

Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 13 | Issue 2


Article 9

5-1-2019

On the Clock, Best Bet to Draft Cyberdefensive Linemen: Federal Regulation of Sports Betting from a Cybersecurity Perspective

William H. Williams

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/bjcfcl>

 Part of the [Computer Law Commons](#), [Entertainment, Arts, and Sports Law Commons](#), [Gaming Law Commons](#), [Internet Law Commons](#), and the [Other Law Commons](#)

Recommended Citation

William H. Williams, *On the Clock, Best Bet to Draft Cyberdefensive Linemen: Federal Regulation of Sports Betting from a Cybersecurity Perspective*, 13 Brook. J. Corp. Fin. & Com. L. 539 (2019).

Available at: <https://brooklynworks.brooklaw.edu/bjcfcl/vol13/iss2/9>

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of Corporate, Financial & Commercial Law by an authorized editor of BrooklynWorks.

ON THE CLOCK, BEST BET TO DRAFT CYBERDEFENSIVE LINEMEN: FEDERAL REGULATION OF SPORTS BETTING FROM A CYBERSECURITY PERSPECTIVE

ABSTRACT

*On May 14, 2018, Justice Alito delivered the majority opinion for the United States Supreme Court in *Murphy v. National Collegiate Athletic Association (NCAA)*. The Professional and Amateur Protection Act (PASPA), a twenty-six-year-old federal statute, was deemed unconstitutional; thus, this decision allows state legislatures to legalize sports betting within their borders. With many states independently legalizing sports gambling, the regulatory landscape throughout the country is becoming a patchwork of state statutes. Additionally, top tier sporting organizations heavily depend on data analytics to formulate game plan strategy, train efficiently, rehab player injuries, gauge team and player performance, etc. The popularity of sports gambling continues to grow in the United States, and the proliferation of data usage will only expand as teams and players seek a competitive advantage. However, sports teams and athletes are not the only entities seeking an edge, as hackers will attempt to steal private and proprietary data for a significant edge when placing sports bets. It is imperative that leagues, teams, sports betting operators, and legislators must not overlook the cybersecurity component when regulating the industry. This Note argues that federal regulatory oversight is the most favorable approach from a cybersecurity perspective, and states can build on this framework as they see fit. Federal agencies, such as the Federal Trade Commission (FTC), Securities Exchange Commission (SEC), and federal law enforcement agencies, are well-versed in persistent cybersecurity issues and compliance regulations. A central, federal regulatory model is advantageous to the growth and integrity of the blossoming sports gambling industry and the established sports industry.*

INTRODUCTION

"I am sensitive to arguments in favor of deferring to the States, and I believe that the Federal Government should be careful to preempt state authority only when an issue is of national importance. But, based on what I know about the dangers of sports betting, I contend that its dangers are of national importance. Such dangers and the interstate effects of sports betting justify this Federal action."

- Bill Bradley, National Basketball Association (NBA) Hall-of-Famer & former United States Senator for New Jersey¹

1. *Post-PASPA: An Examination of Sports Betting in America Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. on the Judiciary*, 115th

The highly anticipated United States Supreme Court decision, *Murphy v. National Collegiate Athletic Association*, struck down the Professional and Amateur Protection Act of 1992 (PASPA).² This signaled a “win” for federalism and those entities clamoring for their piece of the proverbial pie in an expanding legalized sports gambling landscape.³ In its decision, the Court relied on the Tenth Amendment and its anti-commandeering doctrine. As Justice Alito wrote for the majority, “Our job is to interpret the law Congress has enacted and decide whether it is consistent with the Constitution. PASPA is not. PASPA ‘regulate[s] state governments’ regulation’ of interstate commerce. The Constitution gives Congress no such power.”⁴ The entire statute was deemed unconstitutional, rather than severing and salvaging parts of the statute, as Justice Ginsberg advocated for in her dissent.⁵ Ultimately, Justice Alito stated for the majority, “legalization of sports gambling requires an important policy choice, but the choice is not ours to make. Congress can regulate sports gambling directly, but if it elects not to do so, each State is free to act on its own.”⁶ This 6-3 decision allows individual states to legalize and regulate sports betting within their borders.⁷ Since the *Murphy* decision, several states swiftly acted to legalize sports betting.⁸ Additionally, New York and Arkansas recently passed a bill opening the door to legalizing sports betting with plans to operate legal sports books in the future.⁹

Congr. 1–2 (2018) (statement of Jocelyn Moore, Executive Vice President, Communications and Public Affairs, National Football League) <https://republicans-judiciary.house.gov/wp-content/uploads/2018/06/NFL-Statement-House-Judiciary-Post-PASPA-Hearing-Sept.-27-2018.pdf> (quoting Bill Bradley during the 1992 Senate debate of the PASPA bill) [hereinafter *Moore, Post-PASPA*].

2. See *Murphy v. Nat’l Collegiate Athletic Ass’n*, 138 S. Ct. 1461, 1485 (2018).

3. See Sam Kamin, *Murphy v. NCAA: It’s about much more than gambling on sport*, THE HILL (May 15, 2018, 8:00 AM), <https://thehill.com/opinion/judiciary/387653-murphy-v-ncaa-its-about-much-more-than-gambling-on-sports>.

4. *Murphy*, 138 S. Ct. at 1485 (quoting *New York v. United States*, 505 U.S. 144, 166 (1992)).

5. See *id.* at 1489–90 (Ginsburg, J., dissenting that, “When a statute reveals a constitutional flaw the Court ordinarily engages in a salvage rather than a demolition operation . . . The Court wields an ax to cut down § 3702 instead of using a scalpel to trim the statute . . . Deleting the alleged ‘commandeering’ direction would free the statute to accomplish just what Congress legitimately sought to achieve: stopping sports gambling regimes while making it clear that the stoppage is attributable to federal, not state, action.”).

6. *Id.* at 1484–85.

7. See Craig A. Newman, *Cybercrime Meets Insider Trading in Sports*, N.Y. TIMES (July 6, 2018), <https://www.nytimes.com/2018/07/06/business/dealbook/sports-betting-cybercrime.html>.

8. See Ryan Rodenberg, *State-by-State Sports Betting Bill Tracker*, ESPN (Feb. 24, 2019), http://www.espn.com/chalk/story/_/id/19740480/gambling-sports-betting-bill-tracker-all-50-states (reporting that as of February 24, 2019, these states include Delaware, New Jersey, Mississippi, West Virginia, New Mexico, Pennsylvania, and Rhode Island, joining Nevada, Oregon, and Montana, which already have grandfathered exemptions under PASPA. This list has been updated multiple times over the course of writing this Note, as the industry continues to expand to additional states).

9. See *id.*

The economic environment, where the likes of New Jersey fought for the overturning of PASPA, had individual states clamoring for new sources of revenue despite a thriving national economy.¹⁰ Despite unemployment figures at a seventeen-year low and stock markets flourishing for most of 2018, state governments are still tapping into “rainy-day funds” and relying on “one-time gimmicks.”¹¹ In 2017, twenty-seven states did not realize their revenue expectations and quick fixes were no longer available.¹² However, since New Jersey sports books became operational in June 2018, the New Jersey Division of Gaming Enforcement released sports wagering revenue results of \$40,449,676 from June through September 2018, with \$23,961,038 coming from September alone.¹³ With an influx of revenue on the minds of state legislators, as many as twenty-two additional states as well as Washington, D.C., have introduced bills seeking to legalize sports betting.¹⁴ With the seemingly vast profitability, it will only be a matter of time before many of the remaining states explore legalization. However, there are pitfalls to rapidly scaling an industry, such as protecting the entities and data from formidable cyberincendiaries.

On September 27, 2018, the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations held a hearing titled, “Post PASPA: An Examination of Sports Betting in America.” Subcommittee Chairman Jim Sensenbrenner (R-WI) laid out three options for ‘post-Murphy,’ “including: (1) reenact a federal ban on sports betting by prohibiting corporations (and not states) from engaging in sports betting activities; (2) have Congress defer to the states and allow states to legalize and regulate the business; or (3) have Congress adopt uniform minimum standards to provide guidance to states that choose to legalize.”¹⁵ This Note will argue that the scope of data and cyber protection of sports franchises’ information necessitates federal intervention to complement state policies and regulations. Sports franchises and leagues, State Gaming Commissions,

10. See The Data Team, *Despite a strong economy, American states are desperate for revenue*, THE ECONOMIST (Apr. 6, 2018), <https://www.economist.com/graphic-detail/2018/04/06/despite-a-strong-economy-american-states-are-desperate-for-revenue>.

11. See *id.*

12. See *id.* (according to the National Association of State Budget Officers).

13. See Press Release from Gurbir S. Grewal, Attorney General, DGE Announces September 2018 Total Gaming Revenue Results, New Jersey Department of Law & Public Safety (Oct. 12, 2018), available at <https://www.nj.gov/oag/ge/docs/Financials/PressRel2018/September2018.pdf> (signifying September revenue results—\$23,961,038 up from \$16,487,491 from the previous three months combined—are more indicative of anticipated revenue as online sports gambling has launched and more sportsbooks are available. This September boom is likely increased by the commencement of the 2018 American football seasons.).

14. See Rodenberg, *supra* note 8 (noting that 17 states are considered to be in the ‘moving toward legalization’ category).

15. Laurie McKay, Mark A. Clayton, & Edward R. Winkofsky, *Post PASPA: An Examination of Sports Betting in America*, GREENBERG TRAURIG, LLP ALERT: GAMING (Sept. 28, 2018), <https://www.gtlaw.com/en/insights/2018/9/post-paspa-an-examination-of-sports-betting-in-america>.

and state governments are not sufficiently equipped to protect against cybercriminals, especially as the internet plays a significant role in the growing legalized sports gambling industry.

This Note will explore and offer suggestions to resolve regulatory issues facing the sports and sports betting industries within the scope of cybersecurity. Part I provides an overview of sports data analytics and its increasing value to leagues, teams, and players. Part II discusses the various categories of data in sports, while Part III explores notable cyberattacks in the sporting landscape. Part IV reviews the state of cybersecurity measures and the role of the Federal Trade Commission (FTC) in consumer protection from unfair and deceptive practices. Part V compares the issue of sports betting to the securities market and the lessons to be gleaned from the Securities and Exchange Commission's (SEC) approach to outsider trading liability. Lastly, Part VI addresses the arguments for state regulation of sports betting and the shortcomings of state regulation due to the development of the internet and heavy reliance on data.

I. THE EXPLOSION OF VALUABLE SPORTS DATA

While the legalized sports betting industry is nascent, data analytics are undeniably ubiquitous with professional and amateur sports, namely Division I collegiate athletics. The "Big Data" revolution has arrived and "increasingly large datasets are being mined for important and often surprising insights."¹⁶ Complex statistics and sabermetrics¹⁷ have inundated sports fans in the search for objective knowledge about sports.¹⁸ The Oakland Athletics' success and the release of *Moneyball*¹⁹ propelled a new view of statistical methods and sports strategy into the minds of front office executives.²⁰ The tremendous volume of data gathered and analyzed by teams across the sporting landscape is a sophisticated effort to gain a

16. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 393 (2014).

17. Sabermetrics strives to quantify athletes' (originally baseball players') performances "based on objective statistical measurements, especially in opposition to many of the established statistics that give less accurate approximations of individual efficacy." Rob Neyer, *Sabermetrics*, ENCYCLOPEDIA BRITANNICA, <https://www.britannica.com/sports/sabermetrics> (last visited Mar. 3, 2019). For some of the earliest famed sabermetric authors like Pete Palmer and Bill James, "sabermetrics centered around understanding, around reconciling the differences between what they saw on the field and how those within baseball said the game was played and won." Jack Moore, *How Wall Street Strangled the Life Out of Sabermetrics*, VICE SPORTS (Oct. 22, 2014, 8:30 AM), https://sports.vice.com/en_us/article/aem895/how-wall-street-strangled-the-life-out-of-sabermetrics.

18. See Newman, *supra* note 7.

19. See Lara Grow & Nathaniel Grow, *Protecting Big Data in the Big Leagues: Trade Secrets in Professional Sports*, 74 WASH & LEE L. REV. 1567, 1575 (2017) (explaining that Michael Lewis' 2003 best-selling book, *Moneyball: The Art of Winning an Unfair Game*, highlighted the successfully utilized statistical methods of Major League Baseball general manager Billy Beane of the Oakland Athletics).

20. See Newman, *supra* note 7.

competitive edge over opponents.²¹ Sports teams analyze and store non-public information such as medical records, the extent of an injury, game plans, internal communications, individual player performance metrics, and biometric monitoring device data.²²

Traditionally, sports organizations' proprietary data has been shielded from other organizations through trade secret laws, such as the Uniform Trade Secrets Act (USTA), the Economic Espionage Act (EEA), and the Defend Trade Secrecy Act (DTSA).²³ Principally, "a trade secret is legally protected as long as its owner takes reasonable efforts, under the circumstances, to protect the secret."²⁴ Thus, if the secret is reasonably protected, the law "provides a remedy against a third party who misappropriates that secret, such as by hacking into a server or hiring a competitor's employee to learn the secret."²⁵ The value of sports franchises' proprietary information was on display in June 2015, when the Federal Bureau of Investigation (FBI) uncovered, after a yearlong investigation, that St. Louis Cardinals' scouting director Christopher Correa illegally hacked into the internal computer network of the Houston Astros.²⁶ Correa gained access to the Astros' scouting system, known as Ground Control, "in order to view the team's proprietary information (including Houston's player scouting reports and statistical analyses, in addition to the leaked trade-discussion notes)."²⁷ This case²⁸ underscored the explosion of "computer-driven analytics in baseball and other sports" as well as the increasingly vital importance of proprietary data to professional teams in the industry.²⁹ Correa pled guilty to five criminal counts of unauthorized access of a protected computer, resulting in 46 months in prison and a court order to

21. See Grow & Grow, *supra* note 19, at 1577–78.

22. Biometric monitoring data includes sleep patterns, heart rate, body composition, nutrition levels, etc. See Zachary Zaggar, *Sports Teams Must Tackle Hacking Risk Amid Legal Gambling*, LAW360 (Sept. 24, 2018), <https://www.law360.com/articles/1085391/sports-teams-must-tackle-hacking-risk-amid-legal-gambling>.

23. See Grow & Grow, *supra* note 19, at 1583.

24. ROGER ALLAN FORD, *Trade Secrets and Information Security in the Age of Sports Analytics*, in THE OXFORD HANDBOOK OF AMERICAN SPORTS LAW 491, 500–01 (Michael McCann ed., 2018) (defining, generally, reasonable efforts as "teams should use strong encryption, limit information access to employees with legitimate needs, use strong passwords and two-factor authentication, log accesses, even keep especially sensitive information under physical lock and key. Having employee policies that prohibit disclosure and requiring employees to sign nondisclosure agreements likewise helps show that a team takes reasonable steps to maintain secrecy.").

25. *Id.* at 500.

26. See Tyler Kepner, *Former Cardinals Executive Pleads Guilty to Hacking Astros*, N.Y. TIMES (Jan. 8, 2016), <https://www.nytimes.com/2016/01/09/sports/baseball/former-cardinals-executive-christopher-correa-pleads-guilty-to-hacking-astros.html?module=inline>.

27. Grow & Grow, *supra* note 19, at 1580.

28. Plea Agreement, *United States v. Christopher Correa*, No. H-15-679 (S.D. Tex. Jan. 8, 2016) (describing the charges to which Correa pled guilty and the punishment resulting).

29. Kepner, *supra* note 26.

pay \$279,038 in restitution.³⁰ The severity of this sentence underscored the importance of the stolen data and highlighted the need for sports organizations “to take measures to secure and legally protect their most valuable and sensitive information.”³¹

With the advent of legalized sports gambling in states and the value of proprietary sports data, many industry members are deeply concerned about cyberthreats of hackers looking to gain an edge in sports wagering using non-public data.³² The integrity of the sports betting industry is at stake as well as the integrity of the sports themselves.³³ In both instances, fans of the sport and those wagering on the sport place a considerable onus on legitimate, untampered competition, and those within the industry exclaim their “commitment to upholding integrity across all facets of a legal, regulated sports betting market.”³⁴ Compromised athlete privacy, extortion, and money laundering are all problems that can accompany sports betting when hackers unlawfully obtain nonpublic information to profit from directly or sell to others.³⁵ The substantial amounts of money and participants soon to be associated with sports gambling activities create the potential of an emerging “black market for data” utilized for sports betting.³⁶ There is genuine concern in the “potential for technology-facilitated mischief of all types.”³⁷ Although difficult to calculate, illegal sports betting in the United States is estimated to fall between \$150 billion to \$400 billion annually.³⁸ The sports analytics market is anticipated to reach \$3.87 billion by 2022, an expected growth of 40.1% over six years.³⁹ Teams are going to continue generating outrageous amounts of data. This value and proliferation of data in sports provides “an opportunity for sophisticated cybercriminals, who will inevitably seek to hack into confidential sports information and use it to their advantage in placing legal

30. See Associated Press, *Christopher Correa, Former Cardinals Executive, Sentenced to Four Years for Hacking Astros' Database*, N.Y. TIMES (July 18, 2016), <https://www.nytimes.com/2016/07/19/sports/baseball/christopher-correa-a-former-cardinals-executive-sentenced-to-four-years-for-hacking-astros-database.html>.

31. Grow & Grow, *supra* note 19, at 1580.

32. See Newman, *supra* note 7.

33. See Zagger, *supra* note 22.

34. Hilary Russ, *First sports betting integrity group launched in United States*, REUTERS (Nov. 27, 2018), <https://www.reuters.com/article/us-usa-gambling-sports/first-sports-betting-integrity-group-launched-in-united-states-idUSKCN1NW2MS>.

35. See Newman, *supra* note 7; see also Zagger, *supra* note 22.

36. Zagger, *supra* note 22.

37. *Id.* (expressing the views of Edward J. McAndrew, co-leader of the privacy and data security practice group at Ballard Spahr LLP).

38. See Newman, *supra* note 7.

39. See Business Wire, *Worldwide Sports Analytics Market 2016-2022: Market to Grow by Over 40% to an Aggregate of \$3.97 Billion- Research and Markets*, BUSINESS WIRE, Jan. 12, 2017, 9:24 AM, <https://www.businesswire.com/news/home/20170112005616/en/Worldwide-Sports-Analytics-Market-2016-2022-Market-Grow>.

sports bets. It is where cybercrime will no doubt meet insider trading in sports.”⁴⁰

II. SPORTS ANALYTICS DATA CATEGORIES

Professional sports have always used statistical data⁴¹ to measure athlete performance and compare players. Currently, there are four categories of sports data: (1) statistical data, (2) proprietary team analytics data, (3) biometric data, and (4) medical and player injury data.

A. STATISTICAL DATA

Major League Baseball (MLB) has been a pioneer in sports statistics because of its early inception and the nature of the sport.⁴² There is an inherent “one-on-one matchup between a batter and a pitcher[,]” which results in either the success of the batter or the success of the pitcher.⁴³ In contrast, the other major sports in the United States (basketball, football, and hockey) did not initially lend themselves to the proliferation of statistics because “the performance of any one player on any particular play hinges to a great extent not only on the performance of the player in question, but also his or her interactions with four or more teammates working together as a single unit on the playing field.”⁴⁴ The value of statistical data has exponentially grown with the advent of legalized sports gambling.⁴⁵ The debate on the collection method of game statistics stems from the insistence of leagues, like the National Football League (NFL), to license “official data” to the newly legalized betting establishments.⁴⁶ Official data would be “a league-approved tabulation of what happened in a sports competition” to ensure accuracy and reliability.⁴⁷ Some believe this is an effort for sports leagues to get a direct cut of the legalized sports gambling industry.⁴⁸

40. Newman, *supra* note 7.

41. For example, batting average, points per game, goals, shooting percentage, etc.

42. See Grow & Grow, *supra* note 19, at 1572–73.

43. *Id.* at 1572 (citing ROBERT E. KELLY, *BASEBALL’S OFFENSIVE GREATS OF THE DEADBALL ERA: BEST PRODUCERS RATED BY POSITION, 1901-19*, 1 (McFarland & Co. ed., 2009)) (“Of all sports, baseball is the easiest to quantify.”).

44. *Id.* at 1572–73. See FORD, *supra* note 24, at 494 (“Things become more complicated in sports like basketball and football in which the data is more complex and player interactions matter more.”).

45. See James Glanz & Agustin Armendariz, *When Sports Betting is Legal, the Value of Game Data Soars*, N.Y. TIMES (July 2, 2018), <https://www.nytimes.com/2018/07/02/sports/sports-betting.html>.

46. See Moore, *Post-PASPA*, *supra* note 1, at 3–4.

47. Glanz & Armendariz, *supra* note 45.

48. Game statistical data is outside the scope of this Note, as this type of data is public information. See *id.*

B. TEAM PROPRIETARY ADVANCED STATISTICAL AND DATA ANALYTICS

All four major North American sports leagues continue to utilize advancing technology to create complex analytics models. For instance, the NFL equipped all players' shoulder pads with micro-computer chips to constantly track players' "location and movement."⁴⁹ Additionally, the MLB StatCast system "not only records players' every movement on the field, but also tracks the flight of the baseball itself, including both the number of times the ball rotates after being thrown by a pitcher, and the velocity and angle with which it leaves the hitter's bat."⁵⁰ With the implementation of these data-gathering systems, this data presents "a potentially significant source of competitive advantage for the teams that are best able to develop proprietary methods for analyzing this new information and incorporate it into their decision-making processes."⁵¹

Sports franchises may use advanced analytics to enlighten more traditional forms of proprietary information.⁵² For example, teams are highly protective of playbooks containing strategies and plays; both hand and verbal signals by coaches and teammates; scouting reports of strengths and weakness of both their own players and opponents' players; and "records documenting prior and on-going trade negotiations with other clubs."⁵³ The developments in technological sophistication of statistical and data analytics place proprietary information as a sports team's leading basis for competitive advantage.⁵⁴

C. ATHLETES' BIOMETRIC DATA

This subcategory of big sports data is not a new concept to athletes, but the current application and implementation of biometric data is cutting edge. "'Biometric data' is properly defined as measurements or records that can be used to identify people as individuals; identifiers may be physiological . . . or behavioral."⁵⁵ Therefore, vertical jump height, pitch speed, heart rate, body composition, etc. are all forms of biometric data. The latest innovations of wearable technology are used to optimize player performance and safety with the ability to "gather one thousand data points

49. See Grow & Grow, *supra* note 19, at 1577.

50. *Id.*

51. *Id.* at 1578 (stating that "firms continuously seek a competitive advantage over rivals").

52. See *id.* at 1579.

53. *Id.*; see also Rice Ferrelle, *Combating the Lure of Impropriety in Professional Sports Industries: The Desirability of Treating a Playbook as a Legally Enforceable Trade Secret*, 11 J. INTELL. PROP. L. 149, 150 (2003); 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, 315-16 (2009) (describing the lengths team will go to protect their playbooks).

54. See Grow & Grow, *supra* note 19, at 1579.

55. Barbara Osborne, *Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport*, 28 MARQ. SPORTS L. REV. 37, 38 (2017).

per second, per athlete.”⁵⁶ Athlete biometric data is typically collected “to monitor a player’s health, wellness, and performance; establish baselines, perform diagnostics, understand player load, educate coaches and players on the effects of training on players; and to design appropriate training and recovery regimens” to prevent, monitor, and rehabilitate injury.⁵⁷ Tatiana Melnik, a healthcare lawyer, says, “There’s a huge benefit to the player . . . they can get treated faster, and potential long-term damage can be contained,” as a result of data collected from wearable technology.⁵⁸

Presently, federal statutes are absent in regulating the collection of biometric data, but in some contexts, state governments are acting to regulate biometric data collection.⁵⁹ Under the federal statutory framework of the Health Insurance Portability and Accountability Act (HIPAA),⁶⁰ some forms of biometric data are protected only “when collected by health care providers.”⁶¹ Consequently, teams are responsible for self-regulating astronomically large amounts of personal data.⁶²

D. MEDICAL DATA

HIPAA “compel[s] entities that deal with health information to comply with certain privacy and security requirements.”⁶³ Much of the medical staff employed by professional sports teams could be considered healthcare providers and thus are “subject to the privacy and security requirements of HIPAA.”⁶⁴ The Privacy Rule of HIPAA⁶⁵ applies to “teams that submit a bill, charge for a service, or transmit personal health information to an insurance plan in an electronic format.”⁶⁶ The Security Rule of HIPAA similarly covers personal health information in electronic format only and “requires entities to ensure physical, administrative (including risk analysis

56. *Id.*

57. *See id.* at 40.

58. Marc Tracy, *With Wearable Tech Deals, New Player Data Is Up for Grabs*, N.Y. TIMES (Sept. 9, 2016), <https://www.nytimes.com/2016/09/11/sports/ncaaf/football/wearable-technology-nike-privacy-college-football.html>.

59. *See Osborne, supra* note 55, at 46; *see also* Gavin W. Skok, *Washington State Passes Law Restricting Commercial Collection, Storage and Use of Biometric Data*, FOX ROTHSCHILD LLP (June 8, 2017), <https://dataprivacy.foxrothschild.com/2017/06/articles/privacy-rights/washington-state-passes-law-restricting-commercial-use-of-biometric-data/> (noting that Washington joins Illinois and Texas with a Biometric Information Privacy Act to “statutorily restrict the collection, storage and use of biometric data for commercial purposes.”).

60. *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. § 164.514(b) (2018) (listing identifiers of the individual that must be removed to achieve the “safe harbor” method of de-identification. The statute highlights finger and voice prints.) [hereinafter HIPAA].

61. *See Osborne, supra* note 55, at 46.

62. *Id.* at 46–47.

63. *Id.* at 51.

64. *Id.* at 52.

65. *See generally* 45 C.F.R. § 164 (2018) (describing the Privacy Rule of HIPAA).

66. *Osborne, supra* note 55, at 52.

measures), and technical (including access and transmission) security safeguards are in place for protecting [personal health information].”⁶⁷ Additionally, and relevant to data security, the National Institute of Standards and Technology (NIST) created a Cybersecurity Framework in 2014 to supplement the HIPAA Security Rule and “identify potential gaps in their programs.”⁶⁸

III. NOTABLE HACKS AND DATA BREACHES IN SPORTS

Data breaches and hacks have become troublingly pervasive and continue to increase in prevalence.⁶⁹ Seemingly every day, there is another announcement of a major hack with criminals escaping with millions of sensitive records.⁷⁰ Many prominent retailers, healthcare providers, social media platforms, financial institutions, and the U.S. government have had their data substantially compromised.⁷¹ The motives and methods of corporate data breaches are wide-ranging,⁷² but it is clear that sports organizations are similarly vulnerable, especially as the dependence on data technology increases.⁷³ As previously summarized, a motive centered on gaining competitive advantage occurred when Christopher Correa, scouting director of the St. Louis Cardinals, was sentenced to federal prison and permanently banned from baseball for hacking into the Houston Astros database.⁷⁴ Again, this occasion demonstrates a major sports organization’s failure to adhere to the basic cybersecurity practices of secure access and password protocol. Below are examples of nefarious hacking situations in the sporting world, emphasizing the increasing interplay between sports and cyberspace.

67. *Id.* at 51; *see also* 45 C.F.R. § 160.103 (2018); *see generally* 45 C.F.R. § 164 (2018) (describing the Security Rule of HIPAA).

68. *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, U.S. DEP’T OF HEALTH & HUM. SERV. OFF. FOR C.R. 1 (Feb. 22, 2016), <https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf> (explaining the HIPAA cybersecurity intersection with the NIST cybersecurity framework).

69. *See Data Breaches Compromised 4.5 Billion Records in First Half of 2018*, BUSINESS WIRE, Oct. 9, 2018, <https://www.businesswire.com/news/home/20181008005322/en/> (noting a report of “945 data breaches led to 4.5 billion data records being compromised worldwide in the first half of 2018. Compared to the same period in 2017, the number of lost, stolen or compromised records increased by a staggering 133 percent.”).

70. *See* MICHAEL CHERTOFF, *EXPLODING DATA: RECLAIMING OUR CYBER SECURITY IN THE DIGITAL AGE* 49 (Atlantic Monthly Press, 2018).

71. *See* Richie Birns, Alexander Southwell & Ben Arad, *How a new defensive line can protect sports properties*, SPORTS BUS. J. (Aug. 29, 2016), <https://www.sportsbusinessdaily.com/Journal/Issues/2016/08/29/Opinion/From-the-Field-of-Cybersecurity.aspx?hl=breach>.

72. *See generally* CHERTOFF, *supra* note 70 (analyzing these issues of method and motive throughout the book).

73. *See* Birns, Southwell & Arad, *supra* note 71.

74. *See* Eric Fisher, *Breaches highlight difficult task of keeping data secure*, SPORTS BUS. J. (Oct. 23, 2017), <https://www.sportsbusinessdaily.com/Journal/Issues/2017/10/23/In-Depth/Data-sidebar.aspx?hl=hacking> (referencing summary in the introduction).

A. HACKTIVIST INCIDENTS

A hacktivist incident is hacking a website or network to convey a political or social message. There are four hacktivist incidents worth noting. Firstly, in 2014, the Islamic State in Iraq and Syria (ISIS) hacked an English rugby team's website and the Syrian Electronic Army (SEA) hacked FC Barcelona's Twitter account to "display their organizations' extremist messages."⁷⁵ Secondly, in 2015, there was an alleged hack of Tour de France champion Chris Froome. The hacker attempted to access Froome's performance data to prove use of performance-enhancing drugs.⁷⁶ Team Sky alleged that hackers manipulated data to indicate that Froome was doping.⁷⁷ Thirdly, Fancy Bear, a Russian hacking organization, infiltrated the World Anti-Doping Agency and released confidential athlete data for the Rio 2016 Olympics, affecting forty-one athletes, thirteen countries, and seventeen sports.⁷⁸ Fancy Bear's motivation for the hack, gleaned from their website, was to "expos[e] the athletes who violate principles of fair play by taking doping substances."⁷⁹ Fourthly, in April 2017, the International Association of Athletics Federations suspected Fancy Bear of hacking their records on "athletes' therapeutic use exemption applications which, if granted, allow athletes to use otherwise prohibited substances for therapeutic purposes," such as treating illnesses.⁸⁰ Athletes, such as Simone Biles and Serena Williams, had records stolen and released in an effort to portray the United States, the athletes, and doping investigators as hypocritical.⁸¹ Hacktivists inspired by any number of social motives, such as anti-gambling or clean sport sentiment, may be inclined to carry out an attack similar to these above.

75. Christopher LaVigne & Jeewon Kim Serrato, *Hacking scandals highlight vulnerabilities for teams and leagues*, SPORTS BUS. J. (May 8, 2017), <https://www.sportsbusinessdaily.com/Journal/Issues/2017/05/08/Opinion/From-the-Field.aspx>. The tweet from SEA read, "Dear FC Barcelona management, don't let the Qatari money funds you, it's full of blood and kill." James Orr, *Barcelona Twitter account hacked by supports of Syrian president Bashar al-Assad*, INDEPENDENT (Feb. 19, 2014), <https://www.independent.co.uk/sport/football/european/barcelona-twitter-account-hacked-by-supports-of-syrian-president-bashar-al-assad-9138237.html>. FC Barcelona's uniform sponsor was Qatar Airways at the time, and the SEA hackers had extreme hate for Qatar, as civil war in the Arabic region was occurring.

76. LaVigne & Serrato, *supra* note 79.

77. These allegations were linked to Fancy Bear. See Marissa Payne, *Team Sky alleges hacker stole data to frame Tour de France leader Chris Froome for doping*, WASH. POST (July 14, 2015), https://www.washingtonpost.com/news/early-lead/wp/2015/07/14/team-sky-alleges-hackers-stole-data-to-frame-tour-de-france-leader-chris-froome-for-doping/?utm_term=.3e870b7dea3b.

78. See World Anti-Doping Agency, *Cyber Hack Update: Data Leak Concerning 41 athletes from 13 countries and 17 sports*, WADA (Sept. 23, 2016), <https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-41-athletes-from-13-countries-and-17>.

79. See LaVigne & Serrato, *supra* note 79.

80. *Id.*

81. See Rebecca R. Ruiz, *U.S. Says Russians Were Behind Cyberattacks on Antidoping Agency*, N.Y. TIMES (Jan. 6, 2017), <https://www.nytimes.com/2017/01/06/sports/russia-cyberattacks-wada-doping.html>.

B. POOR CYBERSECURITY PRACTICES

Basic quality cyberhealth and cybersecurity practices are foundational to any industry. These incidents underscore the need for basic, prudential protocols and practices in the sporting context. Employee negligence and lack of training are common sources of system breaches. Firstly, in 2016, the Milwaukee Bucks were victims of a phishing scam resulting in the release of tax information, including Social Security numbers and total compensation packages, of all its employees and players.⁸² An unknown party, impersonating Bucks President Peter Feigin using a “spoofed email address,” requested the tax information from a Bucks employee.⁸³ It took approximately three weeks to discover the breach.⁸⁴ The Bucks launched an investigation, notified those impacted, and provided additional privacy training to its staff.⁸⁵ An agent of a Bucks player pointedly said, “The communication received on this major security breach is unacceptable . . . [T]here needs to be accountability for such a mistake, details on the steps taken to rectify it and a process put in place to make sure this never happens again.”⁸⁶ The second incident was an athletic trainer for the Washington Redskins had his laptop stolen from his car in 2017. The computer possessed medical records of players and prospective players from the NFL combine. The Redskins had password protected computers but failed to encrypt their hardware.⁸⁷ After this incident, all “teams have been directed to re-confirm that they have reviewed their internal data protection and privacy policies and that . . . every person with access to medical information has reviewed and received training on the policies regarding privacy and security of that information.”⁸⁸

The following two incidents were careless accidents by professional sports leagues in securing their players’ data. Major League Lacrosse (MLL) accidentally leaked more than 1,000 players’ confidential information.⁸⁹ The league supposedly used an Excel spreadsheet listing personal identifying information.⁹⁰ The MLL received heavy criticism for

82. See LaVigne & Serrato, *supra* note 79.

83. See *id.*

84. See Post Wire Report, *Hacker stole the Bucks’ financial info using oldest trick in the book*, N.Y. POST (May 20, 2016), <https://nypost.com/2016/05/20/hacker-stole-the-bucks-financial-info-using-oldest-trick-in-the-book/>.

85. See *id.*

86. *Id.*

87. John Keim, *Stolen laptop of Redskins trainer contained players’ medical info*, ESPN (June 2, 2016), http://www.espn.com/nfl/story/_/id/15884597/laptop-stolen-washington-redskins-trainer-contained-medical-records-thousands-nfl-players.

88. *Id.*

89. See Fisher, *supra* note 74.

90. Daniel Rapaport, *Major League Lacrosse Accidentally Released Its Players’ Social Security Numbers*, SPORTS ILLUSTRATED (Aug. 29, 2017), <https://www.si.com/more-sports/2017/08/29/major-league-lacrosse> (listing information as “full name, address, telephone

neither encrypting nor password-protecting the information upon the request of the MLL Players' Council and the players.⁹¹ Furthermore, the MLL failed to promptly inform those impacted by the incident.⁹² However, when informed via email, there were instructions to protect their credit and how to file a complaint with the FTC.⁹³ The National Football League Players Association's (NFLPA) database accidentally exposed information of more than 1,100 players and agents.⁹⁴ Kromtech Security, a cybersecurity company, came "across an open Elasticsearch database [a search engine of sorts] sitting on a server for NFLPA.com."⁹⁵ In other words, all the data inside this Elasticsearch database was accessible and compromised to anyone who knew the link.⁹⁶ Hackers who found the database attempted to use ransomware to lock up the database and threatened to release the information to the public unless given a bitcoin payment.⁹⁷ In all of these situations, there was a lack of common sense awareness that needs to be addressed industry wide, and sports betting legislation can begin to tackle basic aspects of cybersecurity.⁹⁸

C. CYBERATTACK IN SPORTS BETTING

DraftKings Inc., a major daily fantasy sports and sports book operator, was attacked in August 2018.⁹⁹ DraftKings filed a suit against unidentified cyberattackers¹⁰⁰ in hopes to discover those responsible for "intentionally sen[ding] thousands of packets of information or commands to [DraftKings'] website with the intent of damaging and negatively impacting [DraftKings] and its operations."¹⁰¹ The attacks, which occurred twice in

number, email address, Social Security number, citizenship, date of birth, height, weight, position, college, graduation year, team, and non-MLL occupation of each player in its player pool.").

91. *See id.*

92. *See id.*

93. No information was reported regarding formal FTC involvement. *See id.*

94. *See* Fisher, *supra* note 74.

95. Thomas Brewster, *1,200 Football Players' Personal Data Exposed In NFL Leak - Colin Kaepernick Included*, FORBES (Oct. 3, 2017), <https://www.forbes.com/sites/thomasbrewster/2017/10/03/colin-kaepernick-nfl-data-leaked-hackers-ransomware-threat/#7b51d9681767>.

96. *See id.*

97. Fortunately, the data breach did not include Social Security numbers or financial information, but the breach did include "players' home addresses, mobile numbers, email addresses, colleges, dates of birth and agent fees. . . ." *See id.*

98. The Cleveland Cavaliers announced official cybersecurity partnership with TrustedSec, a company that provides security through "cyber security tests, hacking simulations, security audits." TrustedSec will act to protect public WIFI in the arena. Kenny Honaker, *Cavs add TrustedSec as 'Official Cyber Security Partner'*, CAVS NATION (Feb. 19, 2019), <https://cavsnation.com/cavs-news-cleveland-adds-trustedsec-official-cyber-security-partner/>.

99. *See* Chris Villani, *DraftKings Files Suit To Unmask Perps In Cyberattack*, LAW360 (Aug. 31, 2018), <https://www.law360.com/articles/1078612/draftkings-files-suit-to-unmask-perps-in-cyberattack>.

100. *See* DraftKings Inc. v. John Does #1-10, Docket No. 1:18-cv-11869 (D. Mass. Aug. 30, 2018).

101. Villani, *supra* note 99.

August 2018, inundated the website with “a three-fold increase of requests per second,” which stifled the ability of legitimate users to participate in website functions.¹⁰² DraftKings filed suit in the U.S. District Court of Massachusetts pursuing the identity and retribution of the responsible party.¹⁰³

These information breaches and attacks on sports organizations denote fundamental shortcomings that leave these organizations glaringly vulnerable.¹⁰⁴ Much of the effort and money of generating progressively secretive and complex data analytic methods is done in-house;¹⁰⁵ therefore, sports teams and leagues are valuable targets of cybercriminals, namely gamblers, mining for confidential information.¹⁰⁶ The value of sports data in a burgeoning gambling industry increases the motivation for hackers to exploit sports organizations.

IV. PREVENTATIVE MEASURES: DATA PROTECTION AND CYBERSECURITY SOLUTIONS

As professional sports continues to reinforce secretive tendencies with data and analytics usage, it resembles other similarly guarded industries like Wall Street.¹⁰⁷ “[S]ecurity breaches and industrial espionage” have also infiltrated the sports industry, similar to the retail or social media industries.¹⁰⁸ In the midst of a data explosion, those entities involved in United States based professional and amateur sports must heed lessons from the FTC on cybersecurity and missteps of company data protection.¹⁰⁹ The sporting industry must place “heightened cybersecurity safeguards into place *now* to protect confidential sports information.”¹¹⁰ Much of the sports gambling regulatory debates involve the social implication of gambling addiction and match-fixing, but the cybersecurity/hacking risk is a serious concern that regulators must not neglect.¹¹¹

102. *See id.*

103. *Id.*

104. *See generally* LaVigne & Serrato, *supra* note 79 (highlighting teams and leagues vulnerabilities, often to basic cybersecurity demands).

105. *See* FORD, *supra* note 24, at 491.

106. *See* LaVigne & Serrato, *supra* note 79.

107. In both Wall Street banking and sports, data information is being vehemently guarded by the executives in order to remedy inefficiencies and gain advantages. *See* Moore, *supra* note 16; *see also* FORD, *supra* note 24, at 491.

108. *See* FORD, *supra* note 24, at 491.

109. *See* ANDREA M. MATWYSHYN, *HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION* 243–44 n. 53 (Stanford Univ. Press 2009).

110. Craig A. Newman, *Sports Data & Cybercrime: Alarm Bells?*, PATTERSON BELKNAP (Sept. 26, 2018), <https://www.pbwt.com/data-security-law-blog/sports-data-cybercrime-alarm-bells/>.

111. *See* Zaggar, *supra* note; *see generally* *Post-PASPA: An Examination of Sports Betting in America Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. On the Judiciary*, 115th Cong. (2018) (statements of Les Bernal, National Director of Stop Predatory Gambling), <https://docs.house.gov/meetings/JU/JU08/20180927/108721/HHRG-115-JU08-Wstate-BernalL-20180927.pdf> (addressing the addictive nature of government-

A. CURRENT LEGAL REMEDIES ALONE ARE INSUFFICIENT

There are many rules and laws in place to protect a team's secrets and data, however, these legal remedies are sometimes "effectively worthless."¹¹² Trade secret laws,¹¹³ paired with nondisclosure and noncompete contracts for employees, protect a wide variety of information.¹¹⁴ Yet, there remain disadvantages in these methods of protection. For example, "preventing an employee from going to work for a competitor is far more disruptive than prohibiting her from disclosing secrets, since it can affect her basic livelihood."¹¹⁵ When obtaining a noncompete agreement, employers may have to provide additional consideration to compensate the employee for future losses in income as a result of the noncompete.¹¹⁶ Finally, "in many cases, obtaining a noncompete agreement may be impossible, since some states ban them outright or significantly limit their scope."¹¹⁷ In a dynamic internet and data analytics industry, noncompete agreements are likely to be short in duration because technology is rapidly evolving.¹¹⁸ The professional sports industry is comparatively small, thus limiting options for professional growth if encumbered by strict noncompete clauses.¹¹⁹

When league or team secrets/data are unduly taken, other legal remedies exist within criminal law. For example, the Computer Fraud and Abuse Act (CFAA)¹²⁰ is useful for obtaining confidential information involving unauthorized access of a computer.¹²¹ The statutory requirement

sanctioned gambling and the financial losses Americans are expected to endure with legalized sports gambling) [hereinafter *Bernal: Post-PASPA*]; see generally *Post-PASPA: An Examination of Sports Betting in America Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. On the Judiciary*, 115th Cong. (2018) (statements of Jon Bruning, Counselor of Coalition to Stop Online Gambling), <https://republicans-judiciary.house.gov/wp-content/uploads/2018/06/Bruning-Testimony.pdf> (addressing the addictive social implication of online gambling and the shortcomings of laws applying to online gambling activity) [hereinafter *Bruning: Post-PASPA*].

112. See FORD, *supra* note 24, at 504.

113. Trade secret law was discussed in Section I: The Explosion of Valuable Sports Data of this Note. See discussion *supra* Section I; see also FORD, *supra* note 24, at 504 (noting that "trade secrecy protects only against wrongful misappropriation by another. If someone obtains the exact same information through legitimate means, then there's no problem.").

114. See FORD, *supra* note 24, at 498 (defining the difference between nondisclosure agreements and noncompete agreements, noting that "nondisclosure agreements prohibit signers from disclosing covered information to third parties, while noncompete agreements prohibit a team's employees from working for the competitor for a fixed period after leaving the team.").

115. *Id.*

116. See *id.*

117. *Id.*

118. See ANN C. HODGES & RAFAEL GREY, *Noncompetition Covenants*, PRINCIPLES OF EMPLOYMENT LAW 166, 167 (2nd ed. 2018); Steve Lohr, *To Compete Better, States Are Trying to Curb Noncompete Pacts*, N.Y. TIMES (June 28, 2016), <https://www.nytimes.com/2016/06/29/technology/to-compete-better-states-are-trying-to-curb-noncompete-pacts.html>.

119. See FORD, *supra* note 24, at 498–99.

120. 18 U.S.C. § 1030 (2012).

121. See FORD, *supra* note 24, at 503.

of computer access “without authorization” is contentious and has led to ambiguity in interpretation.¹²² This remedy is likely useful in many circumstances due to professional teams’ dependence “on networked computers and data to operate.”¹²³ Additional criminal law remedies include mail-fraud and wire-fraud statutes “ban[ning] the use of the mail or most telecommunications services to commit fraud or obtain another’s property or money.”¹²⁴ In *Murphy*, the Supreme Court did not alter the applicability of the federal Interstate Wire Act of 1961 and referred to the previously established “safe harbor” exception in transmitting sports wagering information between jurisdictions where sports wagering is lawful.¹²⁵

Criminal laws can be a powerful tool as both deterrents and remedies to data breaches and stealing confidential information. However, criminal investigations and the prosecution of alleged misconduct are executed by “law enforcement agents and prosecutors instead of private lawyers” and “teams must give up a lot of control,” especially with requirements to cooperate with investigations by divulging secrets and algorithms.¹²⁶ Essentially, the best practice is preventing the taking of secrets and preventing data breaches from occurring by thorough effective information-security on both technical and human factors.¹²⁷

B. COMBAT HACKING THROUGH FEDERALLY GUIDED STANDARDS

A federal regulatory scheme for the sports gambling market must provide laws that incentivize the privately owned and operated companies

122. See *id.* (highlighting the debate over the definition of “without authorization”). One example of this is “if a team employee violated team policies to download data to a personal flash drive, and only later provided that data to a rival team, it might or might not count as unauthorized access since physical access to the computer was authorized but the scope of the access was not.” *Id.* This example displays a narrow interpretation of the CFAA “maintain[ing] that the prohibition only refers to information within a system that an insider does not have explicit authorization to access,” but the “broad interpretation camps maintain that exceeding authorized access refers not just to the situations discussed above, but also to situations in which an employee accesses information that she is authorized to access but does so for the purposes that violate her authorization.” Kevin Jakopchek, “Obtaining” the Right Result: A Novel Interpretation of the Computer Fraud and Abuse Act That Provides Liability for Insider Theft Without Overbreadth, 104 J. CRIM. L. & CRIMINOLOGY 605, 632 (2014).

123. *Id.*

124. *Id.* (citing 18 U.S.C. §§ 1341, 1343 (2008)).

125. See 18 U.S.C. § 1084 (a)–(b) (2012); see also Mark A. Clayton & Erica L. Okerberg, *The Wire Act and Interstate Sports Wagering Post-Murphy*, GREENBERG TRAURIG, LLP ALERT: GAMING (Sept. 4, 2018), <https://www.gtlaw.com/en/insights/2018/9/the-wire-act-and-interstate-sports-wagering-post-murphy>.

126. FORD, *supra* note 24, at 504. Additionally, the cybersecurity laws in the U.S. are “an uncoordinated mishmash of requirements that mostly were conceived long before modern cyber-threats. . . stem[ming] from century old privacy norms, torts, and criminal laws that bear little relation to protection of the confidentiality, integrity, or availability of systems, networks, and data.” Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 988 (2018).

127. See FORD, *supra* note 24, at 504.

“to collaborate with the government in protecting against shared vulnerabilities.”¹²⁸ Information Technology (IT) infrastructure and data security are largely private.¹²⁹ The internet creates an interdependence, or a joint venture, for effective data security of similarly situated entities within an industry.¹³⁰ “Without government expertise and even regulation, coupled with private sector ingenuity and commitment, the internet infrastructure will continue to fall prey to its weakest links.”¹³¹ President Obama signed an Executive Order in 2015 in an effort to promote private sector cybersecurity information sharing.¹³² The intent of Information Sharing and Analysis Organizations (ISAO) was to facilitate the sharing of “information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.”¹³³ It is critical that regulation in the sports gambling industry clearly promote and directly guard information sharing among all entities involved as seen in other areas of the private sector.¹³⁴

Currently, ISAOs service information sharing through Information Sharing and Analysis Centers (ISAC). These ISACs are typically operated through a sector-based model, “meaning that organizations within a certain sector¹³⁵ join together to share information about cyber threats.”¹³⁶ Cooperation across states, sports teams, and leagues is “important so that as large a slice of the market as possible can be monitored.”¹³⁷

Action has been taken to establish the Sports Wagering Integrity Monitoring Association (SWIMA), a nonprofit overseer to detect fraud as sports betting evolves.¹³⁸ This association would essentially function in the same way as an ISAO “that would share betting information in an effort to identify suspicious activity aimed at compromising sporting events.”¹³⁹ The American Gaming Association, a “group that represents the casino industry,

128. CHERTOFF, *supra* note 70, at 206.

129. *See id.*

130. *See id.*

131. *Id.*

132. *See* U.S. Exec. Order No. 13691 (Feb. 13, 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari> (describing the specific methods for sharing cybersecurity information in the private sector).

133. *Id.*

134. CHERTOFF, *supra* note 70, at 206.

135. For example, financial services, energy, aviation, etc.

136. *Information Sharing and Analysis Organizations (ISAOs)*, HOMELAND SEC. (May 21, 2018), <https://www.dhs.gov/isao>.

137. Scott Schectman & Tony Sio, *Why America Should Embrace Market Surveillance in Sports Betting Before It's Too Late*, N.Y. TIMES (Sept. 20, 2018), <https://www.nytimes.com/2018/09/20/business/dealbook/why-america-should-embrace-market-surveillance-in-sports-betting-before-its-too-late.html>.

138. *See* Jeannie O'Sullivan, *Ex-NJ Asst. AG Joins New Sports Betting Watchdog*, LAW360 (Nov. 28, 2018), <https://www.law360.com/articles/1105626/ex-nj-asst-ag-joins-new-sports-betting-watchdog>.

139. Ryan Rodenberg, *'Integrity monitoring association' for sports betting under consideration*, ESPN (Sept. 25, 2018), http://www.espn.com/chalk/story/_/id/24742199/integrity-monitoring-association-sports-betting-consideration.

said it is collaborating on a ‘robust suspicious information sharing repository.’”¹⁴⁰ Sports leagues, including the Professional Golfers’ Association (PGA), have stated a federal requirement is needed so that an all-inclusive approach to information sharing provides the greatest benefit to sports integrity.¹⁴¹ In a 2007 joint letter to Congress from NFL, NBA, MLB, National Hockey League (NHL), and National Collegiate Athletic Association (NCAA) attorneys, they wrote, “[W]e have heard the argument that Internet gambling can actually protect the integrity of sports because of the alleged capacity to monitor gambling patterns more closely in a legalized environment.”¹⁴² Federal intervention in the form of mandating centralized committees or associations will help foster transparency between sports leagues, regulators, and betting providers.¹⁴³ In the case of SWIMA, the organization is funded by the gambling industry as opposed to government funds, but it is a collaborative effort among regulators, law enforcement, and stakeholders “to detect and discourage fraud and other illegal or unethical activity related to betting on sporting events.”¹⁴⁴ SWIMA realizes that federal law enforcement and resources are integral to the success of this watchdog organization.¹⁴⁵

C. PROPER SURVEILLANCE AND THE ROLE OF THE FTC

Fast-forward to the 2000s financial markets where “[m]any investors, regulators, and capital market players were caught flat-footed when markets were computerized decades ago.”¹⁴⁶ The financial industry was not sufficiently prepared for the digital age and the difficulty of tracking trading methods “within a sea of data.”¹⁴⁷ In both the 1930s and the early 2000s, “the cost to the financial industry of catching up with the bad behavior was significantly higher than if it had invested in defensive technologies at the start.”¹⁴⁸ Fortunately, now the systems tasked with surveilling the financial markets have a tremendous capacity for data, which aids in immediately detecting suspicious activity.¹⁴⁹ These types of systems will be critical for policing the sports gambling market, particularly real-time, in-game betting (prop bets).¹⁵⁰ With growth in the quantity of data and cunningness of gamblers, regulators and enforcement agents would be prudent to learn

140. *Id.*

141. *See id.*

142. *Id.*

143. *Id.*

144. O’Sullivan, *supra* note 138.

145. *See id.*

146. Schectman & Sio, *supra* note 137.

147. *See id.*

148. *Id.* (estimating implementation of the Consolidated Audit Trail cost the financial industry over \$50 million in its first year).

149. *See id.*

150. *See id.*

lessons from advancements in the monitoring of the securities market.¹⁵¹ Many risks can now be identified because of similarities to the securities exchange.¹⁵² The security market, like the sports market, exist on a national level, and therefore state regulation alone is inadequate.¹⁵³ A federal framework provides the sports gambling industry a greater chance of staving off an industry equivalent to a stock market crash.

The FTC's purpose is "advancing consumer interests while encouraging innovation and competition in our dynamic economy."¹⁵⁴ Additionally, the FTC collaborates with domestic and international law enforcement agencies and organizations to protect consumers.¹⁵⁵ In the FTC's quest to stop "unfair, deceptive or fraudulent practices in the marketplace," it has regulatory, investigatory, enforcement, and adjudicative powers under the Federal Trade Commission Act.¹⁵⁶ The FTC specializes in data security and privacy measures in the marketplace.¹⁵⁷ The FTC puts forth suggestions/guidelines for data security within companies and has "deemed the reach of its powers to prevent unfairness and deception under Section 5 of the FTC Act to include issues of information security promises made to consumers."¹⁵⁸ The FTC has filed many complaints under the unfairness prong of the FTC Act § 45(a), and the Third Circuit decision in *FTC v. Wyndham* reaffirmed the FTC's expansive enforcement authority in United States corporate privacy and security.¹⁵⁹ Following this case in 2015, the FTC Chairwoman Edith Ramirez stated, "It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information."¹⁶⁰

Many cases settle when the FTC brings an action under FTC Act 15 U.S.C. § 45(a) prohibiting "unfair and deceptive acts or practices in or affecting commerce."¹⁶¹ Thus, there are limited judicial interpretations of

151. *See id.*

152. Schectman & Sio, *supra* note 137.

153. *See* Keith C. Miller & Anthony N. Cabot, *Regulatory Models for Sports Wagering: The Debate Between State vs. Federal Oversight*, 8 UNLV GAMING L.J. 153, 174 (2018).

154. *What We Do*, FTC, <https://www.ftc.gov/about-ftc/what-we-do> (last visited Nov. 28, 2018) [hereinafter *FTC: What We Do*]

155. *See id.*

156. *Id.*

157. *See* ANDREW B. SERWIN ET AL., FEDERAL TRADE COMMISSION ACT AND ENFORCEMENT UNDER THE FTC ACT, PRIVACY, SECURITY AND INFORMATION MANAGEMENT: AN OVERVIEW 421 (ABA 2011).

158. Matwyshyn, *supra* note 109, at 243–244.

159. *See* Press Release, FTC, Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter (Aug. 24, 2015), <https://www.ftc.gov/news-events/press-releases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham>.

160. *Id.*

161. Gerald J. Ferguson & Alan L. Friel, *Challenging FTC Regulation of Cyber-security After FTC v. Wyndham*, BAKER HOSTETLER: DATA PRIVACY MONITOR (Nov. 4, 2015),

the statute.¹⁶² Wyndham Worldwide Corporation's computer systems were hacked on three separate occurrences within one year.¹⁶³ Personal and financial information of many thousands of consumers was stolen, and Wyndham's inadequate data security resulted in \$10.6 million in fraudulent charges.¹⁶⁴ The Third Circuit affirmed that "Wyndham engaged in unfair cybersecurity practice that, 'taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."¹⁶⁵ This decision effectively puts companies on notice to meet certain baseline privacy and security standards set by *Wyndham*.¹⁶⁶ This case does not provide a bright-line rule on minimum adequate cybersecurity practice; therefore, each company must align their policies and practices with the "risks given the varieties of industries, customers, vendors, markets, and regulations."¹⁶⁷

V. SPORTS GAMBLING ANALOGIZED TO SECURITY EXCHANGE

A. EFFECTIVE SIMILARITIES

In certain parts of the world,¹⁶⁸ the sports gambling scene resembles the trading floor of the New York Stock Exchange.¹⁶⁹ There are monitors with live data feeds to facilitate "in-play wagering."¹⁷⁰ The sports gambling industry in the United States should adopt more than just the atmosphere of the Securities Exchange.¹⁷¹ Sports wagering and securities regulation both "concern the regulation of exchanges involving contracts where the purchaser/bettor is attempting to earn profits based on a future contingent event."¹⁷² In both markets, developing laws and strict regulation would serve to curtail insiders, including those who nefariously possess insider information, from acting (trading or betting) on that information not available to the investing or betting public.¹⁷³ The SEC was created "to restore investor confidence in our capital markets by providing investors

<https://www.dataprivacymonitor.com/cybersecurity/challenging-ftc-regulation-of-cyber-security-after-ftc-v-wyndham/>.

162. See *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015).

163. See *id.*

164. See *id.*

165. *Id.*

166. See David Adler, *FTC v. Wyndham and corporate cybersecurity*, CIO FROM IDG (Sept. 1, 2016), <https://www.cio.com/article/3110012/security/ftc-v-wyndham-and-corporate-cybersecurity.html>.

167. *Id.*

168. For example, Europe, Asia, and Australia. See Schectman & Sio, *supra* note 137.

169. See *id.*

170. See *id.*

171. See *id.*

172. Miller & Cabot, *supra* note 153, at 173.

173. See *id.*

and the markets with more reliable information and clear rules of honest dealing.” The SEC had to restore investor confidence after state government regulatory schemes proved ineffective, since “stock promoters complied only with the laws of the states with the least regulation or the most corruption and used that as a basis for offering the stocks on a national basis.”¹⁷⁴ The states were only willing to concede regulatory power after the stock market crash in 1929.¹⁷⁵ Thus, the Securities Exchange Act of 1934 established the SEC with the purpose “to eliminate the idea that use of inside information for personal advantage was a normal emolument of corporate office.”¹⁷⁶ The sports betting industry possesses similar needs of deterrence and protection against betting on insider information.

B. TREATMENT OF OUTSIDER TRADING BY THE SEC

Throughout this discussion, there have been references to insider, confidential, trade secret, and non-public information. The act of cybercriminals taking confidential team or league information and betting on this information is most analogous to outsider trading, a form of insider trading on securities where the individual does not have a fiduciary duty to investors. The conventional ideas of insider trading must be established in order to analyze the SEC’s treatment of outsider trading.

Section 16(b) of the Securities and Exchange Act of 1934 addresses insider trading by allowing shareholders to sue officers, directors, or shareholders “to recover any short-swing profits gained by the purchase and sale, or sale and purchase, of any equity security in the company occurring within six months of each other.”¹⁷⁷ Section 16(b)’s purpose is to “prevent [] the unfair use of information which may have been obtained by such beneficial owner, director or officer by reason of his relationship to the issuer.”¹⁷⁸ Insider trading violations are governed by Rule 10(b)-5, which prohibits fraud or misrepresentation in securities transactions.¹⁷⁹ Furthermore, Rule 10(b)-5 has three provisions for the purchase or sale of a security: (a) prohibits the use of “any device, scheme, or artifice to defraud;”¹⁸⁰ (b) prohibits material misstatements and omissions;¹⁸¹ (c) prohibits engaging in “any act, practice, or course of business which

174. *Id.* at 174.

175. *See id.*

176. *Dirks v. SEC*, 463 U.S. 646, 653 n. 10 (1983) (quoting *In re Cady, Roberts & Co.*, 40 SEC 907, 912 n. 15 (1961)).

177. Adam R. Nelson, *Extending Outsider Trading Liability to Thieves*, 80 *FORDHAM L. REV.* 2157, 2163 (2012).

178. 15 U.S.C. § 78p (2012).

179. *See* John Reed Stark, *Inside The SEC’s Outsider Trading Program: Part 1*, *LAW360* (Oct. 29, 2018), <https://www.law360.com/articles/1096312/inside-the-sec-s-outsider-trading-program-part-1>.

180. 17 C.F.R. § 240.10b-5(a) (2011).

181. *See* Nelson, *supra* note 177, at 2165 (citing 17 C.F.R. § 240.10b-5(b)).

operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.”¹⁸² Section 10(b) and Rule 10(b)-5 are “not intended as a specification of particular acts or practices that constitute fraud, but rather are designed to encompass the infinite variety of devices by which undue advantage may be taken of investors and others.”¹⁸³ This language set the stage for a slowly developed “judicially created concoction” prohibiting insider trading.¹⁸⁴

The classical theory of insider trading states that insiders must either disclose or abstain from trading on material non-public information lest that insider be liable for fraud.¹⁸⁵ This classical theory only imposes a fiduciary duty on shareholders and their tippees.¹⁸⁶ Additionally, misappropriation theory, an expansion of classical theory, “extended liability from insiders, to outsiders who receive tips from insiders, to outsiders who owe a duty to the source of the information.”¹⁸⁷ In *O’Hagan*, the Supreme Court “stated that the misappropriation theory . . . was intended to target outsiders without a fiduciary duty to shareholders of the company in whose securities they traded”¹⁸⁸ and created a “duty of trust and confidence” to the source of the information.¹⁸⁹ This judicial expansion was an effort to ensure honest markets and investor confidence. The Court determined the alternative would be unworkable and opined “permitting unchecked use of misappropriated information would permit certain individuals to gain an informational advantage that other parties could not overcome through research and would cause investors to either refuse to participate in the market, or discount securities.”¹⁹⁰ The concern expressed here is one of legitimacy for sports betting, since participants are less likely to partake in a unfair enterprise.

From 2005 to 2016, the SEC staff greatly prioritized the targeting of the outsider thief breaking “through a virtual window, in cyberspace” and “reasoning that hack-and-trade cyber thieves were masquerading as company insiders and were therefore committing securities fraud.”¹⁹¹ The SEC brought enforcement actions against individuals who had no

182. 17 C.F.R. § 240.10b-5(c).

183. *In re Cady, Roberts & Co.*, 40 SEC 907, 911 (1961).

184. Stark, *supra* note 179.

185. See Bradley J. Bondi & Steven D. Lofchie, *Practitioner Note: The Law of Insider Trading: Legal Theories, Common Defenses, and Best Practices for Ensuring Compliance*, 8 N.Y.U J. L. & BUS. 151, 160 (2011).

186. See Nelson, *supra* note 177, at 2178.

187. *Id.* at 2192 (expanding on classical theory in Chief Justice Burger’s dissent in *Chiarella* and the Supreme Court opinions of *Carpenter* and *O’Hagan*).

188. *Id.* at 2185 (citing *United States v. O’Hagan*, 521 U.S. 642, 652–53 (1997)).

189. See *United States v. O’Hagan*, 521 U.S. 642, 652–54 (1997) (explaining that the defendant misappropriated the non-public information to purchase securities).

190. Nelson, *supra* note 177, 2180–81 (citing *United States v. O’Hagan*, 521 U.S. 642, 658–59 (1997)).

191. Stark, *supra* note 179.

relationship to the source of the information other than gaining or stealing material non-public information and trading securities based on this information.¹⁹² Within this ten year period, the SEC enforcement action highlighted the pervasive threat from sophisticated hackers of confidential information, which may preview similarly nefarious acts to come in the sports betting world.

Two outsider trading cases especially display the parallel cybersecurity issues posed in the securities market and the sports betting market. In 2008, *SEC v. Oleksandr Dorozhko* became the seminal case in the extension of outsider trading liability.¹⁹³ Dorozhko opened an online trading account and deposited \$42,500, then with this money he purchased \$41,670.90 in put options of IMS Health Inc. stock.¹⁹⁴ Shortly after, IMS announced their earnings were 28% below third quarter expected earnings.¹⁹⁵ Thus, the next morning the stock dropped severely, and Dorozhko sold all his put options for a \$286,000 profit.¹⁹⁶ The SEC managed to uncover that Dorozhko had hacked the earnings report before its release.¹⁹⁷ He had repeatedly attempted to hack the Thomsen Financial Inc. server, the web-hosting service for IMS earnings reports.¹⁹⁸ Dorozhko successfully hacked the server, located the report, and downloaded the non-public information.¹⁹⁹ Interactive Brokers, the online trading company used for the purchase of put options, informed the SEC of irregular trading activity and they were able to trace the activity to Dorozhko's IP address.²⁰⁰ The Southern District Court of New York refused to extend securities fraud liability on Dorozhko because precedent in *Chiarella* and *O'Hagan* maintained that "insider trading was premised on a fiduciary or similar duty to disclose or abstain."²⁰¹

On appeal to the Second Circuit, the Court vacated the Southern District Court of New York decision stating that the lower court misinterpreted precedent and *Dorozhko* satisfies § 10(b)'s requirement of deception or contrivance.²⁰² Furthermore, the Court opined that "what is sufficient is not always what is necessary, and none of the Supreme Court opinions considered by the District Court *require* fiduciary relationship as

192. See Nelson, *supra* note 177, at 2182.

193. See Stark, *supra* note 179.

194. See Nelson, *supra* note 177, at 2183.

195. See Stark, *supra* note 179.

196. See *id.*

197. See *id.*

198. See Nelson, *supra* note 177, at 2183.

199. See *id.*

200. See *id.*

201. *Id.*

202. *Id.* at 2183–84.

an element of an actionable securities claim under Section 10(b).”²⁰³ By Dorozhko misrepresenting himself in stealing the information, the Court determined this was a deceptive device sufficient for outsider trading liability.²⁰⁴

About eight years after *Dorozhko*, in 2015, the SEC charged thirty-two defendants with fraud in a cyberhacking scheme of news releases.²⁰⁵ The SEC charged two Ukrainian men, Ivan Turchynov and Oleksandr Ieremenko, of leading a hacking scheme of newswire services to steal hundreds of earnings announcements before the data was released to the public.²⁰⁶ Over a five year span, the defendants procured over \$100 million in profits by illegally trading on and disseminating stolen data.²⁰⁷ The SEC investigation discovered Turchynov and Ieremenko relayed the hacked data, for a price, to traders in Russia, Ukraine, Malta, Cyprus, France, New York, Pennsylvania, and Georgia.²⁰⁸ Specifically, the defendants used “proxy servers to mask their identities and by posing as newswire service employees and customers,” and they advertised their hacking ability via video to recruit and elicit payments from traders for their services.²⁰⁹ The authorities have yet to locate Turchynov and Ieremenko, but many of those involved have incurred civil liability for securities fraud and plead guilty to criminal counts of conspiracy to commit wire fraud, conspiracy to commit computer hacking, and aggravated identity theft.²¹⁰ According to the former Director of the SEC’s Division of Enforcement, the SEC’s “use of innovative analytical tools to find suspicious trading patterns and expose misconduct demonstrates that no trading scheme is beyond our ability to unwind.”²¹¹ There are a number of other hacking incidents involving trading of securities and the SEC, including a Chinese hacking scheme in 2016 and the hack of the SEC’s Electronic Data Gathering and Retrieval system (EDGAR) in 2017.²¹²

203. Nelson, *supra* note 177, at 2183–84 (quoting SEC v. Dorozhko, 574 F.3d 42, 49 (2d Cir. 2009)); see SEC v. Dorozhko, 606 F. Supp. 2d 321, 326 (S.D.N.Y. 2008), *vacated by* SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009).

204. See Stark, *supra* note 179.

205. See Press Release, SEC, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015), <https://www.sec.gov/news/pressrelease/2015-163.html>.

206. See Stark, *supra* note 179.

207. See Press Release, *supra* note 205.

208. See *id.*

209. *Id.*

210. See Press Release, The U.S. Att’y’s Off. District of N.J., Hacker Sentenced to 30 Months In Prison for Role in Largest Known Computer Hacking and Securities Fraud Scheme (May 22, 2017), <https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities>.

211. Press Release, *supra* note 205 (quoting Andrew Ceresney, the former Director of the SEC’s Division of Enforcement).

212. See Stark, *supra* note 179.

C. GOVERNMENT AGENCY'S COMMITMENT AND RESOURCES TO CYBERSECURITY

Government agencies, such as the SEC and FTC, are the fiduciary of the American taxpayer and work “on behalf of the American people.”²¹³ Federal legislation, including the Clinger-Cohen Act of 1996,²¹⁴ the E-Government Act of 2002,²¹⁵ and the Federal Information Security Management Act of 2002,²¹⁶ “involves both securing federal systems and fulfilling the appropriate federal role in protecting nonfederal systems.”²¹⁷ A 2017 Executive Order stated that it will hold agency heads responsible and “accountable for managing cybersecurity risk to their enterprises.”²¹⁸ The President of the United States will hold these agency heads responsible for implementing the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST.²¹⁹ The items and procedures outlined in the Executive Order are instituted, “to ensure the internet remain valuable for future generations . . .” and “to promote open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft.”²²⁰ The federal government agencies are hyperaware of the cybersecurity issues and hold a legislatively mandated high standard of responsibility.²²¹ The Executive Branch of the Federal Government is using its authority and capabilities to support cybersecurity risk management.

213. See U.S. Exec. Order No. 13800 (May 11, 2017), <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

214. “*The Clinger-Cohen Act of 1996* made agency heads responsible for ensuring the adequacy of agency information-security policies and procedures, established the chief information officer (CIO) position in agencies, and gave the Secretary of Commerce authority to make promulgated security standards mandatory.” ERIC A. FISHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 2 (2014).

215. “*The E-Government Act of 2002* serves as the primary legislative vehicle to guide federal IT management and initiatives to make information and services available online and includes various cybersecurity requirements.” *Id.*

216. “*The Federal Information Security Management Act of 2002 (FISMA)* clarified and strengthened NIST and agency cybersecurity responsibilities, established a central federal incident center, and made OMB, rather than the Secretary of Commerce, responsible for promulgating federal cybersecurity standards.” *Id.*

217. *Id.*

218. U.S. Exec. Order No. 13800, *supra* note 213.

219. See *id.*

220. *Id.*

221. See generally Fisher, *supra* note 214 (outlining the current statutes pertaining to cybersecurity in government agencies).

VI. STATE REGULATORY ADVOCATES

State gambling regulators have taken a firm stance against federal oversight since PASPA was deemed unconstitutional.²²² Proponents of individual state regulation of sports gambling rely on gaming laws historically belonging within the purview of states' rights.²²³ State lotteries, casino games, and sports gambling have different levels of chance and skill.²²⁴ In 2015, the Borgata Casino hosted the first 'Free Throw Basketball Tournament,' where participants wagered on their ability to make foul shots in a highly regulated competition with over forty rules listed.²²⁵ If they were to bet on other shooters or professional basketball players' foul shots, then information about the competitors gives some participants a distinct advantage. The human factor and the flow of information, especially with the use of technology, takes sports gambling into a different sphere than what states traditionally regulate. With increased skill and decreased chance, the external factors escalate, making regulation responsibilities more complex.

In a statement signed by four state gaming commissioners, the concern is that integrity fees and federal oversight would "increase the costs of legal sports betting [and] siphon much-needed tax revenues away from state coffers."²²⁶ Furthermore, advocates of state regulatory control push to emulate the decades of experience that Nevada provides from legalized sports betting. The Chair of the Nevada Gaming Control Board outlined Nevada's critical legal regulation concerns: (1) integrity in gaming, (2) the impact of reasonable tax rates and fee structures, (3) combatting illegal operators is a perpetual reality, (4) sports wagering technology of the highest quality, and (5) issues of gambling addiction.²²⁷ States can improve on or adopt the Nevada regulatory model. Essentially, states would be regulatory "'laboratories' for other states to learn from."²²⁸ Additionally,

222. See James Glanz, *States Are Pushing to Keep Federal Regulation Out of Sports Gambling*, N.Y. TIMES (May 23, 2018), <https://www.nytimes.com/2018/05/23/sports/sports-gambling-regulation.html>.

223. See *id.*

224. See Eric Chemi, *Skill, chance, gambling, legality: They're all separate*, CNBC: THE BIG CRUNCH WITH ERIC CHEMI (Nov. 12, 2015), <https://www.cnbc.com/2015/11/12/skill-chance-gambling-legality-theyre-all-separate.html>.

225. See *id.*

226. Glanz, *supra* note 222. Integrity fees are the sports leagues taxing a percentage of each bet placed in which their league is implicated in the bet. This fee is then used to maintain the integrity of the sport.

227. See generally *Post-PASPA: An Examination of Sports Betting in America Before the Subcomm. on Crime, Terrorism, Homeland Security and Investigations of the H. Comm. On the Judiciary*, 115th Congr. (2018) (statement of Becky Harris, Chair, Nevada Gaming Control), <https://republicans-judiciary.house.gov/wp-content/uploads/2018/06/Chairwoman-Becky-Harris.pdf> (outlining several concerns regarding the regulation of legalized sports betting) [hereinafter *Harris: Post-PASPA*].

228. Miller & Cabot, *supra* note 153, at 164.

states argue regulatory autonomy enables “a sports wagering system that fit[s] their own peculiar set of values and regulatory goals . . . and states might be more responsive to technological change and would be able to adapt more quickly to proposals for innovation.”²²⁹

However, there are overwhelming drawbacks to exclusive state regulatory control. State Gaming Commissions and state legislators have acknowledged the need for strong federal support of enforcement agencies.²³⁰ States believe geofencing their borders is sufficient to control intrastate sports gambling,²³¹ but Full Committee Chairman of the House Judiciary Committee Bob Goodlatte and the expert testimony of Jon Bruning, Counsel of the Coalition to Stop Online Gambling, are acutely suspicious of states’ ability to handle an internet that knows no borders.²³² Online sports gambling is the most lucrative avenue for the industry, as “most of New Jersey’s sports bets have been placed online (\$539 million) compared with in person at a casino or racetrack (\$388 million).”²³³ Sports leagues, the internet, and cybersecurity are not confined to state borders. Chairman Goodlatte observed:

With the development of the Internet, however, state prohibitions and regulations governing gambling have become increasingly hard to enforce as electrometric communications move freely across borders. Many gambling operations are beginning to take advantage of the ease with which communications can cross state lines in order to elicit illegal bets and wagers from individuals in jurisdictions that prohibit those activities.²³⁴

Prohibiting cybersecurity lapses and preventing sports gambling on nonpublic information are critical to maintaining integrity in the sport and protecting consumers as well as the privacy of the athletes.

On December 19, 2018, Senator Charles Schumer (D-N.Y.) and Senator Orrin Hatch (R-Utah) introduced a bipartisan federal bill that “would have the U.S. Justice Department set minimum standards for states to offer sports betting.”²³⁵ The Sports Wagering Market Integrity Act of 2018²³⁶ looks to

229. *Id.* at 165.

230. See Glanz, *supra* note 222.

231. See Harris: *Post-PASPA*, *supra* note 227, at 13 (defining geolocation and geofencing as “[g]eolocation is [the] process by which a user’s location can be identified through use of their mobile device. Geolocation typically calls upon multiple resources such as GPS, WIFI, or mobile cell tower triangulation through the use of radio-frequency (RF) technology.” Geofencing creates virtual borders that can use this geolocation to trigger alarms if the mobile devices enters or exits the boundary.)

232. See Bruning: *Post-PASPA*, *supra* note 111, at 4–5.

233. Wayne Parry, *New Jersey sport betting market closing in on \$1B mark*, ASSOCIATED PRESS, Dec. 12, 2018, <https://www.apnews.com/70681866fb5f4be79c62a7f24b467971>.

234. See Bruning: *Post-PASPA*, *supra* note 111, at 4–5 (quoting Chairman Goodlatte).

235. Wayne Parry, *AP NewsBreak: Feds eye move to regulate legal sports betting*, ASSOCIATED PRESS, Dec. 19, 2018, <https://apnews.com/a3e2b43f3931436e8156f54471ad5fc3>.

236. Sports Wagering Market Integrity Act of 2018, 115 S. 3793, 115th Cong. (2018).

address integrity concerns that cannot be patrolled within state borders.²³⁷ Schumer emphasized, “I knew that Congress had an obligation to ensure that the integrity of the games we love was never compromised. That is why I believe the time is now to establish a strong national integrity standard for sports betting that will protect consumers and the games themselves from corruption.”²³⁸ Leagues, such as the NFL, PGA, MLB, NHL, and NBA, have sought a uniform set of rules as opposed to the patchwork of laws currently differing in each state.²³⁹ Most importantly, regarding the issues presented in this note, “the federal bill also would create a National Sports Wagering Clearinghouse to receive and share sports wagering data and suspicious transaction reports among sports wagering operators, state regulators, sports organizations, and federal and state law enforcement.”²⁴⁰ Schumer and Hatch admitted this bill is a placeholder and the result of major efforts since the *Murphy* decision.²⁴¹

CONCLUSION

With the introduction of the Sports Wagering Market Integrity Act and the proposal of a National Clearinghouse, sports betting is trending towards a federal regulatory framework. Federal regulators cannot lose sight of pressing issues of cybersecurity within the sports industry and the regulatory bodies most suitable to enforce the integrity and viability of a thriving United States sports betting industry. Both the SEC and FTC, federal regulatory agencies, have the expansive power to conduct investigations and bring both civil actions in federal court or administrative actions through their Division of Enforcement.²⁴² These government agencies have the expertise and the proper resources to protect consumers and the markets. The federal regulatory framework incorporating aspects of the SEC and FTC to “administer the law, promulgate and enforce regulations, and coordinate regulation with states”²⁴³ will be highly beneficial to an internet and data-driven sports gambling industry. As the sports betting industry continues to grow, a National Sports Wagering Clearinghouse may not be sufficient or possess the necessary authority to prove effective. “It would be unfortunate if the expansion of sports betting in the U.S. were threatened or stunted because of regulatory failings that undermined the integrity of the activity[,]”²⁴⁴ and a federal agency

237. See Parry, *supra* note 235.

238. *Id.*

239. See *id.*

240. *Id.*

241. Senator Schumer and Senator Hatch do not anticipate this bill to pass, but they hope it will be foundational for future work in federally regulating sports betting. *Id.*

242. See *What We Do*, SEC, <https://www.sec.gov/Article/whatwedo.html>. (last visited Nov. 28, 2018); see also *FTC: What We Do*, *supra* note 154.

243. Miller & Cabot, *supra* note 153, at 171.

244. *Id.* at 183.

dedicated to sports wagering, like an SEC to the securities or FTC to consumer protection, will provide proper safeguards.

*William H. Williams**

* B.A., Bard College, 2014; M.A. Seton Hall University, 2016; J.D. Candidate, Brooklyn Law School, 2020. Thank you to the Brooklyn Journal of Financial, Corporate, and Commercial Law staff, especially Caitlin, Echo, and Krista, for their tireless work and feedback. I appreciate my parents forwarding all articles about sports gambling throughout the process. Lastly, thank you to Joanna Regan for the support.

BROOKLYN LAW SCHOOL FACULTY 2018–2019

Faculty Emeriti

RICHARD ALLAN, B.A., LL.B., Professor of Law Emeritus
URSULA BENTELE, B.A., J.D., Professor of Law Emerita
JOSEPH CREA, B.A., J.D., LL.M., LL.D., Professor of Law Emeritus
MARY FALK, B.A., J.D., Associate Professor of Legal Writing Emerita
LINDA FELDMAN, B.A., M.A., J.D., Associate Professor of Academic Support Emerita
MARTIN HAUPTMAN, LL.B., LL.M., Professor of Law Emeritus
WILLIAM HELLERSTEIN, B.A., J.D., Professor of Law Emeritus
BAILEY KUKLIN, B.S., J.D., Professor of Law
GARY MINDA, B.A., M.A., S.J.D., Professor of Law Emeritus
ARTHUR PINTO, A.B., J.D., Professor Law
GARY SCHULTZE, B.A., J.D., Professor of Law Emeritus
JOAN G. WEXLER, B.S., M.A.T., J.D., Dean & President Emerita

Faculty

NICHOLAS ALLARD, B.A., B.A./M.A., J.D., President & Joseph Crea Dean and Professor of Law
WILLIAM ARAIZA, B.A., M.S., J.D., Professor of Law
JULIAN ARATO, B.A., M.Phil., J.D., LL.M., J.S.D., Assistant Professor of Law
CAMERON W. ARNOLD, B.A., M.A., J.D., Assistant Professor of Legal Writing
JONATHAN ASKIN, A.B., J.D., Professor of Clinical Law
MIRIAM BAER, A.B., J.D., Professor of Law
JODI S. BALSAM, B.A., J.D., Associate Professor of Clinical Law
CHRISTOPHER BEAUCHAMP, B.A., M.Phil., Ph.D., Professor of Law
DEBRA BECHTEL, B.A., J.D., Associate Professor of Clinical Law
ANITA BERNSTEIN, B.A., J.D., Anita and Stuart Subotnick Professor of Law
BRADLEY BORDEN, B.B.A., M.B.A., J.D., LL.M., Professor of Law
DANA BRAKMAN REISER, B.A., J.D., Professor of Law
HEIDI BROWN, B.A., J.D., Associate Professor of Law
I. BENNETT CAPERS, B.A., J.D., Stanley A. August Professor of Law
STACY CAPLOW, B.A., J.D., LL.M., Associate Dean of Professional Legal Education and Professor of Law
NATALIE CHIN, B.S., J.D., Assistant Professor of Clinical Law
NEIL B. COHEN, S.B., J.D., Jeffrey D. Forchelli Professor of Law
STEVEN DEAN, B.A., J.D., Vice Dean and Professor of Law
SHANE DIZON, B.A., J.D., Associate Professor of Academic Success and Director of the Academic Success Program
ROBIN EFFRON, B.A., J.D., Professor of Law
ELIZABETH FAJANS, B.A., M.A., Ph.D., Associate Professor of Legal Writing
JAMES FANTO, B.A., M.A., Ph.D., J.D., Gerald Baylin Professor of Law
NINA FARBER, B.A., J.D., Assistant Professor of Legal Writing
MARYELLEN FULLERTON, B.A., J.D., Professor of Law
MARSHA GARRISON, B.A., J.D., Suzanne J. and Norman Miles Professor of Law

MICHAEL GERBER, B.A., J.D., Professor of Law
HEIDI GILCHRIST, B.A., J.D., Assistant Professor of Legal Writing
CYNTHIA GODSOE, A.B., J.D., Associate Professor of Law
JOEL GORA, B.A., LL.B., Professor of Law
SUSAN GREENE, B.A./B.S., J.D., Assistant Professor of Legal Writing
SUSAN HAZELDEAN, B.A., J.D., Assistant Professor of Law
SUSAN HERMAN, B.A., J.D., Centennial Professor of Law
EDWARD JANGER, B.A., J.D., David M. Barse Professor of Law
BERYL JONES-WOODIN, B.A., J.D., Professor of Law
JOY KANWAR, B.A., J.D., M.S.E.L, Assistant Professor of Legal Writing
ROBERTA KARMEL, B.A., LL.B., Centennial Professor of Law
ADAM KOLBER A.B., J.D., Professor of Law
MINNA KOTKIN, A.B., J.D., Professor of Law
NOAH KUPFERBERG, A.B., J.D., Assistant Professor of Legal Writing
BRIAN LEE, B.A., M.A., Ph.D., J.D., Professor of Law
GREGG MACEY, B.A., M.A., J.D., Ph.D., Professor of Law
KATE MOGULESCU, B.A., J.D., Assistant Professor of Law
CHRISTINA MULLIGAN, B.A., J.D., Associate Professor of Law
AMY MULZER, B.A., J.D., Instructor of Clinical Law
SAMUEL MURUMBA, LL.B., LL.M., Ph.D., Professor of Law
MINOR MYERS, B.A., J.D., Professor of Law
KAREN PORTER, B.A., M.S., J.D., Associate Professor of Clinical Law
K. SABEEL RAHMAN, A.B., M.Sc & M.St., J.D., Ph.D., Assistant Professor of Law
DAVID REISS, B.A., J.D., Professor of Law
JAYNE RESSLER, B.A./B.S., J.D., Associate Professor of Law
ALICE RISTROPH, B.A., J.D., Ph.D., Professor of Law
ELIZABETH SCHNEIDER, B.A., M.Sc., J.D., Rose L. Hoffer Professor of Law
JOCELYN SIMONSON, B.A., J.D., Assistant Professor of Law
JANET SINDER, A.B., J.D., M.S., Director of the Library and Professor of Law
LAWRENCE SOLAN, B.A., Ph.D., J.D., Don Forchelli Professor of Law
ALEX STEIN, LL.B., LL.M., Ph.D., Professor of Law
WINNIE TAYLOR, B.A., J.D., LL.M., Professor of Law
CARRIE TEITCHER, B.A., J.D., Assistant Professor of Legal Writing
MARIA TERMINI, B.A., M.A., J.D., Assistant Professor of Legal Writing
AARON TWERSKI, B.S., J.D., Irwin and Jill Cohen Professor of Law
MARJORIE S. WHITE, A.B., J.D., Associate Professor of Clinical Law

Visiting Faculty

LAUREN FIELDER-REDMAN, B.A., LL.M., J.D., Visiting Associate Professor of Law
YEHONATAN GIVATI, Ph.D., S.J.D., LL.M., M.A., LL.B., Visiting Associate Professor of Law
MEG HOLZER, B.A., J.D., Visiting Assistant Professor of Legal Writing
CATHERINE KIM, B.A., J.D., Visiting Associate Professor of Law

STEPHAN LANDSMAN, B.A., J.D., Visiting Professor of Law
GABRIELLE MARSHALL, B.A., J.D., Visiting Assistant Professor of Legal Writing
CHRISTOPHER MICHAELSEN, LL.M., PhD, Visiting Adjunct Professor of Law
THANE PITTMAN, B.A., M.A., Ph.D., Visiting Professor of Law
CARMEN MARIA REY, B.A., J.D., Visiting Assistant Professor of Clinical Law
ALLAN J. SAMANSKY, B.A., M.A., J.D. Visiting Professor of Law
CECILIA A. SILVER, A.B., M.St., J.D., Visiting Assistant Professor of Legal Writing

Librarians

JUDY BAPTISTE-JOSEPH, B.A., M.L.S., Cataloging Librarian
CAROLYN J. BROWN, B.A., M.L.I.S., J.D., Reference Librarian and Adjunct Professor of Law
KATHY DARVIL, A.B., M.S.I., J.D., Access Services/Reference Librarian
and Adjunct Professor of Law
JEAN J. DAVIS, B.A., J.D., M.S.L.I.S., Associate Librarian for International Law
and Adjunct Professor of Law
JEFF GABEL, B.F.A., M.F.A., M.L.I.S., Catalog & E-Resources Manager
LOREEN PERITZ, B.A., J.D., M.S.L.I.S., Reference Librarian and Adjunct Professor of Law
SUE SILVERMAN, B.A., J.D., M.L.I.S Reference Librarian and Adjunct Professor of Law
JANET SINDER, A.B., J.D., M.S., Director of the Library and Professor of Law
ERIC YAP, A.B., J.D., M.I.M, M.L.I.S., Reference Librarian
HAINAN YU, B.A., M.S., Systems Librarian

BROOKLYN LAW SCHOOL BOARD OF TRUSTEES

2018–2019

STUART SUBOTNICK '68

Chairman of the Board
President and Chief Executive Officer
Metromedia Company

FRANCIS J. AQUILA '83

Vice Chairman of the Board
Sullivan & Cromwell, LLP

DAVID M. BARSE '87

DMB Holdings

DENNIS J. BLOCK '67

Senior Chairman
Greenberg Traurig, Global Mergers and Acquisitions Practice

FREDERICK COHEN '67

Duane Morris, LLP

FREDERICK CURRY '03

Deloitte Financial Advisory Services, LLP

JEFFREY J. FEIL '73

President and Chief Executive Officer
The Feil Organization

MARTIN A. FISCHER '64

West Center Associates

JEFFREY D. FORCHELLI '69

Forchelli, Deegan, Terrana, LLP

DEBRA HUMPHREYS '84

Founder & Chair of the Board of Trustees
Thomas Jefferson Independent Day School

ROBERT M. KAUFMAN '57

Proskauer Rose, LLP

HON. CLAIRE KELLY '93

Judge
U.S. Court of International Trade

EILEEN T. NUGENT '78

Skadden, Arps, Slate, Meagher & Flom, LLP

JOHN P. OSWALD '84

President and Chief Executive Officer
Capital Trust Group

HON. RAMON E. REYES, JR. '92

Judge
U.S. District Court, Eastern District of NY

STEVEN G. SCHEINFELD '85

Fried, Frank, Harris, Shriver & Jacobson, LLP

LAWRENCE A. SUCHAROW '75

Co-Chairman

Labaton Sucharow

STEVEN L. ZELKOWITZ

Chief Executive Officer

Sycamore Energy Consulting

Recent Graduate Trustee Members

ANNA ASHUROV '12

Vice President, Financing Group
Goldman Sachs

AN DUONG '12

Vice President, Head of Strategy & Analytics
Operational Risk Assurance
Bank of New York Mellon

Members Emeriti

ROBERT B. CATELL

Chairman
Advanced Energy Research and Technology Center (AERTC) at
New York State University at Stony Brook

FRANCES MARGOLIS FRIEDMAN '39

FLORENCE SUBIN '75

