defensive measures against the supposed perpetrator, such as the Cowboys hacking back against the Patriots, as discussed in the introduction? Again, such a response would seem to run afoul of the CFAA, but questions remain over the interpretation of “unauthorized access” along with the likelihood of enforcement. The U.S. Department of Justice, for instance, has only gone so far as to call the practice “likely illegal.”\textsuperscript{46} Meanwhile, some critics contend that the CFAA bars organizations from responding to cyberattackers, even those located in foreign nations.\textsuperscript{47} Yet that has not stopped organizations from hacking back. For example, “[a]t the Black Hat USA security conference in 2012, [thirty-six] percent of respondents said they had engaged in ‘retaliatory hacking’ on at least one occasion.”\textsuperscript{48}

Historically, U.S. law enforcement has not looked favorably upon such a “vigilante view” of cybersecurity, with some indicating that the problem is too large for law enforcement to manage and that “problems still arise when companies ‘get caught or when innocent bystanders are harmed.’”\textsuperscript{49} Attribution is a central, and challenging aspect of this problem. Richard Ledgett, the former deputy director of the NSA, has said “[a]tttribution is really hard. Companies have come to me with what they thought was solid attribution, and they were

\textsuperscript{45} See Jeff Kosseff, Defining Cybersecurity Law, 103 IOWA L. REV. 985, 1019 (2018) (“The CFAA also has attracted criticism from some commentators for its likely—though far from certain—prohibition on the ability of private parties to ‘hack back’ against those that attack them.”); see also Jay P. Kesey & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyber-space, 25 HARV. J. L. & TECH. 429, 435 (2012) (equating “cyber counterstrikes” to “hack[ing] back”).


\textsuperscript{49} Craig et al., supra note 41, at 732 (quoting Robert Anderson et al., OFFENSE VS. DEFENSE 1, 22 (White Paper 2005), https://pdfs.semanticscholar.org/4918/c5cf455fe22af1e342edfcf640d3b83687af.pdf [https://perma.cc/GQ45-HVXX]).
wrong.”50 Stewart Baker, former assistant secretary for policy at the U.S. Department of Homeland Security (DHS), has asserted that defenders, for example, who seek to reacquire data—including trade secrets—that were stolen without authorization might not run afoul of the CFAA prohibitions.51 Other commentators, such as Professor Orin Kerr, point out that the CFAA is focused on protecting the rights of computer owners, not data owners, and so the argument does not pass legal muster.52 Professor Kerr’s interpretation seems to be consistent with the majority view internationally, as seen in the Paris Call for Trust and Security in Cyberspace.53 In practice, however, Baker’s view seems to be winning out, given that, according to Ben Wittes of the Brookings Institution, “[a] fair bit of [hacking back] is going on. No one is saying it is OK. But no one is getting prosecuted for it.”54

B. The Law of Trade Secrecy

In addition to the computer-specific protections afforded by the CFAA, the law of trade secrecy also provides parties with protection from unauthorized cyber intrusion. Although definitions vary, a trade secret may be defined under American law as “any confidential business information which provides an enterprise [with] a competitive edge” and is not publicly known.55 Common exam-

52 See id.

[A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information . . . .

amples include formulas, sales methods, and industrial processes.56 Although na-
tions’ rules vary regarding the manner in which they protect trade secrets—with
some providing express protection under their laws, and others merely protecting
trade secrets under general laws governing unfair competition—the unauthorized
use of trade secrets is generally regarded internationally “as an unfair practice
and a violation of the trade secret.”57 As has already been noted, cyberspace
permits the theft of trade secrets at a scale never before seen in human history.
Some estimates have suggested that 5.2 trillion dollars in economic value is at
risk of cyberattacks for the years 2019 to 2023.58 Although a staggering figure, if
true, it becomes more believable when considering that the vast majority of the
value of S&P 500 firms are now tied up in intangible assets, namely trade secrets
and other intellectual property, as shown in Figure 1.

56 The UTSA, which is generally followed by local authorities within the United States, defines a
trade secret as information that:

(i) derives independent economic value, actual or potential, from not being generally
known to, and not being readily ascertainable by proper means by, other persons who
can obtain economic value from its disclosure or use, and (ii) is the subject of efforts
that are reasonable under the circumstances to maintain its secrecy.

UNIF. TRADE SECRETS ACT § 1(4) (UNIFORM L. COMM’N 1985); see J.H. Reichman, Universal Min-
imum Standards of Intellectual Property Protection Under the TRIPS Component of the WTO Agree-
ment, 29 INT’L LAW. 345, 378 (1995) (noting the UTSA “is widely adopted at the local level in the
United States”). This definition is reinforced by the Restatement (Third) of Unfair Competition Law,
which defines a trade secret as “any information that can be used in the operation of a business or
other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic
advantage over others.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (AM. LAW INST.
1995).

57 What Is a Trade Secret?, supra note 55. See generally, e.g., Scott J. Shackelford et al., Using
BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets Through Bilateral

58 See KELLY BISSELL & LARRY PONEMON, ACCENTURE SEC., NINTH ANNUAL COST OF CY-
cybercrime-study-final.pdf [https://perma.cc/3RLF-DBTC]. Other estimates place the value of lost
intellectual property at approximately $300 billion per year. See Reuters, Congress Just Passed Tough
28/congress-trade-secret-legislation/ [https://perma.cc/PVJ8-V9UM].
Given the potential value of these assets to the U.S. economy, a series of different legal protections have been promulgated at both the federal and state levels in order to deter parties from stealing one another’s trade secrets.

1. Uniform Trade Secrets Act

Dating back to 1979, the UTSA has historically provided the most important legal protection for trade secrets in the United States. Currently, the UTSA has been adopted in some form by forty-eight states and the District of Columbia. Meanwhile, the two remaining jurisdictions—New York and Massachusetts—have both adopted similar requirements for trade secret protection, despite not adopting the UTSA outright.

Under the UTSA, a trade secret is entitled to legal protection so long as it meets two requirements. First, the information in question must “derive[]

---


62 See David Orozco, Amending the Economic Espionage Act to Require the Disclosure of National Security-Related Technology Thefts, 62 CATH. U. L. REV. 877, 889 (2013) (observing that although New York and Massachusetts have not passed the UTSA into law, they have adopted laws that are similar in their effect).

63 Under the UTSA, “information” is defined broadly to include “a formula, pattern, compilation, program, device, method, technique, or process.” UNIF. TRADE SECRETS ACT § 1(4).
independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.”\textsuperscript{64} Specifically, rather than require “absolute secrecy,”\textsuperscript{65} courts have instead interpreted this requirement to merely demand that the information sought to be protected has not “escaped into the mainstream of public knowledge.”\textsuperscript{66}

Second, a plaintiff pursuing a case under the UTSA must also show that the trade secret “is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”\textsuperscript{67} Courts applying this requirement aim to strike a balance between enabling companies to use “sufficient precautions to protect a company’s secret on the one hand, while not imposing overly-burdensome precautions that would impair the functioning of its business on the other hand.”\textsuperscript{68} Along these lines, companies “need not undertake ‘[h]eroic efforts’” to protect the secrecy of their information, but instead simply employ sufficient measures under the circumstances.\textsuperscript{69} Examples of sufficient reasonable efforts may include utilizing electronic protective measures such as password protection and computer firewalls, along with more traditional options such as utilizing contractual provisions like non-disclosure and non-compete agreements.

Assuming that the two UTSA requirements are met, a company can then pursue legal relief against anyone who has misappropriated its trade secret. Under the UTSA, misappropriation can occur in one of two ways: (i) through the “acquisition of a trade secret . . . by improper means,” or (ii) through the knowing “disclosure or use of a trade secret” acquired by improper means.\textsuperscript{71} The act defines “improper means” to include methods such as “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.”\textsuperscript{72} Should the plaintiff prevail in a misappropriation case under the UTSA, potential remedies include injunctive relief, damages for “both the actual loss caused by [the] misappropriation and [any] unjust enrichment” received by the infringer, along with pu-

\textsuperscript{64} Id.

\textsuperscript{65} Elizabeth A. Rowe, \textit{Contributory Negligence, Technology, and Trade Secrets}, 17 GEO. MASON L. REV. 1, 9 (2009) (offering that it is well established that “reasonable efforts do not require absolute secrecy”).

\textsuperscript{66} JAMES POOLEY, \textit{TRADE SECRETS} § 4.04(2)(a) (2017).

\textsuperscript{67} UNIF. \textit{TRADE SECRETS ACT} § 1(4)(ii).

\textsuperscript{68} Rowe, supra note 65, at 9.

\textsuperscript{69} Grow & Grow, supra note 61, at 1586 (quoting Matthew J. Frankel, \textit{Secret Sabermetrics: Trade Secret Protection in the Baseball Analytics Field}, 5 ALBANY GOV’T L. REV. 240, 253 (2012)).

\textsuperscript{70} See Frankel, supra note 69, at 253 (discussing potential reasonable measures).

\textsuperscript{71} UNIF. \textit{TRADE SECRETS ACT} § 1(2).

\textsuperscript{72} Id. § 1. Notably, the law also “identifies actions that do not qualify as misappropriation, including reverse engineering, observing the information in public display, and discovery by independent creation.” Grow & Grow, supra note 61, at 1592–93.
nitive damages and attorney’s fees in cases involving willful and malicious misappropriation.\(^7\)

2. Economic Espionage Act

The 1996 enactment of the EEA marked the first attempt to federalize and criminalize the law of trade secrecy.\(^7\) The passage of the act was motivated by the fact that federal prosecutors had, at times, previously struggled to shoehorn the theft of a trade secret into other, more generally applicable laws—such as those prohibiting mail and wire fraud—as well as Congress’s increased concern over foreign economic espionage.\(^7\)

Specifically, the EEA prohibits two different forms of trade secret theft. First, the law prohibits the misappropriation\(^7\) of a trade secret in order to benefit a foreign entity.\(^7\) Second, the law criminalizes any domestic theft of a trade secret for economic gain.\(^7\) For purposes of both provisions, the EEA defines the concept of a trade secret in a manner similar to that adopted in the UTSA.\(^7\) Specifically, the EEA requires that the information’s owner take reasonable measures to keep it secret and that “the information derives independent economic value, actual or potential, from not being generally known.”\(^8\)

The EEA, however, diverges from the UTSA in several important respects. For starters, in order to trigger liability under the EEA, the trade secret must be used in interstate or foreign commerce.\(^8\) Similarly, in contrast to the UTSA, the EEA also imposes a *mens rea* requirement by mandating a showing

---

\(^{73}\) UNIF. TRADE SECRETS ACT § 3.

\(^{74}\) See Grow & Grow, supra note 61, at 1594.

\(^{75}\) See Kelley Clements Keller & Brian M.Z. Reece, Economic Espionage and the Theft of Trade Secrets: The Case for a Federal Cause of Action, 16 TUL. J. TECH. & INTELL. PROP. 1, 8–12 (2013) (noting that pre-existing federal criminal statutes “were not designed to penalize trade secret theft,” before summarizing the legislative history of the EEA).

\(^{76}\) Specifically, the EEA defines misappropriation as an act involving one who:

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; [or] (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization . . . .


\(^{77}\) Id. § 1831(a).

\(^{78}\) 18 U.S.C. § 1832(a).


\(^{81}\) Id. § 1832.
that the defendant acted with unlawful intent.82 Finally, unlike the UTSA—which only applies in cases of actual misappropriation—the EEA “prohibits both attempted trade secret theft and conspiracies to commit misappropriation.”83

Those convicted of unlawful trade secret misappropriation under the EEA face a potential jail sentence of ten years in cases of domestic theft, or fifteen years for foreign espionage, along with maximum fines of five million dollars.84 Meanwhile, an organization held in violation of the foreign espionage provision faces a fine of the greater of ten million dollars or three times the value of the misappropriated trade secret.85

3. Defend Trade Secrets Act

Finally, and most recently, Congress helped U.S. firms better protect their trade secrets through the passage of the DTSA in 2016.86 The DTSA was intended to foster “uniform standards for what constitutes trade secret theft,” while also empowering aggrieved organizations to file civil suits in federal court.87 Technically, the DTSA amended the EEA to add a new federal civil cause of action for the misappropriation of a trade secret.88 As with the EEA, the DTSA similarly tracks the definition of a trade secret employed by the UTSA. The DTSA requires the trade secret owner to take reasonable measures to maintain the secrecy of its information, and that the information have “economic value . . . from not being generally known.”89 Similarly, like the UTSA, the DTSA also defines misappropriation to include either (i) “the acquisition of a trade secret . . . by improper means,” or (ii) the “disclosure or use of a trade secret” acquired by improper means.90

Where the DTSA diverges from the UTSA—and, for that matter, the EEA—is with respect to its ex parte seizure provision. Specifically, the act provides that under “extraordinary circumstances, [courts may] issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret.”91 In addition, unlike the UTSA, the DTSA

---

83 Grow & Grow, supra note 61, at 1596; see 18 U.S.C. §§ 1831(a)(4)–(5), 1832(a)(4)–(5).
84 18 U.S.C. §§ 1831(a), 1832 (a).
85 Id. § 1831(b).
86 Id. § 1836.
87 Reuters, supra note 58.
88 Grow & Grow, supra note 61, at 1597.
89 18 U.S.C. § 1839(3).
90 Id. § 1839(5)(A)–(B).
91 Id. § 1836(b)(2)(A)(i).
also provides plaintiffs with access to the federal courts.92 Otherwise, the DTSA generally offers plaintiffs the same remedies that are available under the UTSA: injunctive relief and monetary damages.93

As will be seen in the next section, teams belonging to the four major U.S. professional sports leagues possess an array of information that would qualify for protection under the various federal and state protections for trade secrets.

III. POTENTIAL CYBER THREATS TO THE U.S. PROFESSIONAL TEAM SPORTS INDUSTRY

U.S. professional sports teams have typically been quick to adopt emerging new technology,94 acquiring everything from iPads95 to wearable devices capable of biometric tracking.96 Despite their teams’ increased reliance on these devices, however, the leagues themselves have been relatively slow to develop rules regulating their teams’ use—and, perhaps more importantly, potential manipulation—of these emerging technologies.97 Indeed, there are a variety of areas in which teams could potentially seek to obtain a competitive advantage over their rivals through the manipulation of commonly used technology.

95 See Stack, supra note 1.
97 See infra notes 148–177 and accompanying text.
A. Security of In-Game Technology

The greatest area of potential concern for professional sports leagues is likely to be ensuring the security of the technology relied on by teams while competing on the playing field itself during the course of a game. Like most other areas of commerce, sports teams have increasingly digitized their work environments, with players and coaches now relying on technology to perform a variety of tasks.

Perhaps most significantly, teams have increasingly utilized tablet computers to take the place of more traditional hard-copy versions of their playbooks.\(^98\) Digitized playbooks offer teams several potential advantages over paper copies. Digitized versions are quicker and easier to modify. They allow players immediate and constant access to their coaches’ latest strategic planning, and provide teams with a potential cost savings of as much as $100,000 per year in printing costs by dispensing with the need to reprint the playbooks on a daily or weekly basis.\(^99\) Digitized playbooks have also proven to be more secure than their hard-copy counterparts by not only enabling teams to utilize password protection but also allowing them to quickly erase a player’s team-issued tablet computer immediately upon his being traded to another franchise.\(^100\) At the same time, teams have used tablet computers to streamline other areas of communication with their players. For example, teams use the devices to disseminate practice schedules and departure times for road trips.\(^101\)

Although certainly convenient, teams’ increased reliance on tablets also poses a host of potential cybersecurity threats. Even if the potential nightmare scenario discussed in the introduction above—for example, an NFL team gaining access to its rival’s digitized playbook during the closing minutes of the Super Bowl—never emerges, teams could still gain any number of potential competitive advantages over their competitors by securing unauthorized access

\(^{98}\) See Gregory N. Hoole & Robert A. Bailey, The iPad and the Law, FED. LAW., May 2012, at 26 (reporting that “the Tampa Bay Buccaneers became the first NFL club to discontinue the use of paper copies of playbooks; instead the team distributed its playbook and videos to all its players in electronic format via an iPad”); see also Nicole Martinelli, iPad a Slam Dunk with NBA, CULT OF MAC (Apr. 7, 2011), https://www.cultofmac.com/89516/ipad-a-slam-dunk-with-nba/ [https://perma.cc/B3A9-98MT] (observing that “a number of NBA teams” are using iPads for everything “[f]rom playbooks to bus schedules”); Stack, supra note 1 (discussing NFL teams’ use of iPad playbooks).

\(^{99}\) See Ryan Faas, Why Most Teams Are Ditching Their Playbooks for iPads, CULT OF MAC (Sept. 5, 2012), https://www.cultofmac.com/188847/why-most-nfl-teams-are-ditching-their-playbooks-for-ipads-feature/ [https://perma.cc/C87G-U6E7] (noting that one NFL team reportedly spent over $100,000 per year printing over 100 copies of its playbook each week for its players and coaching staff).

\(^{100}\) See Joe Aimonetti, The iPad Has Revolutionized the NFL, CNET (July 18, 2012), https://www.cnet.com/news/the-ipad-has-revolutionized-the-nfl/ [https://perma.cc/4HKN-M6QM] (“iPads can be remotely erased, even before a player realizes he has been released or traded.”).

\(^{101}\) See Martinelli, supra note 98 (“Our whole calendar is mapped out [on the team-issued iPads]. Guys can know when buses are leaving, when planes are leaving.”) (quoting then-Washington Wizards assistant coach Ryan Saunders).
to their rivals’ tablet computers. Pre-game access to a competitor’s playbook, for instance, could provide invaluable insight into the opposition’s strategic game plan. Meanwhile, teams could secure a potential competitive advantage by manipulating other franchises’ digitized practice or travel schedules ahead of key matchups.

In addition to tablet computers, professional sports teams also rely on other potentially vulnerable technologies during the course of a game. In MLB, for example, teams are permitted to review a video replay before deciding whether to use their only opportunity to contest an umpire’s call on the field during a given game.102 These video signals could be used to interfere with the outcome of a game in several ways.

Recently, for instance, the potential manipulation of these video replays was thrust into the spotlight when reports emerged that both the Houston Astros and Boston Red Sox—the 2017 and 2018 World Series champions, respectively—had impermissibly used video replay feeds to decipher the signs used by the opposing team’s catcher to call each pitch.103 In the case of the Astros, players from the team then relayed this information to the batter at the plate in real time, via a series of whistles, claps, or banging of a trash can.104 Although the extent to which these schemes ultimately affected the outcome of the game on the field is unclear, they have nevertheless highlighted the potential impact that the manipulation of video replay systems can have on the integrity of the underlying competitions.105

Alternatively, in the future, because MLB teams must decide whether to challenge a call within thirty seconds from the end of the play, a team could potentially delay or otherwise interfere with a rival team’s video replay signal,

---

102 See Kenneth K. Kilbert, Instant Replay and Interlocutory Appeals, 69 BAYLOR L. REV. 267, 292 (2017) (explaining that in MLB “[e]ach team’s manager now gets one challenge per game; that is, he may initiate instant replay review on one reviewable play per game,” and that “if the manager’s challenge is successful and the play is overturned, the manager retains the ability to challenge one more play during the game, but in no event may the manager challenge more than two plays in a game”); see also A Guide to MLB’s New Expanded Replay Rules, CBS Chi. (Feb. 25, 2014), https://chicago.cbslocal.com/2014/02/25/a-guide-to-mlbs-new-expanded-replay-rules/ [https://perma.cc/XL39-D4Z9] (“A member of each team’s video staff can communicate his opinion of a call to his team’s dugout. Each team will have access to the same video feeds for review in any given ballpark. There will be a phone connecting the video room and dugout.”).


thereby providing the wrongdoer with a potentially critical competitive advantage.106 Similar concerns may also arise in the NFL, where teams sometimes rely on an assistant coach monitoring a video feed to decide whether to contest a particular call made on the field by a referee.107

B. Security of Shared Data

In addition to the technology relied on by teams’ playing and coaching staffs on the field during the course of a game, franchises in the four major U.S. professional sports leagues also rely on a plethora of shared data off the field in order to formulate strategies for upcoming games, make player personnel decisions, and analyze potential trades. Thus, preserving the accuracy and reliability of this data is of increasingly critical importance for the sports industry.

Perhaps most notably, the leagues recently began to employ new technology to capture detailed data regarding the events that transpire on the playing field. Specifically, through the use of intricate camera and sensor systems, teams can now track and record every event that occurs during the course of a game.108 MLB teams, for instance, implemented a system called StatCast that can not only record every movement a player makes on the field, but also track the flight of the baseball itself. Moreover, StatCast can also capture the velocity at which a ball is hit or tossed, as well as the number of times it rotates after being thrown by a pitcher.109 Similar systems are installed in NFL stadiums110

106 Manager Challenge, MAJOR LEAGUE BASEBALL, http://m.mlb.com/glossary/rules/manager-challenge [https://perma.cc/5GNR-HLE8] (“A manager has a 30-second time limit to inform the umpire (by verbal communication or hand signal) whether he wishes to use his manager challenge to invoke replay review, and the challenge may not be rescinded once it has been exercised.”).

107 See John Kelly, How NFL Review Rules Work, HOW STUFF WORKS, https://entertainment.howstuffworks.com/nfl-review-rules2.htm [https://perma.cc/9SYC-TYKQ] (noting that NFL coaches may “receive advice from an assistant coach in the booth who’s watching the network television feed”); see also Kilbert, supra note 102, at 287 (“[The NFL’s] current system allows each team’s coach to initiate instant replay review of two plays per game, with the potential of a third challenge if both of the earlier challenges are successful. Each challenge requires the team to use one of its timeouts. If a challenge is unsuccessful (i.e., the call on the field is not overturned), that team loses one of its timeouts. If a challenge is successful (i.e., the call on the field is overturned), the timeout is restored and no timeout is charged to that team.”) (footnotes omitted).

108 See Grow & Grow, supra note 61, at 1577.

and NBA arenas as well, with an analogous system scheduled to be implemented by the NHL in time for its 2020 playoffs. The data recorded by these systems is then typically shared among all of the leagues’ teams.

Teams are increasingly relying on the data produced by these systems to make a host of decisions. Most notably, the data produced by advanced tracking systems can be used to better assess a player’s physical abilities, data that not only helps inform a team’s decision on whether to acquire or trade a particular player but also how much money to offer the player during a salary negotiation. In addition, the data revealed by these systems can be used to help a team craft its in-game strategy, and allow clubs to pinpoint opposing players who may be moving a bit slower on the field in recent weeks, for instance.

As a result, sports teams could potentially obtain a competitive advantage by manipulating the tracking data that is captured by these systems. The precise mechanisms through which these data could be altered, and the extent to which they can be changed, will vary by league depending on the type of tracking systems used. Using MLB’s StatCast system as an example, it is theoretically possible that a team could seek to recalibrate the radar and high-speed cameras installed in their stadium in a way that would skew the resulting data. Because this radar and camera equipment is permanently installed in each team’s stadium, a team could presumably gain access to these devices relative-
ly easily whenever it desires. Alternatively, a team could theoretically manipulate this data by intercepting it before it is transmitted to the rest of the league, or by accessing the league-wide server on which it is centrally stored. Either way, the offending franchise would then be in a position to adjust the resulting data accordingly when using it internally, while leaving the rest of the league to unwittingly rely on skewed data.

In addition to the on-field tracking systems employed by the various leagues, the teams in each league are also increasingly sharing electronic medical records for their players in order to help facilitate trades and other player transactions. In MLB, for instance, the league maintains a central database into which teams record any medical treatment the clubs’ training staffs provide to their players—all the way “down to hot tubs, aspirin and anti-inflammatories.” Teams can then access the electronic medical records relating to an opposing team’s player during the final stages of discussion surrounding a proposed trade to assess the current physical condition of the potential trade target(s). Similar systems are currently utilized by the other leagues as well.

As with the on-field tracking systems discussed above, this shared medical data is also a potentially attractive target for manipulation by teams. Most obviously, some teams may be incentivized to underreport medical treatment provided to their own players in order to mitigate any potential concern from

---


118 See id. (“All MLB teams feed medical information into a central database known as the Sutton Medical System, designed to both maintain the privacy of individual players and to be accessible to teams when needed—such as when trades are made.”).

119 See Anne Zieger, NFL Uses eCW to Do Concussion Assessment, HEALTHCARE IT TODAY (July 29, 2013), https://www.healthcareitdtnow.com/2013/07/29/nfl-uses-ecw-to-do-concussion-assessment/ [https://perma.cc/YTP9-RDGR] (“Late last year, the NFL announced that it was using eClinicalWorks’ EMR to standardize their healthcare documentation for players. (Around the same time, the NBA announced that it was implementing Cerner’s EMR.”)).
their prospective trading partners. More nefariously, teams could even theoretically seek to modify the medical records relating to players on other teams. By fabricating additional, troubling entries in a particular player’s medical history, for example, a team could attempt to drive down trade interest in the player across the rest of the league, and thereby lower the price the offending team ultimately has to pay in order to acquire him. Alternatively, a team could even try to remove entries from an opposing player’s record in hopes of duping a rival into unwittingly acquiring an injured player.

C. Security of Proprietary Databases

In order to harness the increasingly large amounts of data that U.S. professional sports franchises are accumulating from the advanced tracking systems discussed above—and in an effort to centralize other, more traditional forms of data such as in-person scouting assessments and trade discussions with other teams—most teams have built their own internal, proprietary database systems to help inform their personnel and strategic decision-making processes. These databases represent a potential goldmine of information, as they document most of a team’s current internal thinking. By acquiring access to a rival franchise’s proprietary database, a team could thus discover a plethora of valuable information, including new methods of statistical analysis, the competitor’s trade strategies, and the players it is targeting in an upcoming draft.

Consequently, these internal, proprietary databases represent an extremely attractive target for potential cyber espionage. Indeed, in the professional sports industry’s most noteworthy cybersecurity breach to date, an executive from MLB’s St. Louis Cardinals accessed the proprietary database belonging to the rival Houston Astros—a system whimsically dubbed “Ground Control”—without authorization on a number of occasions throughout 2013 and

---

120 Indeed, MLB’s San Diego Padres were accused of underreporting medical treatment in 2016, as discussed in greater detail below. See infra notes 198–202 and accompanying text (discussing the incident).

121 See supra notes 108–114 and accompanying text (describing tracking systems).

122 See, e.g., John Niyo, Hail, Caesar! Tigers Finally Ready to Play Numbers Game, DETROIT NEWS (May 15, 2017), https://www.detroitnews.com/story/sports/columnists/john-niyo/2017/05/15/niyo-tigers-adapting-evolving-numbers-game/101736818/ [https://perma.cc/7AG9-6E8N] (reporting that MLB’s Detroit Tigers are developing a “new centralized data hub for the organization,” and quoting the team’s senior director of baseball analytics and operations as stating that “most—if not all—teams have a similar type of system now”).

2014. Although the subsequent sanctions issued in the case of the Cardinals “hacking”—as discussed in further detail below—will undoubtedly provide some deterrence against future breaches of this sort within MLB, these databases, given their value, are likely to remain an enticing cyber-target for some rival executives in what is often a particularly cut-throat industry.

D. Security of Biometric Tracking Devices

As noted above, professional sports franchises are increasingly utilizing wearable fitness-tracking devices to monitor their players in a variety of ways. Indeed, as one author recently noted, “[t]he use of biometric data in the sports industry is not new. Historically, teams have collected and used a wide variety of biometric and biomechanical measurements, including vertical jump, pitch speed, reaction time, heart rate, body composition, and self-reported wellness information.” Today, however, emerging technologies enable teams to monitor their players in ever more detailed—and potentially invasive—ways by allowing them to “measure the number of calories their players consume and burn in a given day, their heart rate during practice and games, and even the amount and quality of their sleep each night.” At the same time, other new devices—such as MotusTHROW—let teams monitor their players physiologically in real-time during practices or games and detect the stress level that players are placing on various joints and tendons.

---

125 See infra notes 179–187 and accompanying text.
126 See WEBROOT, DENVER BRONCOS MAINTAINS COMPETITIVE EDGE WITH WEBROOT SECURE ANYWHERE BUSINESS - ENDPOINT PROTECTION 1 (2016), https://www.webroot.com/shared/pdf/case-study-broncos.pdf [https://perma.cc/VKW3-EMCG] (“In today’s highly competitive sports environment, a team’s information can be a key competitive advantage, both on the field and in their business operations.”).
127 See supra note 96 and accompanying text.
128 Barbara Osborne, Legal and Ethical Implications of Athletes’ Biometric Data Collection in Professional Sport, 28 MARQ. SPORTS L. REV. 37, 37 (2017).
129 Grow & Grow, supra note 61, at 1578; see also Osborne, supra note 128, at 41–45 (listing biometric data collection devices currently in use in the professional sports industry); Rachel Arrison, Note, “You’re Wearing That?”: Why Data Generated from Wearable Technology Should Be Protected Under Privacy Law, 26 SPORTS LAW. J. 211, 213–14 (2019) (discussing the sensitive nature of data collected by wearable biometric trackers).
130 See MotusTHROW, MOTUS GLOBAL, https://motusglobal.com/motusbaseball.html [https://perma.cc/EC5F-5TCX] (describing MotusTHROW as a wearable device that “records biomechanical data from every throw made in practice and games” to “increase your arm’s fitness in a safe manner” and “determine[] optimal throwing levels that go beyond age-old pitch counts and inning totals”).
131 See Nicholas Zych, Collection and Ownership of Minor League Athlete Activity Biometric Data by Major League Baseball Franchises, 14 DePaul J. SPORTS L. 129, 133–34 (2018) (“More advanced and costly Wearables, such as Whoop Strap and the Catapult Sensor (‘Catapult’), have made a splash in the professional sports market while remaining relatively small in the public market. . . . These Wearables gather information regarding body strain, recovery, and sleep analytics.”).
collection and use of such forms of biometric data is only expected to grow in the future.\footnote{See Joe Cioli, Goldman Sachs: There’s a Fortune to Be Made Analyzing Sports Stats, BUS. INSIDER (July 13, 2017), http://www.businessinsider.com/goldman-sachs-sports-economy-analytics-statistics-2017-7 [https://perma.cc/7D8G-CWCV] (“[T]eams across sports at all levels are increasingly using GPS trackers, accelerometers, biometric sensors and advanced optical player tracking.”).}

Although much of the resulting data collected from these IoT devices is likely to be stored on the proprietary team databases discussed above,\footnote{See supra notes 121–126 and accompanying text.} the biometric collection devices themselves represent a potential source of cybersecurity risk. By gaining unauthorized access to wearable devices used by the players on an opposing team, a franchise could potentially gain valuable information about its opponent’s players ahead of a key game. Knowing how well an opposing team’s players slept the night before, for instance, could allow a club to find a potential point of attack by repeatedly challenging an individual who got less than the ideal amount of rest ahead of the game. Similarly, data regarding the stress levels that various players’ joints had incurred during recent practices could yield insight into which opposing players may be nursing an injury, and thus might be unable to perform at his or her highest level.

\textbf{E. Gambling-Related Concerns}

Finally, another area in which cybersecurity threats may endanger the integrity of a league’s games is the emerging sports gambling marketplace. Following the U.S. Supreme Court’s 2018 decision in \textit{Murphy v. National Collegiate Athletic Association}\footnote{Murphy v. Nat’l Collegiate Athletic Ass’n, 138 S. Ct. 1461 (2018).}—in which the Court struck down the Professional and Amateur Sports Protection Act (PASPA),\footnote{See 28 U.S.C. §§ 3701–3704 (2018). The PASPA created “a ban on state-sponsored sports gambling nationwide” but “exempt[ed] Nevada and at least eight other states from its scope via a perpetual grandfathering clause.” Ryan M. Rodenberg & John T. Holden, \textit{Sports Betting Has an Equal Sovereignty Problem}, 67 DUKE L.J. ONLINE 1, 1–2 (2017), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1024&context=dlj_online [https://perma.cc/D5GJ-XAAR].} and thereby cleared the way for the legalization of sports gambling at the state-level—a number of new municipalities are expected to legalize gambling on professional sporting events in the coming years.\footnote{See Mark Brnovich, \textit{Betting on Federalism: Murphy v. NCAA and the Future of Sports Gambling}, 2018 CATO SUP. CT. REV. 247, 247 (“Sports gambling is a big business already, and it will likely grow bigger still after Murphy.”).}

Legalized gambling could trigger a number of cybersecurity-related concerns for professional sports leagues. With the advent of more widespread sports betting, leagues will need to invest resources to detect the potential fix-
ing of matches.137 These efforts, in turn, will need to be protected against potential unauthorized intrusions into the computer systems being utilized to help the leagues detect unusual betting activity. Similarly, with the leagues pushing for laws requiring betting houses to use official league-sanctioned statistics for their sports gambling outcomes,138 these efforts create the possibility that the leagues’ official statistics could themselves become the subject of a cyber intrusion.139 Indeed, even slight alterations of the official league records regarding the outcomes on the playing field—such as the number of yards a running back rushed for in a particular football game—could yield significant profits for unscrupulous bettors.

At the same time, leagues may also find it necessary to monitor for unauthorized betting-related activity occurring within their own stadiums. In professional tennis, for instance, the men’s and women’s professional tours have been forced to monitor and ban the so-called practice of “courtsiding,” in which an audience member attempts to obtain a potentially critical informational advantage by using wireless communications technology to convey the results of a particular play to his or her betting associates.140 By obtaining immediate notifications regarding the results of a play, these associates may be able to quickly place a bet on the results of the already completed play before the outcome is transmitted via television broadcast and the betting market is officially closed.141

---

137 Cf. Patrick Doughty, *Pound for Pound: A Legal Analysis of the Gambling, Alcohol, and Taxation Issues the NFL Must Weigh as It Expands to London*, 22 Jeffrey S. Moorad Sports L.J. 593, 598–99 (2015) (“The leagues asserted legalized gambling would lead fans, whether rightly or wrongly, to believe the games were being played with less integrity, such as a perceived increase in match-fixing between officials and players.”); see also Adam Kilgore, *For Sports Leagues, Legalized Sports Betting Offers New Risks, and Massive Rewards*, WASH. POST (May 14, 2018), https://www.washingtonpost.com/sports/for-sports-leagues-legalized-sports-betting-offers-new-risks-and-massive-rewards/2018/05/14/5ce4caf4-5790-11e8-858f-72ebcb4d6067_story.html?utm_term=.f1eb24a5a6a [https://perma.cc/M6WM-7LYH] (observing that for professional sports leagues, legalized sports gambling “creates . . . the need for oversight”).


141 See id.
The same potential informational advantages are likely to materialize in the emerging betting markets relating to the four major U.S. professional sports leagues. Getting even a few seconds of advanced notice of the outcome of a critical fourth-down play in a professional football game, for instance, could enable a bettor to place a more accurate wager on the eventual outcome of the game. Deterring this sort of behavior within a team’s stadium is likely to require the implementation of various network-related cybersecurity protections, along with more traditional forms of visual detection.

IV. LEAGUES’ CURRENT FRAMEWORK FOR CYBER-RISK MANAGEMENT

Although the trade secret protections outlined above in Part II.B putative-apply to the U.S. professional sports industry, in reality teams are unlikely to directly rely on these laws to enforce their rights against their league rivals. Indeed, “[u]nder each league’s constitution . . . teams are generally prohibited from suing each other, or one another’s employees, in court. Instead, any dispute between rival franchises and/or their employees is generally subject to arbitration before their respective league commissioner.”¹⁴² This reality makes the formulation and enforcement of league-wide policies governing trade secrets and cybersecurity all the more critical.

Unfortunately, despite the multitude of potential cybersecurity threats afflicting U.S. professional sports teams, the four major leagues appear to have been relatively slow to address these possible vulnerabilities with specific league-wide rules or regulations. Although each of the four leagues was unwilling to share any substantive details regarding its current cybersecurity policies,¹⁴³ MLB reportedly relied on its teams to protect themselves from cyber intrusions, rather than impose any league-wide cybersecurity requirements on its franchises, as recently as 2015.¹⁴⁴ Consequently, although the industry has only experienced one publicized competition-related cybersecurity breach to date—the “hacking” of the Houston Astros’ database by their MLB rival St.

¹⁴² Grow & Grow, supra note 61, at 1617–18.
¹⁴³ Specifically, MLB responded to an inquiry by stating that the league currently maintains a league-wide cybersecurity policy that applies to both the league office and all clubs, but was unwilling to share any additional details regarding the policy. See Email from Michael Teevan, Vice President, Comm’ns, Major League Baseball, to authors (Jan. 3, 2019, 11:12 EST) (on file with authors). Meanwhile, the NFL, NBA, and NHL either failed to respond to inquiries or declined to provide any information at all regarding their policies. See, e.g., Email from Tim Frank, Senior Vice President, Basketball Comm’ns, Nat’l Basketball Assoc., to authors (Jan. 2, 2019, 16:35 EST) (on file with authors).
¹⁴⁴ Shaikin, supra note 5 (explaining that teams in the MLB are responsible for handling their own cybersecurity, though MLB experts are available for consultation). As noted above, today MLB maintains a league-wide cybersecurity policy that applies to both the league office and all clubs. See Email from Michael Teevan, supra note 143.
Louis Cardinals, mentioned above—\textsuperscript{145} it is impossible to know whether other teams have simply failed to identify similar breaches to their own systems. In fact, the aforementioned Astros breach was only detected after the Cardinals’ employee responsible for the intrusion leaked a number of Houston’s internal team documents to the sports website Deadspin in 2014.\textsuperscript{146}

This makes the formulation of league-wide rules regulating cybersecurity all the more important. Unfortunately, although general provisions contained in the various league constitutions and bylaws could be used to penalize intra-league cybersecurity violations, it is not clear that the existing penalty structures in place sufficiently deter this sort of activity.\textsuperscript{147} Indeed, prior cases in which leagues have punished teams for electronic-device-related breaches are likely to serve as key precedents, and thus limit the potential range of punishment options available to leagues in these cases.

\textit{A. Existing Applicable League Rules}

Although no league currently appears to have a rule in place directly regulating cybersecurity breaches among their franchises, other, more generalized prohibitions could be used by the leagues to address future cyber intrusions.

1. Major League Baseball

Under the MLB Constitution,\textsuperscript{148} the league commissioner—currently Rob Manfred\textsuperscript{149}—is generally empowered to investigate and punish “any act, transaction or practice charged, alleged or suspected to be not in the best interests of the national game of [b]aseball.”\textsuperscript{150} Should the commissioner determine that a team, or one of its officials or employees, have committed such an act not in the best interest of the sport, he may then assess one or more of a list of predetermined punishments on the offending club or person. Specifically, under

\textsuperscript{145} See supra notes 124–125 and accompanying text.

\textsuperscript{146} See Barry Petchesky, \textit{Leaked: 10 Months of the Houston Astros’ Internal Trade Talks, Deadspin} (June 30, 2014), http://deadspin.com/leaked-10-months-of-the-houston-astros-internal-trade-1597951970 [https://perma.cc/9SM4-HNQF] (“Documents purportedly taken from Ground Control and showing 10 months’ worth of the Astros’ internal trade chatter have been posted online at . . . a site where users can anonymously share hacked or leaked information.”).

\textsuperscript{147} Of course, existing federal and state laws may provide additional deterrence.


\textsuperscript{149} See Rob Manfred, Commissioner of Major League Baseball, MAJOR LEAGUE BASEBALL, https://www.mlb.com/official-information/executives/rob-manfred [https://perma.cc/XZ5L-3EYR].

\textsuperscript{150} MLB CONST., supra note 148, at art. II § 2(b); see also Matthew B. Pachman, \textit{Limits on the Discretionary Powers of Professional Sports Commissioners: A Historical and Legal Analysis of Issues Raised by the Pete Rose Controversy}, 76 VA. L. REV. 1409, 1420–30 (1990) (discussing the scope of this so-called “best interests of baseball” power).
the existing league constitution, any fine issued by the commissioner is “not to exceed $2,000,000 in the case of a Major League Club, [and] not to exceed $500,000 in the case of an owner, officer or employee.”\footnote{MLB CONST., supra note 148, at art. II § 3(a).} In addition, the commissioner may also suspend or remove the offending person from the league, withhold any other benefit afforded to the team or official under “the Major League Rules, including but not limited to the denial or transfer of player selection rights” in the MLB draft, or impose any “such other [punitive] actions as the Commissioner may deem appropriate.”\footnote{Id.}

In addition to this catch-all provision in the league constitution, MLB has also enacted a specific policy relating to the use of “Cell Phones and Electronic Devices In and Around [the] Clubhouse and On-field.”\footnote{Major League Baseball, Cell Phones and Electronic Devices in and Around Clubhouse and On-Field (on file with author).} This policy generally prohibits teams from using “electronic equipment or devices . . . for the purpose of stealing signs or conveying other information designed to give a [c]lub a competitive advantage,” while specifically prohibiting the use of “any type of walkie-talkies, mobile phones, ‘smart watches’ (e.g., Apple watches), laptop computers, tablets or other communication devices, in or near the dugout, in the bullpens or on the playing field” before or during a game.\footnote{Id.} Violations of the policy “will subject both the [c]lub and offending individual to discipline by the Commissioner’s Office.”\footnote{Id.}

2. National Football League

As with MLB, the NFL Constitution and Bylaws also endow Roger Goodell, the league’s current commissioner, with relatively broad authority to investigate and punish any “conduct detrimental to the welfare of the [l]eague or professional football.”\footnote{NFL CONST., supra note 156, at art. VIII § 8.13(A).} Specifically, under Article VIII of the NFL Constitution, “the Commissioner shall have complete authority to,” among other potential penalties, “[s]uspend and/or fine” any person or team guilty of conduct detrimental to the league “in an amount not in excess of five hundred thousand dollars ($500,000).”\footnote{NFL CONST., supra note 156, at art. VIII § 8.13.} In addition, the Commissioner may “award selection choices and/or deprive the offending club of a selection choice or choices” in

\footnote{Id.}
the NFL Draft.\textsuperscript{158} Meanwhile, in cases where the Commissioner determines that the penalties above are “not adequate or sufficient, considering the nature and gravity of the offense involved, he may refer the matter to the [NFL’s] Executive Committee,” and recommend any other potential punishment “he deems appropriate.”\textsuperscript{159}

As with MLB, the NFL league rules also contain some specific provisions regarding the on-field use of electronic devices. Under Article IX of the NFL Constitution, teams are prohibited from using “any communications or information gathering equipment, other than Polaroid-type cameras or field telephones, including without limitation videotape machines, telephone tapping or bugging devices, or any other form of electronic device that might aid a team” during the course of a game.\textsuperscript{160} Meanwhile, aside from “[l]eague-issued Microsoft Surface tablets,” the league has enacted a specific Electronic Device Rule, which generally prohibits “the use of cellular phones, smart phones, tablet devices, computers, wearable electronic devices such as Google Glass, and other electronic equipment by coaches, players, and other club personnel” in any “club-controlled areas including, but not limited to, sidelines and coaches’ booths,” from “ninety (90) minutes prior to kickoff through the end of the game, including halftime.”\textsuperscript{161}

Finally, with respect to the league authorized tablet computers, NFL rules specifically prohibit teams from modifying their computers’ hardware or software in any manner that might provide them with a competitive advantage.\textsuperscript{162} Moreover, should a team’s tablet computers malfunction prior to the start of a game, league rules provide that the opposing team must also refrain from using its own devices until such time that both teams’ computers are in full working order.\textsuperscript{163} Importantly, however, if a team’s devices should malfunction after the game has begun, then the opposing team is not required to cease using its own

\textsuperscript{158}Id.
\textsuperscript{159}Id.
\textsuperscript{160}Id. at art. IX § 9.1(C)(14).
\textsuperscript{162}See NFL Equity Rule, NAT’L FOOTBALL LEAGUE, https://operations.nfl.com/the-rules/nfl-equity-rule/ [https://perma.cc/D7JL-8HJE] (“The tablets, set up and maintained by league-employed purple hat technicians on game day, are configured so that clubs can’t modify them to gain an unfair competitive advantage. Attempts to alter tablet hardware or software without league approval are prohibited.”).
\textsuperscript{163}See id. (“If sideline or booth devices are not working properly at kickoff, the opposing team is limited to using only as many operational devices as the affected team has. For example, if one team has seven working devices in the bench area at kickoff, the other team is limited to using seven devices in its bench area. When the malfunctioning devices are restored, both teams can resume using all of their devices.”).
devices.164 This rule creates a potential incentive for teams to manipulate one another’s tablets after kickoff.

Moreover, in addition to the above limitations relating to the use of electronic devices, the NFL has also formulated a specific policy relating to social media usage by players, coaches, and team personnel.165 Under the policy, players, coaches, and other football operations personnel are prohibited from using social media from ninety minutes before kickoff until after the traditional post-game media interviews.166

3. National Basketball Association

Similar to his counterparts in MLB and the NFL, the commissioner of the NBA—currently Adam Silver167—is likewise granted broad discretion to adjudicate “matters that may adversely affect the Association or its Members.”168 In cases in which a team employee has been found “guilty of conduct prejudicial or detrimental to the Association,” the commissioner is empowered to “suspend [the individual] for a definite or indefinite period, [and/or] to impose a fine not exceeding $1,000,000.”169 Meanwhile, a specific provision in the league constitution governs cases in which confidential or non-public team or league information is disclosed for gambling-related purposes.170 In these cases, the punishment for the disclosure of any “information concerning the medical, personal, or other condition of any Player, Coach, or Referee; any Player transaction; any disciplinary action taken or to be taken by the Association or a Team; and Referee schedules, assignments, statistics, and ratings,” is placed “within the absolute and sole discretion of the Commissioner and may include a fine, suspension, expulsion and/or perpetual disqualification from further association with the Association or any of its Members.”171

---

164 See id. (“The equity rule no longer applies once the tablet systems are fully functional for both clubs, or once the game has started with full functionality.”).
166 Id.
169 NBA CONST., supra note 168, at art. 35A § (d).
170 See id. at art. 35A § (g)(ii-iv).
171 Id.
Moreover, as with the NFL, the NBA has also formulated a specific policy relating to social media usage by players, coaches, and team personnel. Under the policy:

[T]he use of cell phones, PDAs and other electronic communications devices—and thus accessing Twitter, Facebook and similar social media sites—is now prohibited during games for players, coaches and other team personnel involved in the game. The league has defined “during games” as the period of time beginning 45 minutes before the opening tip and ending “after the postgame locker room is open to the media and coaches and players have first fulfilled their obligation to be available to media attending the game.”

This policy thus has the secondary effect of limiting team officials’ use of electronic devices for more potentially nefarious purposes.

4. National Hockey League

Finally, the NHL Constitution similarly grants the league commissioner, Gary Bettman, the power to resolve matters involving activity “that in the opinion of the Commissioner is detrimental to the best interests of the League or professional hockey.” As with the other leagues, in such cases the commissioner has the “full and complete authority to discipline” offending individuals through expulsion or suspension with fines not to exceed one million dollars, or in cases “affect[ing] the competitive aspects of the game, by awarding or transferring players and/or draft choices and/or depriving the offending Member Club of draft choices.”

Similar to the NFL and NBA, the NHL has also enacted a social-media policy, under which team executives are prohibited from using social media “beginning at 11 a.m. on the day of the game and ending after post-game me-

---


175 Id. at art. VI § 6.3(j)(1).
dia obligations,” with players’ usage similarly curtailed “beginning two (2) hours prior to the opening face-off and ending upon cessation of post-game media obligations.” Any violations of the policy are punishable via a monetary fine.

B. League Disciplinary Precedents

Although the authority granted to the commissioner of each league to investigate and punish activity not in the best interest of the league’s respective sport would seemingly give these individuals the power necessary to handle cybersecurity-related violations, in reality their discretion is more limited. When exerting their authority under their respective league constitution, commissioners will typically impose a punishment only after considering the extent to which parties have been penalized for wrongdoing in prior analogous cases. Consequently, the existence of relevant prior precedent may constrain the leagues’ ability to punish cybersecurity violations between teams.

1. Major League Baseball

MLB has dealt with several disciplinary cases in recent years that would likely serve as precedent for a potential cybersecurity-related infraction in the future. The most notable of these cases is, of course, the aforementioned “hacking” incident involving the Houston Astros and St. Louis Cardinals. Specifically, throughout the 2013 and 2014 seasons, former Cardinals’ executive Christopher Correa illegally accessed the Astros’ internal computer network and proprietary database. Correa was able to access the Astros’ system by using the old password of a former Cardinals’ employee who had gone on to work for Houston. The Astros eventually detected the unauthorized access...
after internal team documents were leaked to the website Deadspin in 2014.182

Correa was ultimately prosecuted and—after pleading guilty to five criminal charges—sentenced by a federal judge to forty-six months imprisonment and ordered to pay over $279,000 in restitution.184 MLB then elected to issue its own punishment in the case, with Commissioner Rob Manfred placing Correa on the league’s “permanently ineligible list,” which effectively banned him from the sport for life.185 In addition, Manfred decided that the Cardinals franchise itself was “liable for the misconduct” of its former employee, and stripped St. Louis of its first two picks in the 2017 MLB Draft and awarded them to the Astros.186 Manfred also fined the Cardinals two million dollars—the highest amount then allowed under the league constitution—and ordered the team to send the money to Houston as restitution.187 Thus, the Cardinals-Astros affair sets a clear precedent for future cases of cyber-espionage involving MLB franchises.

Meanwhile, in 2017, MLB investigated two separate incidents in which team employees were alleged to have engaged in the unauthorized use of electronic devices during the course of a game. The first incident arose after a series between the Boston Red Sox and New York Yankees, during which the Yankees believed Red Sox officials were improperly using an Apple Watch in the dugout to help steal New York’s signs.188 During the ensuing league investigation, Boston reportedly admitted that a member of its coaching staff had

---

182 See Petchesky, supra note 146 (discussing the leak of ten months’ worth of the Houston Astros’ internal trade discussions and the information contained therein).


184 Associated Press, supra note 123.

185 Goold, supra note 181 (“The commissioner placed Correa, who is serving a 46-month sentence in federal prison, on the permanently ineligible list, effective immediately. That is the same list that includes others banned from baseball like Pete Rose and infamous members of the 1919 White Sox.”).

186 Id.

187 See id. (discussing the punishment Manfred levied on the Cardinals).

188 See Michael S. Schmidt, Boston Red Sox Used Apple Watches to Steal Signs Against Yankees, N.Y. TIMES (Sept. 5, 2017), https://www.nytimes.com/2017/09/05/sports/baseball/boston-red-sox-stealing-signs-yankees.html?smid=tw-nytsports&smtyp=cur&r=0 [https://perma.cc/NUV3-8T7A] (“The Yankees, who had long been suspicious of the Red Sox’ stealing catchers’ signs in Fenway Park, contended the video showed a member of the Red Sox training staff looking at his Apple Watch in the dugout. The trainer then relayed a message to other players in the dugout, who, in turn, would signal teammates on the field about the type of pitch that was about to be thrown, according to the people familiar with the case.”).
improperly used an electronic device in the dugout. Due to the team’s candor, MLB limited the punishment to a rather insubstantial monetary fine. Nevertheless, MLB warned that future incidents along these lines would face much harsher sanction, including the loss of draft picks.

Several weeks later, the unauthorized use of an Apple Watch was once again in the news when Arizona Diamondbacks coach Ariel Prieto was spotted wearing the device in the dugout during a playoff game against the Colorado Rockies. MLB’s subsequent investigation later determined that Prieto had worn the watch inadvertently, and that it had not been used for any “baseball-related communication.” Both Prieto and the Diamondbacks, however, were fined an unspecified amount due to their violation of the league’s electronic device policy.

Most recently, MLB announced in January 2020 that it was levying several punishments against the Houston Astros for the team’s aforementioned sign-stealing scheme. Specifically, the league suspended both the team’s general manager, Jeff Luhnow, and its field manager, A.J. Hinch, for the 2020 season. (Both Luhnow and Hinch were subsequently fired by the Astros for their involvement in the scheme.) The team also lost both its first- and second-round draft picks in the 2020 and 2021 drafts, and was ordered to pay a five million dollar fine.

Finally, MLB was confronted with a case of alleged data manipulation by one of its clubs during the 2016 season. That summer, the San Diego Padres completed two mid-season trades—one with the Boston Red Sox and the other with the Miami Marlins—in which the club traded away pitchers who received medical treatment from the team’s training staff for various issues with their pitching arms. Neither the Red Sox nor the Marlins were informed about the


190 See id. (“MLB did make it clear to all teams that any similar future transgressions will be handled more harshly and will involve picks.”).


192 Id.

193 See id.

194 See infra notes 103–105 and accompanying text.


196 Id.

197 Id.

198 See Olney, supra note 117 (discussing the incidents).
medical treatment ahead of the trade, and both complained to MLB that San Diego failed to disclose this relevant information.199

A league investigation ultimately revealed that the Padres maintained two sets of medical records, one for internal use and the other to be shared with other MLB teams via the electronic-medical-records database discussed above.200 Although Padres officials insisted that they never intended to deceive anyone, the league nevertheless suspended the team’s general manager, A.J. Preller, for thirty days for his involvement in the incident.201 In addition, MLB helped broker an agreement between the Marlins and Padres under which the teams agreed to return some of the players they exchanged in the trade.202

2. National Football League

As with MLB, several prior incidents in the NFL also serve as potential precedents for any future cybersecurity-related disciplinary cases. First, in 2006, Jim Mora, the then-head coach of the Atlanta Falcons, was caught using his cell phone on the sidelines during a late-season game against the Tampa Bay Buccaneers.203 Afterward, Mora explained that he was using the phone to call a team official to determine how a tie would affect his team’s playoff status.204 Nevertheless, the unauthorized usage violated Article IX of the NFL Constitution, which prohibits the use of “any communications or information

199 See id. (noting teams “were enraged by what they perceived to be strategic deception: veiling medical information that could have been pivotal in trade discussions”).

200 See Hattery, supra note 109, at 268 (“[T]he Padres had compiled two sets of health records, one set to be disclosed in trade negotiations and one set to remain under confidential control of the team.”); see also supra notes 116–118 and accompanying text (describing MLB’s electronic-medical-records system).


202 See Olney, supra note 117 (noting that after the Padres traded pitchers Colin Rea and Andrew Cashner to Miami, “MLB executives [later] facilitated the return of Rea to the Padres, with San Diego returning pitcher Luis Castillo to Miami”).


204 See id. (“Victories by the Cowboys and Redskins earlier that day meant that an Atlanta loss would eliminate the Falcons from the NFC playoff race, but Mora was unsure if they could remain in contention by tying Tampa Bay. He used a cell phone in an attempt to contact team officials and seek clarification on Atlanta’s status.”).
The Sport of Cybersecurity

gathering equipment . . . that might aid a team” during the course of a game.205 As a result, Mora was fined $25,000 by the league.206

Perhaps more notable, however, is the punishment the NFL doled out in response to the so-called “Spygate” affair in 2007.207 Specifically, during a game between the New England Patriots and the New York Jets, league security officials confiscated a video camera used by the Patriots’ video assistant Matt Estrella while standing on the team’s sideline.208 The NFL’s subsequent investigation concluded that Estrella was using the camera to record the signals used by the Jets’ coaches to relay play calls to their players on the field. This constituted a violation of the league rule prohibiting the use of video-recording devices during the course of a game.209

Commissioner Roger Goodell ultimately punished New England rather harshly, in no small part due to the fact that the NFL specifically warned teams about the unauthorized use of video cameras on the sidelines a little over a year before the incident after learning of earlier alleged video-camera-related infractions by the Patriots.210 Specifically, Goodell fined Patriots head coach Bill Belichick $500,000—the maximum allowable amount under the league constitution—along with a $250,000 fine for the team itself.211 In addition, Goodell stripped the team of its first-round pick in the 2008 NFL Draft.212 Thus, the punishment issued in the Spygate incident likely serves as the most relevant precedent for future cases in which an NFL team gains a competitive

---

205 NFL CONST., supra note 156, at art. IX § 9.1(C)(14).
206 See NFL Hits Mora with $25K Fine, supra note 203 (“Atlanta Falcons coach Jim Mora was contrite after the NFL fined him $25,000 for using a cell phone on the sidelines during an overtime loss at Tampa Bay two weeks ago.”).
208 See Alexander F. Tilton, Comment, Mayer v. Belichick: “Spygate” Scandal Is Not the Court’s Concern, 18 SPORTS LAW. J. 341, 341 (2011) (“League security personnel confiscated a video camera and videotape from the Patriots’ employee after he allegedly focused the camera on Jets’ coaches while they were using signals to communicate with the players on the field.”).
209 See Samuel J. Horovitz, If You Ain’t Cheating You Ain’t Trying: “Spygate” and the Legal Implications of Trying Too Hard, 17 TEX. INTELL. PROP. L.J. 305, 307 (2009) (“A subsequent investigation determined that the Patriots had violated league rules by videotaping the Jets coaches sending signals to players during the game.”).
210 See id. (reporting that a “warning memo” circulated by the NFL in 2006 “was believed to have been prompted in part by suspicions of similar past videotaping violations by the Patriots”).
211 See Belichick Draws $500,000 Fine, but Avoids Suspension, ESPN (Sept. 13, 2007), https://www.espn.com/nfl/news/story?id=3018338 [https://perma.cc/Q94X-VN48] (“New England Patriots coach Bill Belichick was fined the NFL maximum of $500,000 Thursday and the Patriots were ordered to pay $250,000 for spying on an opponent’s defensive signals.”).
212 See id. (“Commissioner Roger Goodell also ordered the team to give up its first-round draft choice next year if it reaches the playoffs this season, or its second- and third-round picks if it misses the postseason.”).
advantage over one of its rivals through the use of unauthorized electronic devices on the field.

V. POLICY IMPLICATIONS

This final Part explores the policy implications of the cybersecurity risks described in Part III, and the governance gaps revealed in Part IV. First, we lay out a theoretical lens through which to view next steps in enhancing the cybersecurity practices of professional sports leagues with a focus on the literature of polycentric governance. Next, we offer suggestions for how the sports leagues could better protect themselves from the existing competition-related cybersecurity threats. Finally, we highlight the potential role that government—potentially both domestically (at the federal and state levels) and internationally—may play in helping to secure the integrity of the leagues and their games.

A. What We Can Learn from Using the Lens of Norm Entrepreneurs and Polycentric Governance

One of the ways to consider the regulation of U.S. professional sports leagues generally, and the issue of cybersecurity in particular, is the dynamic field of polycentric governance—championed by numerous scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom—in which multiple stakeholders “negotiate rules and policies to solve common problems.” This multidisciplinary approach has demonstrated the benefits of self-organization and networking regulations “at multiple scales.” It can, under certain circumstances, enhance “flexibility across issues and adaptability over time,” and can hasten the uptake of best practices that could generate

---

213 See infra notes 216–231 and accompanying text.
214 See infra notes 232–249 and accompanying text.
215 See infra notes 250–271 and accompanying text.
216 See Michael D. McGinnis, An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework, 39 POL’Y STUD. J. 169, 171–72 (2011) (defining polycentricity as “a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes”).
218 Elinor Ostrom, A Polycentric Approach for Coping with Climate Change, 15 ANNALS ECON. & FIN. 97, 97 (2014).
positive network effects and result in the emergence of a norm cascade toward
the Security of Things in professional sports.\textsuperscript{220}

The field of polycentric governance seems well suited to addressing the
issues raised in this Article for at least two reasons. First, as has been noted
here and elsewhere, the legal environment of U.S. professional sports leagues
is fragmented, with the federal and state governments historically taking a
hands-off approach to regulation in favor of the leagues managing their own
conduct.\textsuperscript{221} There are some exceptions to this general rule, such as in the case
of stadiums being public facilities and their resulting classification as critical
infrastructure by the U.S. Department of Homeland Security.\textsuperscript{222} Nevertheless,
the fact that multiple stakeholders—discussed further below—are collaborat-
ing in governance at multiple levels highlights the links with polycentricity.

Second, given the polycentric nature of the professional sports industry,
Professor Elinor Ostrom’s design principles for institutional analysis are perti-
nent and can provide insights to franchise owners, players, and fans.\textsuperscript{223} These
include the importance of: (1) “clearly defined boundaries for the user pool . . .
and the resource domain”;\textsuperscript{224} (2) “[p]roportional equivalence between benefits
and costs”;\textsuperscript{225} (3) “[c]ollective choice arrangements ensur[ing] that the
resource users participate in setting . . . rules”;\textsuperscript{226} (4) “monitoring . . . by the ap-
propriators or by their agents”;\textsuperscript{227} (5) “[g]raduated sanctions” for rule viola-
tors;\textsuperscript{228} (6) “[c]onflict resolution mechanisms [that] are readily available, low
cost, and legitimate”;\textsuperscript{229} (7) “[m]inimal recognition of rights to organize”;\textsuperscript{230}

\begin{footnotesize}
\begin{footnotes}
\item[220] See Martha Finnemore & Kathryn Sikkink, \textit{International Norm Dynamics and Political
Change}, 52 INT’L ORG. 887, 895–98 (1998) (discussing the point at which norms begin to cascade
through a society).
\item[221] See, e.g., Nathaniel Grow, \textit{Regulating Professional Sports Leagues}, 72 WASH. & LEE L. REV.
573, 580–81 (2015) (observing that “[f]ederal antitrust law is the primary legal authority regulating
the operation of professional sports leagues in the United States,” but noting that “despite society’s
reliance on the Sherman Act to regulate the professional sports industry, antitrust law has failed to
effectively govern the monopoly sports leagues”).
\item[222] See \textit{Commercial Facilities Sector}, supra note 35.
\item[223] See generally SCOTT J. SHACKELFORD, \textit{MANAGING CYBER ATTACKS IN INTERNATIONAL
\item[225] Elinor Ostrom, \textit{Polycentric Systems: Multilevel Governance Involving a Diversity of Organi-
zations, in GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES IN-
volving a Diversity of Organizations} 105, 118 tbl. 5.3 (Eric Brousseau et al. eds., 2012) (citing
ELINOR OSTROM, \textit{GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE
ACTION} 90 (1990)).
\item[226] BUCK, supra note 224, at 32.
\item[227] Id.
\item[228] Id.
\item[229] Id.
\item[230] Ostrom, supra note 225, at 118 tbl. 5.3.
\end{footnotes}
\end{footnotesize}
and (8) “governance activities [being] . . . organized in multiple layers of nested enterprises.”

Not all of Professor Ostrom’s design principles are applicable in this context, given that cybersecurity is more of a public good than a common pool resource, but some do have salience, especially depending on the level of analysis undertaken. For example, they speak to the importance of having clear rules setting out escalating penalties for teams engaging in nefarious cybersecurity practices, and a robust monitoring and conflict resolution regime to ensure compliance to cybersecurity policies as is further discussed below. Other insights include the importance of setting adequate boundary conditions, the need for proportionality, ensuring a robust role for civil society (including fans and journalists), and effective monitoring. These insights are applied and further unpacked in the following sections.

**B. Proposing an Updated Cybersecurity Policy for U.S. Professional Sports Leagues**

As is apparent from the foregoing discussion, protecting trade secrets, fans, and players from the array of cybersecurity threats faced by U.S. professional sports leagues is a multi-faceted and dynamic problem. As such, this Article asserts that leagues should take the lead in improving their cybersecurity and data privacy standards for franchises and fans. To date, rather than deal with cybersecurity issues in a proactive way, the four major U.S. sports leagues have unfortunately instead largely elected to adopt a reactive posture, choosing to deal with cyber breaches on an ad hoc basis once they are discovered. For instance, rather than establishing league-wide cybersecurity best practices for their teams, leagues generally defer to their franchises to protect themselves from cyber intrusions. Cases like the aforementioned hacking of MLB’s Houston Astros by the St. Louis Cardinals, however, highlight the need for more comprehensive, league-wide policies.

In all, we argue that five steps are warranted to help better secure the professional sports leagues surveyed against the array of cyber threats they face. First, in an effort to put the principles of polycentric governance into practice, we argue that governance should happen at the level most appropriate to the envisioned harm. As such, any shared, league-wide systems necessitate league-wide policies that the franchise owners would help fashion in order to ensure that cybersecurity best practices are deployed to help manage in-stadium player tracking technology, injury-reporting databases, and gambling-detection.

---

231 Id.
232 See Shaikin, supra note 5 (citing an unnamed MLB official who stated that MLB teams are responsible for addressing their own cybersecurity needs).
233 See supra notes 179–187 and accompanying text.
mechanisms. Such collaboration should be hastened by leveraging the new Sports ISAO discussed above.\textsuperscript{234} Moreover, this step echoes the third Ostrom design principle that good governance should take the form of defined user pools (e.g., professional sports franchises) practicing “[c]ollective choice arrangements” that ensure “that the resource users participate in setting . . . rules.”\textsuperscript{235}

Second, although individual teams should continue to improve their own cybersecurity due diligence, best practices should be more easily shared through the Sports ISAO to ensure that the teams are implementing baseline cybersecurity standards such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework.\textsuperscript{236} A working group relating to the European Union’s recent General Data Protection Regulation (GDPR) should also be established by the Sports ISAO to further this cause, and at the same time assist in the international expansion plans for U.S. professional sports leagues.\textsuperscript{237} The leagues could also go further and establish a joint Security Operations Center (SOC) similar to that created by the financial sector to help improve the cybersecurity standards of its constituents.\textsuperscript{238}

Third, again building off of the Ostrom design principles discussed above relating to the importance of graduated sanctions,\textsuperscript{239} we recommend that league rules be formulated for data breaches with escalating penalties depending on the nature of the infraction, while also taking into consideration that a breach between two teams has ramifications for the entire league.\textsuperscript{240} These best

\textsuperscript{234} See supra notes 4, 64 and accompanying text.

\textsuperscript{235} BUCK, supra note 224, at 32.

\textsuperscript{236} See Shaikin, supra note 5 (reporting on the extent to which individual teams are responsible for their own cybersecurity). For an overview of the NIST Cybersecurity Framework, see NAT’L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/L3YV-MREJ].

\textsuperscript{237} See infra note 267 and accompanying text (discussing the leagues’ varied plans to expand their operations to Europe).


\textsuperscript{239} See BUCK, supra note 224, at 32.

\textsuperscript{240} For instance, although the punishment that MLB handed down in the Astros-Cardinals case appeared to assume that Houston was the sole victim of the breach, the Cardinals’ unauthorized intrusion allowed the club to gain additional knowledge that gave it a potential informational advantage over everyone in the league, arguably warranting more severe punishment than the league doled out. Cf. Tom Verducci, Lax Hack Smack: MLB, Rob Manfred Let Cardinals Off Easy in Hacking Scandal, SPORTS ILLUSTRATED (Jan. 30, 2017), https://www.si.com/mlb/2017/01/30/cardinals-astros-hacking-chris-correa [https://perma.cc/HQ89-FQYY] (arguing that the punishment the Cardinals received as a result of the hacking incident was light considering the circumstances). Indeed, the Cardinals’ breach
practices should incorporate, to the extent possible, GDPR standards discussed further below, such as establishing a 72-hour data breach notification window along with the right of data portability and heightened consent requirements, especially for sensitive data. We note that, in some cases, the formulation of new, sufficiently punitive league rules may require amending the respective league’s constitution to provide for higher maximum fine amounts to help incentivize the uptake of these best practices.\(^{241}\)

Fourth, it is imperative for the leagues to work to protect the biometric data they collect via tracking devices, and to help ensure that players are protecting their own data responsibly. To accomplish these feats, the leagues should establish mandatory (and regularly audited) cybersecurity hygiene programs that include penetration testing and anti-phishing initiatives. Further, the leagues should proactively implement cybersecurity best practices related to IoT security, such as requiring NIST Cybersecurity Framework compliance from vendors and suppliers.\(^{242}\) To this end, the leagues could take the affirmative step of launching a bug-bounty competition of the kind that many private and public-sector organizations—including Microsoft and the Department of Homeland Security—have already announced, to help shore up vulnerabilities.\(^{243}\)

Fifth and finally, we recommend that leagues consider moving to an independent arbitration system for cybersecurity-related disputes, rather than relying on the league commissioner to serve as arbitrator in these cases.\(^{244}\) Indeed, arbitration-by-commissioner has previously resulted in allegations of bias, with many fans believing that a particular league’s commissioner was predisposed to rule in favor of a team with a particularly influential owner, because these owners will, to a large extent, determine whether the league will ultimately elect to renew the commissioner’s contract.\(^{245}\) This, again, implicates an

...
Ostrom design principle—low-cost, effective dispute resolution. We further recommend that the findings of these arbitral panels be made available throughout the leagues to help build precedent and fill in cybersecurity governance gaps that are still apparent in the existing frameworks.

It should be noted that, in some cases, these issues may require leagues to reach agreement with their applicable players’ union. As discussed above, several existing cyber threats—including the use of biometric-tracking devices and the storage of electronic medical records—directly implicate data relating to, and collected from, players. Consequently, any new league policies in these areas will likely have to be subjected to union approval via the collective-bargaining process. Indeed, both MLB’s and the NBA’s most recent collective bargaining agreements specifically discuss the permissible use of biometric-tracking devices on the playing field. The players’ amenability to reach agreement with the leagues on these matters is uncertain, as in some cases players are independently seeking to monetize their biometric data themselves. Nevertheless, given the potential ramifications of a cyber breach in this area, leagues should make a concerted effort to reach an agreement with the players and their unions on these matters.

C. A Potential Government Solution for U.S. Professional Sports Leagues’ Cybersecurity Risks

Should owners fail to develop sufficient cybersecurity policies independently, it is possible that government may eventually consider stepping in to fill the void. This could take the form of the federal government taking steps to protect teams’ trade secrets, along with their stadiums and practice facilities, as was described in Part I. Such steps are politically difficult, given the long history of Congressional resistance to ‘comprehensive’ cybersecurity reform and coaches, the expediency of the NFL’s investigation” into the aforementioned Spygate scandal “seemed dubious,” given Commissioner Roger Goodell’s relationship with New England Patriots’ owner Robert Kraft).

246 See BUCK, supra note 224, at 32.

247 See Jay Moyer, The Law of Sports, 79 COLUM. L. REV. 1590, 1593 (1979) (reviewing JOHN C. WEISTART & CYM H. LOWELL, THE LAW OF SPORTS (1979)) (observing that “virtually all player-related practices within a sports league, including the so-called player restraints, are terms and conditions of employment and are therefore mandatory subjects of collective bargaining”).

248 See Darren Rovell, MLB Approves Device to Measure Biometrics of Players, ESPN (Mar. 6, 2017), https://www.espn.com/mlb/story/_/id/18835843/mlb-approves-field-biometric-monitoring-device [https://perma.cc/M7LU-Z6R6] (noting that MLB “approved the use of a continuous biometric monitor that can be worn by players during games” and that “[t]he NBA’s new collective bargaining agreement allows players to wear biometric monitors, but only during practice”).

249 See Rhett Jones, NFL Players Strike a Deal to Sell Their Biometric Data, Gizmodo (Apr. 24, 2017), https://gizmodo.com/nfl-players-strike-a-deal-to-sell-their-biometric-data-1794616994 [https://perma.cc/P2A8-UZWT] (reporting that fitness wearables manufacturer Whoop “struck a deal with the NFL Players Association . . . that will make it possible for players to sell their health data”).
efforts—as the history of the Cybersecurity Act of 2012 can attest—as well as the federal government’s general reluctance to regulate the sports industry. Nevertheless, a high-profile incident—such as a cyberattack on a major sporting event such as the Super Bowl or either the Olympics or World Cup, both of which the United States will host in the 2020s—could change the political calculus.

Perhaps more likely, then, is that teams may inadvertently be swept up by other, more general cybersecurity regulations enacted at the federal or state levels. For example, as with its groundbreaking 2002 privacy law that ushered in the first data-breach notification standards—an idea that has since been copied by the other forty-nine states—California’s 2018 Consumer Privacy Act is helping to set a new standard for U.S. privacy protections. Given the number of teams operating in the state, California’s new law thus has potentially significant ramifications for the U.S. professional sports industry. Although it does not go quite as far as the EU’s GDPR, it does include provisions that allow consumers to sue over data breaches, and decide when, and how, their data is being gathered and used by companies like Facebook and Google. Although there remains debate about the scope and effectiveness of this intervention, the law may well help shape the cybersecurity practices of professional sports


251 Cf. Grow, supra note 221, at 580–81 (observing that antitrust laws regulate U.S. professional sports leagues but do so ineffectively).


leagues in California, such as by requiring added efforts to protect the privacy rights of players and fans. An accounting of state-level cybersecurity laws as of July 2018 is included in Table 1.

Table 1: Status of State-Level Cybersecurity Laws

<table>
<thead>
<tr>
<th>Type of State Law</th>
<th>Coverage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking, Unauthorized Access, Computer Trespass, Viruses, Malware</td>
<td>All 50 States</td>
<td>All fifty states have enacted laws that generally prohibit actions that interfere with computers, systems, programs, or networks.</td>
</tr>
<tr>
<td>Data Breach Notification Laws</td>
<td>All 50 States</td>
<td>A total of twenty-three states and Guam have enacted laws targeting phishing schemes. Many other states have laws concerning deceptive practices or identity theft that may also apply to phishing crimes.</td>
</tr>
<tr>
<td>Anti-Phishing Laws</td>
<td>23 States: Alabama, Arkansas, Arizona, California, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia and Washington, as well as Guam</td>
<td></td>
</tr>
</tbody>
</table>

257 These data have been compiled from Computer Crime Statutes, NAT’L CONF. OF ST. LEGISLA- TURES (June 14, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/ computer-hacking-and-unauthorized-access-laws.aspx#Hacking [https://perma.cc/MKJ7-FNU2]. It should also be noted that, in addition to these laws, twelve states maintain “data security laws,” eight of which include a requirement for firms to implement “reasonable” cybersecurity practices. See id. One example is Indiana, where “[a] data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.” IND. CODE 24-4.9-3-3.5(c) (2018). For more on this topic, see JEFF KOSSEFF, CYBERSECURITY LAW 42–43 (2017). At least thirty-one states also boast data disposal laws that regulate when and how data is destroyed, including the use of “reasonable measures” to ensure that these data are “unreadable or undecipherable.” Id. at 49. Special thanks to Tristen Waite for her help in compiling these data.
| **Anti-Spyware Laws** | 20 States: Alaska, Arizona, Arkansas, California, Georgia, Hawaii, Illinois, Indiana, Iowa, Louisiana, Nevada, New Hampshire, New York, Pennsylvania, Rhode Island, Texas, Utah, Virginia, Washington, and Wyoming, as well as Guam, and Puerto Rico | Currently five states have statutes that address ransomware, or computer extortion; however, other state laws prohibiting malware and computer trespass may be used to prosecute these crimes as well. |
| **Anti-Ransomware Laws/Computer Extortion Laws** | 5 States: California, Connecticut, Michigan, Texas, and Wyoming |  |

Two regulatory trends are also relevant to discuss with regards to the cybersecurity of U.S. professional sports leagues: active defense and international cybersecurity standards. First is the current debate—referenced above[^258]—to allow organizations to engage in active defense measures, up to and including

[^258]: See supra notes 45–54 and accompanying text.
‘hacking back,’ if their intellectual property has been compromised. Although this idea has long been a relatively fringe concept, it is getting more mainstream attention, even rising to the level of being included in the 2016 Republican National Committee (RNC) platform.259 As noted above, according to the Department of Justice, this practice is “likely illegal” under the CFAA at the federal level,260 as well as at the state level as illustrated in Table 1. Nevertheless, there are efforts currently at the federal and state levels to change the status quo. Specifically, the Active Cyber Defense Certainty (ACDC) Act would permit organizations to operate beyond their network perimeter, including the potential to conduct surveillance on entities “who are thought to have done hacking in the past or who, according to a tip or some other intelligence, are planning an attack.”261 The bill also clarifies “the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network.”262 In particular, it specifies that people facing criminal charges under the CFAA for illegal hacking can defend themselves by claiming that their activities were “active cyber defense measures.”263 If passed, this could permit teams to “hack back” at opposing teams or other entities that compromise their networks. Similarly, Georgia’s State Bill 315, which passed in May 2018, permitted “active defense measures that are designed to prevent or detect unauthorized computer access” until Governor Nathan Deal vetoed the bill due to its “national security implications and other potential ramifications.”264

Such measures could have particular salience in the U.S. professional sports industry. Because executives often frequently move between franchises in a particular league,265 teams may worry that their former employees will wrongly take their former club’s intellectual property to their new employer. This was the stated motivation behind the former St. Louis Cardinals’ executive’s hacking into the Houston Astros’ computer system in 2013 and 2014, for

259 See Paul Szoldra, This One Sentence in the GOP Platform Has Cybersecurity Experts Freaking Out, BUS. INSIDER (July 21, 2016), http://www.businessinsider.com/gop-platform-hacking-back-2016-7?pundits_only=0&get_all_comments=1&no_reply_filter=1 [https://perma.cc/PQ5C-5JFH].
261 Schmidle, supra note 50.
263 Id.
265 Cf. Grow & Grow, supra note 61, at 1610 (observing that due to the fact that “the potential universe of qualified applicants for many of the vacancies that a sports team may need to fill can often be quite small” teams depend on outside hiring to find qualified “coaches, scouts, or front office personnel”).
instance.266 Should such active defense measures be legalized at the state or federal level, sports teams may seek to utilize these protections in order to defend their intellectual property from perceived infringement. This possibility further highlights the need for leagues to adopt proactive measures regulating their teams in this regard.

Second, as U.S. professional sports leagues look to expand their operations abroad,267 they should be cognizant of new regulatory requirements, particularly in the EU. Indeed, these laws have already been called a “game changer” for European sports leagues.268 Generally, GDPR is an expansive regulatory regime with a wide array of requirements on covered firms, ranging from ensuring data portability and consent to mandating that firms disclose a data breach within seventy-two hours of becoming aware of the incident and conduct a post mortem to ensure that it will not recur.269 GDPR is particularly relevant to professional sports leagues due to its provisions regarding data portability. Under GDPR, players, staff, fans, and volunteers may now be allowed to request their data, and have it deleted, while franchises may have to transfer proprietary data regarding their former players to their new team following a trade.270 Although a full accounting of the potential implications of GDPR for the U.S. professional sports industry is beyond the scope of this article, the bottom line is that U.S.-based leagues considering expansion oppor-

---


270 See Keane, supra note 268.
tunities to Europe need to put into place GDPR security and privacy requirements like many U.S. firms are already doing, lest they run the risk of running afoul of GDPR penalties, which can range up to four percent of an organization’s total global revenue.\footnote{See Michelle Drolet, GDPR Fines: How Much Will Non-Compliance Cost You?, CSO (Oct. 23, 2017), https://www.csoonline.com/article/3234685/data-protection/gdpr-fines-how-much-will-non-compliance-cost-you.html [https://perma.cc/7GNS-GWX3].}

CONCLUSION

There is a long history of U.S. professional sports leagues rallying to ensure the integrity of their respective games from threats as diverse as illegal gambling to doping. So far, though, as this Article has shown, these same leagues do not appear to be doing enough to protect their franchises, players, and fans from the array of cyber threats threatening the integrity of their games. Moving forward, a polycentric approach that includes franchise owners, players unions, and federal and state-level policymakers is essential to hasten the uptake of baseline cybersecurity standards and to eventually get ahead of the curve by taking steps such as implementing GDPR requirements globally. These measures are essential to protect the sports and players we love from abuses, both online and offline, a topic that that is now more important and more timely than ever as the Internet of Everything expands.