NEW YORK UNIVERSITY

JOURNAL OF INTELLECTUAL PROPERTY AND ENTERTAINMENT LAW

VOLUME 8 FALL 2018 NUMBER 1

USING THE ECONOMIC ESPIONAGE ACT TO PROTECT TRADE SECRETS IN BASEBALL

BRETTE TROST*

In 2016, Christopher Correa, a former employee of the St. Louis Cardinals, was sentenced to forty-six months in prison for violating the Computer Fraud and Abuse Act when he accessed a Houston Astros database without authorization. However, these were not the only charges Correa could have faced. This note uses the Correa case to illustrate how the Economic Espionage Act can be used to prevent trade secret theft in Major League Baseball. More specifically, this note asserts that the sabermetric data systems used by MLB teams to evaluate and track players are legally protectable trade secrets. Furthermore, due to the fluid nature of the baseball analytics talent pool and barriers to civil prosecution inherent in baseball's structure, the Economic Espionage Act presents the best way to combat the misappropriation of this information. The note goes on to distinguish between teams' off-field and on-field tactics and discusses how, if at all, this framework should apply to the collection and use of biometric data.

INTRODUCTION

Sports are the paradigm of competition. They are perhaps the arenas of business in which winning is most objectively quantifiable and competition is on display every night. On the field, competitive tactics are expected and gamesmanship is routine. Yet behind the scenes, there is an army of data scientists who are competing in their own way. Their competition does not revolve around which team collects the most runs after nine innings but rather around who can discover the most effective means of evaluating the players on the field.

This facet of the game is no secret. However, the extent to which some are willing to go to gain a competitive edge became strikingly apparent in 2016, when Christopher Correa, a member of the St. Louis Cardinals' baseball operations staff, received a forty-six-month prison sentence for hacking into a Houston Astros' database.[1] The database, known as "Ground Control," was built by the Astros' baseball operations department to house scouting reports, trade discussions,

---

* J.D. Candidate, New York University, 2019; B.A., English, University of Pennsylvania, 2013. The author would like to thank Professor Harry First for his expertise and guidance.

[1] Judgement in a Criminal Case at 1-3, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016).

proprietary statistical analysis, injury histories, projections for players, contract information, and more.[2]

Major League Baseball ("MLB") has undergone a major transformation over the last two decades. A game that once largely relied on subjective analyses and gut instincts to assess players, professional baseball—through the collection and study of statistical data—is now obsessed with an objective search for truth.[3] This objective analysis, or sabermetrics as it is commonly known, began as a hobby held by a few people scattered throughout the baseball world,[4] but it has since turned into an industry-wide practice, rapidly becoming the fixation of nearly every team in the league.[5] Teams now hire the most technical and scientific minds in the country, such as NASA engineers, data scientists from leading statistical software companies, and PhDs in cognitive neuroscience, applied statistics, and machine learning, in order to gain any slight competitive edge in discovering the most intricate details of a player's ability.[6]

Sabermetrics, named after the Society of American Baseball Research ("SABR"), is defined as "advanced statistical collection and analysis to develop objective knowledge about baseball for use in player evaluation and tactical decision-making."[7] Collecting certain statistics, such as batting average and earned run average, has been a part of the game since baseball's inception.[8] However, for

---

[2] Evan Drellich, *Astros' Formula for Success Builds on Its Own Data Bank*, HOUS. CHRON. (Mar. 10, 2014, 9:00 AM), http://www.houstonchronicle.com/sports/astros/article/Astros-formula-for-success-builds-on-its-own-5300746.php.

[3] *See generally* Leigh Steinberg, *Changing the Game: The Rise of Sports Analytics*, FORBES (Aug. 18, 2015, 3:08 PM), https://www.forbes.com/sites/leighsteinberg/2015/08/18/changing-the-game-the-rise-of-sports-analytics/#638221644c1f (describing analytics as the "present and future of professional sports" and that any team not using them is at a "competitive disadvantage").

[4] Lara Grow & Nathaniel Grow, *Protecting Big Data in the Big Leagues: Trade Secrets in Professional Sports*, 74 WASH. & LEE L. REV. 1567, 1575 (2017) [hereinafter Grow & Grow] ("[P]ractically every team in MLB today utilizes sabermetric principles to at least some extent . . . .").

[5] *Id.*

[6] Ben Baumer, *In a Moneyball World, a Number of Teams Remain Slow to Buy into Sabermetrics*, MLB article within *The Great Analytics Rankings*, ESPN (Feb. 23, 2015), http://www.espn.com/espn/feature/story/_/id/12331388/the-great-analytics-rankings#.

[7] R. Mark Halligan & Matthew J. Frankel, Nixon Peabody CLE Presentation: Secret Sabermetrics: Trade Secret Protection in the Baseball Analytics Field (Apr. 9, 2012), https://nixonpeabody.adobeconnect.com/_a769300970/p25o1a1pgvg/.

[8] Grow & Grow, *supra* note 4, at 1571-72 ("As early as 1845 . . . newspapers began printing box scores recapping the statistical achievement of players in amateur baseball contests.").

most of the twentieth century, the examination of more granular data was only performed by "amateur statisticians from outside the baseball establishment" and "statistically-inclined fans."[9] By the end of the century, several companies, such as Baseball Prospectus and STATS LLC, began to collect more extensive data, including the speed and type of every pitch thrown during a game. Nonetheless, while baseball has been played in the United States since 1840, it was not until 2003, when Michael Lewis published the book *Moneyball: The Art of Winning an Unfair Game*,[10] that baseball industry insiders awoke to the potential of using analytical techniques to assess talent. Lewis' book focused on one team, the Oakland Athletics, as it embarked on what was seen at the time as a unique and innovative process.[11] Now, every team relies at least to some extent on the use of analytics.[12]

Baseball teams own many of the same types of information as that which traditional businesses own, such as customer lists, pricing data, and marketing strategies. These categories of information are generally considered trade secrets when companies take reasonable measures to protect them.[13] Unlike traditional businesses, however, teams collect and store a plethora of data specific to the baseball industry, including statistical analyses (such as compilations and algorithms for new metrics),[14] scouting reports, trade proposals or discussion notes, playbooks, verbal or hand signals used on the field, player skill techniques, player training techniques, dietary and nutritional regimens, physical therapy techniques, psychological assessment techniques, and biometric analyses.[15] Many people in the

[9] *Id.* at 1574, 1575.

[10] MICHAEL LEWIS, MONEYBALL: THE ART OF WINNING AN UNFAIR GAME (2003).

[11] Grow & Grow, *supra* note 4, at 1575.

[12] *Id.* ("[P]ractically every team in MLB today utilizes sabermetric principles to at least some extent . . . .").

[13] *See* United States v. Nosal, 844 F.3d 1024, 1042-43 (9th Cir. 2016) (customer lists), In re Dana Corp., 574 F.3d 129, 152 (2d Cir. 2009) (pricing data), Optic Graphics, Inc. v. Agee, 591 A.2d 578, 586 (Md. Ct. Spec. App. 1991) (marketing strategies).

[14] Statistical analyses include, for example, the calculation of probabilities for defensive positioning, which has led to the proliferation of the infield shift. The infield shift typically involves moving infielders away from their standard positions to better account for a batter's tendency to put the ball in play on one side of the field. For a brief discussion of the infield shift, see David Waldstein, *Who's on Third? In Baseball's Shifting Defenses, Maybe Nobody*, N.Y. TIMES (May 12, 2014), https://www.nytimes.com/2014/05/13/sports/baseball/whos-on-third-in-baseballs-shifting-defenses-maybe-nobody.html.

[15] *See* Grow & Grow, *supra* note 4, at 1605 (surveying the general counsels of teams across the four professional sports as to what categories of information they deem be trade secrets).

baseball industry assert that such baseball-specific-data, which teams store and collect, constitute trade secrets.[16]

Despite the many potential trade secrets, there have not been any cases that discuss what material qualifies as a trade secret in baseball. Although Correa misappropriated information from Ground Control, a system that housed almost all of the Astros' proprietary information, Correa was instead prosecuted under the Computer Fraud and Abuse Act (CFAA)[17] for hacking Ground Control.[18] What was criminalized was the fact that he accessed the information "without authorization,"[19] not the misappropriation of the information he obtained, and likely used, from the hacking. Due to the lack of court decisions (criminal or civil), there is no direct precedent holding that these types of analytics databases are in fact trade secrets. Nor is there extensive analysis of how teams keep this data secret and whether those controls are effective. Further, strategies the industry and public accept as part of the competitive nature of sports, such as on-field tactics to gain a competitive advantage like "stealing signs," could be more intensely scrutinized if the legal system is used to police what should be considered fair competition in baseball.

Part I of this note will argue that the sabermetric data systems used by MLB teams to evaluate and track players are legally protectable trade secrets. Part II will examine the fluid nature of the baseball analytics talent pool, and will suggest that because of this aspect of the industry, the best way to prevent the misappropriation of these trade secrets is through criminal prosecution under the Economic Espionage Act of 1996 (EEA).[20] Part III will discuss on-field strategies, arguing that although the improper acquisition of on-field plays through tactics like sign-stealing may, in

---

[16] *See id.*; *see also* Rich Lederer, *An Unfiltered Interview with Nate Silver*, BASEBALL ANALYSTS (Feb. 12, 2007), http://baseballanalysts.com/archives/2007/02/an_unfiltered_i.php (referring to the detailed formulas in Nate Silver's analytics system, PECOTA, as a trade secret); Jenny Vrentas, *Mets Statistical Analyst Has Seen Growth and Evolution of Sabermetrics in MLB*, STAR-LEDGER (Apr. 23, 2010), http://www.nj.com/mets/index.ssf/2010/04/mets_statistical_analyst_has_s.html (quoting Ben Baumer saying teams are guarded about the statistical analyses they engage in because "it's trade secrets").

[17] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

[18] Information at 2, 5, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016) (charging Correa with violating 18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(iii)).

[19] 18 U.S.C. § 1030(a)(2)(C) ("Whoever intentionally accesses a computer without authorization . . . and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.").

[20] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended at 18 U.S.C. §§ 1831-1839).

certain cases, technically meet the definition of theft of trade secrets under the EEA, this behavior does not warrant the imposition of criminal sanctions. Finally, Part IV will briefly analyze future questions on the proprietary nature of baseball data, noting that the focus will be less on sabermetric statistical systems and more on the collection, compilation, and ownership of biometric data.

I.
TRADE SECRET LAW AND ITS APPLICATION IN BASEBALL[21]

Since teams deal with many different types of information, Lara and Nathaniel Grow surveyed the general counsels of teams across the four major North American professional sports leagues—baseball, basketball, football, and hockey—on what they believed to be trade secrets.[22] The survey, which received responses from nineteen teams, including two in MLB, revealed that 89.47% claimed that their scouting reports were trade secrets, 78.95% asserted trade secret protection over trade proposal or discussion notes, 73.68% asserted trade secret protection over statistical analyses, and 52.63% asserted trade secret protection over player skill development techniques and biometric analyses.[23] Variations among the general counsels' responses is likely due to the different information-collection practices between the four major North American sports leagues—that is, differences in the amount and type of data collected in one sport compared to the other three sports and differences in how biometric data is relied upon in one sport compared to the other three sports.[24]

---

[21] This will examine only trade secret law in the United States. There is one baseball team in Canada, the Toronto Blue Jays, and thus Canadian law could be implicated. However, for the purposes of this paper, only provisions of U.S. law will be examined. For a brief summary of Canadian trade secret protection in this context, see Grow & Grow, *supra* note 4, at 1599-1601.

[22] Grow & Grow, *supra* note 4, at 1605.

[23] *Id.*

[24] Of the nineteen respondents, two responses came from MLB, seven from the NBA, four from the NFL, and six from the NHL. Each sport has different approaches to the use of data, specifically biometric data. Players in the NHL, NBA, and NFL have been more outspoken with privacy concerns relating to the collection of biometric data and have sought to restrict the use of biometric devices during games. *See, e.g.*, Jeremy Venook, *The Upcoming Privacy Battle over Wearables in the NBA*, ATLANTIC (Apr. 10, 2017), https://www.theatlantic.com/business/archive/2017/04/biometric-tracking-sports/522222/. When it comes to collecting analytical material in general, sports have relied on analytics at different paces. For example, the NFL has "lagged behind other professional leagues amid an otherwise widespread analytics revolution . . . ." Kevin Clark, *NFL's Brewing Information War*, RINGER (June 22, 2016, 1:13 PM), https://www.theringer.com/2016/6/2/16077478/nfl-information-war-data-advanced-stats-73b6eee2d39f.

Given the general counsels' apparent zeal for believing that their scouting reports, trade proposals and discussion notes, statistical analyses, player skill development techniques, and biometric analyses constitute trade secrets,[25] it is worthwhile to analyze whether such information actually satisfies the EEA's requirements for trade secret protection. Using baseball as a case study, this note begins by exploring whether sabermetric data systems fall within the EEA.

Under the EEA, a trade secret is defined as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible," provided that the "owner . . . has taken reasonable measures to keep such information secret," and the information "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable . . . by, another person who can obtain economic value from the disclosure or use of the information."[26] While people in the baseball industry have asserted that the data they collect and the systems they create are trade secrets,[27] there are almost no legal precedents that deal directly with this issue. Though Correa was not charged with violating any trade secret laws, his case provides insight into how baseball data could be subject to trade secret protection and potential criminal prosecution. This note argues that much of the content stored on sabermetric data systems, especially scouting reports and statistical analyses of player talent, can and should receive trade secret protection under the EEA.

A. An Overview of Trade Secret Law

Though laid out in its current form above, how the law, specifically the criminal law, defines a trade secret has changed over the last decade. To help clarify and strengthen trade secret protection, Congress amended the EEA through the enactment of the Theft of Trade Secrets Clarification Act of 2012[28] and the Defend Trade Secrets Act of 2016 (DTSA).[29]

---

[25] Grow & Grow, *supra* note 4, at 1605.

[26] 18 U.S.C. § 1839(3) (2012 & Supp. IV 2017).

[27] *See* Lederer, *supra* note 16 (referring to the detailed formulas in Nate Silver's analytics system, PECOTA, as a trade secret); Vrentas, *supra* note 16 (quoting Ben Baumer saying teams are guarded about the statistical analyses they engage in because "it's trade secrets").

[28] Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627 (codified as amended at 18 U.S.C. § 1832(a) (2012)).

[29] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended in scattered sections of 18 U.S.C.).

In 1996, Congress passed the Economic Espionage Act to fill a hole in the statutory scheme. Lawmakers recognized the necessity of protecting the intangible assets of companies in the United States in response to the challenges prosecutors faced in fitting the misappropriation of these assets into statutes like mail and wire fraud,[30] the National Stolen Property Act,[31] and the CFAA, which were not designed for this type of prosecution.[32] President Bill Clinton acknowledged a growing need for a statute dedicated solely to the protection of these assets through the criminal law, noting that "[t]rade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States."[33]

The EEA provides a fine, a prison sentence of up to ten years, or both for individuals who steal or without authorization appropriate trade secrets as follows:

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly steals, or without authorization appropriates . . . such information . . . shall . . . be fined under this title or imprisoned not more than 10 years, or both.[34]

Much of the jurisprudence that defines trade secrets relies on interpretations under the Uniform Trade Secrets Act (UTSA),[35] a model state law which as of January 2019 has been adopted in forty-seven states and the District of Columbia.[36] The UTSA and EEA provide largely identical definitions of a trade secret, especially

---

[30] *See* 18 U.S.C. § 1341, 1343 (2012) (mail and wire fraud).

[31] 18 U.S.C. §§ 2314-2315.

[32] *See* R. Mark Halligan, *Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 14 J. MARSHALL REV. INTELL. PROP. L. 476, 480 (2015) ("Before the EEA, federal prosecutors relied primarily upon the National Stolen Property Act and the wire and mail fraud statutes to commence criminal prosecutions for trade secret theft. Both statutes were ineffective." (citation omitted)).

[33] *Id.* at 480-81.

[34] 18 U.S.C. § 1832(a).

[35] UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 438 (1990).

[36] *Trade Secrets Act*, UNIFORM LAW COMMISSION, https://my.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 (last visited Jan. 2, 2019).

following the enactment of the DTSA.[37] Judicial interpretations of trade secrets under the UTSA have provided a body of case law to guide the interpretation of the EEA.[38]

B. Definition of Trade Secrets Under the EEA

In order to be a trade secret under the EEA, the prosecutor or plaintiff must show three distinct elements: (i) the alleged trade secret falls within a listed type of information; (ii) the owner has taken "reasonable measures" to keep that information secret; and (iii) the information derives "independent economic value" from not being generally known or ascertainable through "proper means."[39]

The threshold element, that the alleged trade secret falls within a listed type of information, is fairly simple to meet.[40] To fall within the EEA, the alleged trade secret must be "financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible."[41]

In *Nat'l Football Scouting, Inc. v. Rang*,[42] the U.S. District Court for the Western District of Washington addressed the question of whether scouting reports fall within the listed types of information. *Rang* is the "only reported court decision considering the status of proprietary sports-related knowledge under trade secrecy law."[43] In that case, National Football Scouting, Inc. ("National") sued Robert Rang, a part-time sportswriter, and the website for which he wrote, Sports Xchange, for

---

[37] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended in scattered sections of 18 U.S.C.).

[38] *See, e.g.*, United States v. Chung, 659 F.3d 815, 825 (9th Cir. 2011) ("[W]e consider instructive interpretations of state laws that adopted the UTSA without substantial modification."); *see also* United States v. Hanjuan Jin, 833 F. Supp. 2d 977, 1007 n.3 (N.D. Ill. 2012) ("Although there are some differences between the definitions of a trade secret found in the UTSA and the EEA, the Court also considers cases that have interpreted the requirements for a trade secret under state law based on the UTSA.").

[39] 18 U.S.C. § 1839(3).

[40] See Rice Ferrelle, *Combatting 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, 164-65, 168-69 (2003), (listing some of the more obscure types of information that have been considered trade secrets under state law, including "a method of producing unique watercolor paintings," "techniques for personal spiritual advance," and a "technique for barbecuing meats").

[41] 18 U.S.C. § 1839(3).

[42] Nat'l Football Scouting, Inc. v. Rang, 912 F. Supp. 2d 985 (W.D. Wash. 2012).

[43] Grow & Grow, *supra* note 4, at 1617.

copyright infringement and misappropriation of trade secrets under the UTSA. National's business involved providing scouting reports to NFL teams. The reports were compiled and produced by National's own scouts. Twenty-one NFL teams had each paid $75,000 for access to the reports. The reports assigned each player an overall "Player Grade," which was "a numerical expression representing National's opinion of the player's likelihood of success in the NFL."[44] National sued Rang for writing articles which disclosed the Player Grades.

Rang argued that the Player Grades did not qualify as "information" within the meaning of the UTSA because they were subjective opinions, rather than "factual information."[45] The court rejected this argument, saying "the fact that National has assigned a Player Grade to a certain player is not an idea or opinion."[46] Instead, the Player Grades constituted "information" under the statute.[47] The court believed a factual dispute existed as to whether National reasonably kept the information secret and whether the grades had an independent economic value. This, the court held, was a question for the trier of fact. Ultimately, the parties settled.[48]

While the court held that the Player Grades were "information" under the UTSA, it did not take a stance on whether the reports would have constituted "information" had they merely comprised a scout's thoughts on a given player, rather than assigning a Player Grade. It is common practice for scouts to provide a numerical grade when assessing baseball players.[49] However, would scouting reports which lack numerical player values also qualify as "information" under the EEA? The plain meaning of the term "information" and the function of scouting information in relation to the business of running a professional sports team suggest that scouting reports which lack numerical player values would likely still qualify as "information" under the EEA.[50]

---

[44] *Rang*, 912 F. Supp. 2d at 988.

[45] *Id.* at 995.

[46] *Id.* at 996.

[47] *Id.*

[48] Matthew J. Frankel, *Hackers Strike Out: Recent Cases of Alleged Sports Analytics IP Theft*, 1 J. SPORTS ANALYTICS 83, 85 (2015).

[49] Alan Siegel, *Baseball Scouts Use Numbers, Too*, FIVETHIRTYEIGHT (Aug. 11, 2014, 9:40AM), https://fivethirtyeight.com/features/baseball-scouts-use-numbers-too/.

[50] *See* N. Highland, Inc. v. Jefferson Mach. & Tool, Inc., 898 N.W.2d 741, 768. (Wis. 2017) ("Dictionary definitions of 'information' suggest that the term encompasses a broad class of knowledge.").

The compilation of baseball statistics would also qualify as "information"' under the EEA. For example, Inside Edge, a baseball analytics company,[51] reviews at-bats of every player to identify and compile specific indicia useful in determining what percentage of those at-bats lead to "well-hit" balls.[52] The EEA expressly includes "compilations," as long as they meet the statute's other prerequisites. Further, the "method" of compiling that data (i.e., through algorithms and code) and the "design" of that information, are also types of information listed in the EEA's definition of a trade secret.[53] Finally, most of these analyses are performed with the aid of proprietary computer programs, which would undoubtedly qualify.

Under the EEA, the second element to qualify as a trade secret is that the owner must take "reasonable measures"[54] to keep the information secret. The DTSA addresses from whom the information must be kept secret to qualify as a trade secret under the EEA. Originally, the EEA stated that the information must be kept secret from "the public."[55] The DTSA made the definition identical to the UTSA, such that the information must be kept secret from "another person who can obtain economic value" from the disclosure.[56] This narrowed the scope of the provision, as there might be information that is commonly known within an industry but not known to the public.[57]

What qualifies as a "reasonable measure"[58] to keep information secret? Determining reasonableness usually takes the form of cost-benefit analysis to find the optimal level of precaution that is not overly burdensome given the risk.[59] Although this would be fact-specific to each case, media reports reveal that teams

---

[51] As of May 2018, twenty of the thirty MLB clubs used Inside Edge's analytics services. *See* Jeff Arnold, *Remarkable Brings Sports Data to Life, One Stat at a Time*, SPORTTECHIE.COM (May 31, 2018), https://www.sporttechie.com/inside-edge-sports-data-app-remarkable-translates-stats/.

[52] Alan Schwartz, *Score That a Hit (But Was It Well Hit?)*, N.Y. TIMES (Oct. 22, 2006), http://www.nytimes.com/2006/10/22/sports/baseball/22score.html.

[53] 18 U.S.C. § 1839(3) (2012).

[54] *Id.*

[55] Economic Espionage Act of 1996, Pub. L. No. 104-294, § 101(a), 110 Stat. 3488 (codified as amended at 18 U.S.C. § 1839(3)(B)).

[56] Defend Trade Secrets Act of 2016 § 2(b)(1)(A), 18 U.S.C. § 1839(3)(B) (2012 & Supp. IV 2017).

[57] Adam Cohen, *Feature: Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act After* United States v. Aleynikov, 30 YALE J. ON REG. 189, 204 (2013) ("Insiders in a business are considerably more likely to know about particular processes and methods than is the public.").

[58] 18 U.S.C. § 1839(3)(A).

[59] Grow & Grow, *supra* note 4, at 1585.

use the same types of protections as other businesses in securing their materials, such as "walling off" information from those who do not need to know it, using computer security methods (i.e., passwords, firewalls, and surveillance), and having employees sign non-disclosure or non-compete agreements.[60] Contractual provisions can be especially important in this analysis, as a lack of a non-disclosure agreement "may alone defeat [a] trade secret claim."[61]

Under the EEA, the third requirement for qualifying as a trade secret is that the information's economic value derives from the fact that it is not "generally known to" or "readily ascertainable" by "another person who can obtain economic value" from the information.[62] Detailed scouting reports, statistical analysis, and other means of player evaluation help teams create a more competitive product on the field. If another team gains access to these methods of evaluation, it could recreate them at a lower cost. If a team knows what strategy its competitor is going to use, it could more precisely tailor its own strategy. If a competitor knows which players a team values via its scouting reports or the type of statistics the team measures, it could use that in trade negotiations or adopt those strategies if they prove successful and recognize talent before others. To a certain extent, the foregoing relies on the assumption that a more competitive team will lead to a more profitable franchise. Although this metric is slightly undercut by the fact that teams operate as part of a league, which has revenue sharing and as a whole may benefit from a more even playing field,[63] given the expenditures teams make on personnel to create analytics databases[64] and the fact that there are individual revenue streams that

---

[60] *See id.* at 1606 (survey finding that 94.74% of teams used computer security methods, 94.74% used non-disclosure agreements, and 78.95% used non-competes); *see also* Thomas Gorman, *Prospectus Q&A: Mark Johnson*, BASEBALL PROSPECTUS (May 11, 2005), https://www.baseballprospectus.com/news/article/4024/prospectus-qa-mark-johnson/ (referencing the Cardinals' Mark Johnson's non-disclosure agreement); Jon Greenberg, *Q&A: New Cubs 'Saberist' Tom Tango*, ESPN (Jan. 30, 2013), http://www.espn.com/blog/chicago/cubs/post/_/id/14619/qa-new-cubs-saberist-tom-tango (noting the Chicago Cubs' Tom Tango's non-disclosure agreement); Jack Moore, *How Wall Street Strangled the Life out of Sabermetrics*, VICE SPORTS (Oct. 22, 2014, 5:30 AM), https://sports.vice.com/en_us/article/aem895/how-wall-street-strangled-the-life-out-of-sabermetrics (discussing how Andrew Friedman's consultants at the Tampa Bay Rays were "greeted by non-disclosure agreements).

[61] Halligan & Frankel, *supra* note 7.

[62] 18 U.S.C. § 1839(3)(B).

[63] J.C. Bradbury, *Encouraging the Poor to Stay Poor*, N.Y. TIMES (Aug. 28, 2010), http://www.nytimes.com/2010/08/29/sports/baseball/29score.html.

[64] For example, the Los Angeles Dodgers paid Andrew Friedman, their President of Baseball Operations, $35 million. Baumer, *supra* note 6. A team's President of Baseball Operations makes all of the final decisions regarding baseball strategy and talent acquisition and helps to shape the

increase when a team is more competitive,[65] it seems fairly clear that there is economic benefit to having these secret programs.

It may be, at first, counterintuitive to think of scouting reports and sabermetric databases as trade secrets, especially given that all the action being observed and measured occurs in public and is largely preserved on video. However, the fact that the data, in the aggregate, comprises a compilation has important implications for evaluating its secrecy. Although each play is public information, the compilation transforms the constituent parts, which are public, into information that gives the team a competitive advantage and economic benefit, thereby becoming a trade secret.[66]

That is, the analysis that goes into the making of a statistic is what makes it a trade secret. While the Player Grades disseminated in *Rang* and the analysis provided by Inside Edge represent types of analytical compilations accessible to and bought by many teams, teams themselves create closely guarded compilations. For example, the Astros created an algorithm for determining when a player in the minor leagues is ready to be promoted to the major leagues. When the player meets the criteria in the algorithm, a green arrow appears next to that player's name. A grey arrow next to the player signals that the player should be demoted, and a black arrow means the player should be cut.[67] This system is one example of the many ways in

---

analytics department through both hiring personnel and spearheading the development of new analytical tools and programs.

[65] *See* Ferrelle, *supra* note 40, at 166-67 ("[T]eam victories . . . in turn lead[] to increased advertising, television, and radio exposure. This exposure often translates into increased merchandise sales or lucrative media contracts. . . . As a team organization garners more victories, it reaps increased financial rewards."); *see also* 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, 312 (2009) ("Profitability correlates to on-field success.").

[66] *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (AM. LAW INST. 1995) ("[I]t is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of a trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements."); *see also* United States v. Nosal, 844 F.3d 1024, 1042 (9th Cir. 2016) ("The source lists in question are classic examples of a trade secret that derives from an amalgam of public and proprietary source data. To be sure, some of the data came from public sources . . . . But cumulatively, the Searcher database contained a massive confidential compilation of data . . . .").

[67] Joshua Green, *Extreme Moneyball: The Houston Astros Go All in on Data Analysis*, BLOOMBERG BUSINESSWEEK (Aug. 28, 2014, 3:00PM), https://www.bloomberg.com/news/articles/2014-08-28/extreme-moneyball-houston-astros-jeff-luhnow-lets-data-reign.

which teams create their own proprietary trade secrets. The team must decide what data to collect (i.e., speed, direction, distance, angle), how to collect it (human review, cameras, or software), and how to combine and present it (numbers, graphs, charts, graphics, computer programs, or symbols). Scouting reports, even if done through first-hand observation and annotation of results by scouts, contain some of the same compilation features as do statistics (i.e., what attributes of the player to write down and focus on, how to weigh each of those attributes, how to present the report, and how to measure the importance of each individual scouting report when assessing the overall performance of a player within a larger database). The creation of these evaluation systems all required time, money and effort, making them competitively valuable.[68]

C. The Interstate Commerce Requirement and Intent

Once the plaintiff has established that the information at issue is a trade secret, the EEA has two further threshold requirements for criminal prosecution. First, the trade secret must meet the statute's interstate commerce requirement.[69] Second, the prosecution must establish a mens rea requirement—that the actions were taken "with intent."[70]

The interstate commerce requirement of the EEA has been subject to some controversy. As the Act was originally written, the trade secret had to be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[71] The Theft of Trade Secret Clarification Act of 2012 revised this language to its current form, requiring the trade secret to be "related to a product or service used in or intended for use in interstate or foreign commerce."[72] This amendment was passed in response to the Second Circuit's holding in *United States v. Aleynikov*.[73] In *Aleynikov,* a Goldman Sachs employee stole source code for a high-frequency trading system, which was used to make large volumes of trades in securities and commodities. The court held that Aleynikov did not violate the EEA

---

[68] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (AM. LAW. INST. 1995). ("[I[f acquisition of the information through an examination of a competitor's product would be difficult, costly, or time-consuming, the trade secret owner retains protection . . . .").

[69] 18 U.S.C. § 1832(a) (2012) ("Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce . . .").

[70] *Id.*

[71] Economic Espionage Act of 1996, Pub. L. No. 104-294, § 101(a), 110 Stat. 3489.

[72] Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627 (codified as amended at 18 U.S.C. § 1832(a)).

[73] United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012); 158 CONG. REC. H6,848 (daily ed. Dec. 18, 2012) (statement of Rep. Smith).

because the source code did not meet the interstate commerce requirement as it was not "produced for" or "placed in" commerce.[74] Much of the court's reasoning in *Aleynikov* could have applied to the information at issue here (i.e., it was for internal use only and there was no intention to sell or license the product). However, Congress closed this loophole by expanding the statute to cover services (in addition to products) and by broadening the language to include products or services *intended for use* in interstate commerce.[75]

Here, the statistical databases and scouting reports relate to a "product" used in interstate commerce, namely the sport of baseball. Although baseball may not be a product in the tangible sense, it is surely a product in the same way that most forms of viewable entertainment are products. Professional athletes playing baseball is what the teams are marketing and selling to the public. Baseball is intended for public consumption through the attendance of live events and the viewing of television broadcasts. Given the congressional intent to broaden the EEA's interstate commerce requirement, it is not a stretch to say that the systems are intended for use in baseball, which is a product used in interstate commerce. Further, though baseball has historically been subject to an antitrust exemption, which was rooted in a finding that the business of baseball was not a part of interstate commerce,[76] the United States Supreme Court later clarified in *Flood v. Kuhn*[77] that "[p]rofessional baseball is a business and it is engaged in interstate commerce."[78]

Finally, the EEA distinguishes itself from its civil counterpart by including a high mens rea requirement for the remaining elements. The alleged thief must (i) *intend* to convert the trade secret to the economic benefit of someone other than the owner, (ii) *intend* or *know* that the theft will injure the owner of the trade secret, and

---

[74] *Aleynikov*, 676 F.3d at 79-82.

[75] 158 Cong. Rec. H6,848 (daily ed. Dec. 18, 2012) (statement of Rep. Smith) ("The Second Circuit's Aleynikov decision revealed a dangerous loophole that demands our attention. In response, the Senate unanimously passed S. 3642 in November.").

[76] Fed. Baseball Club of Balt. v. Nat'l League of Prof'l Base Ball Clubs, 259 U.S. 200, 208-09 (1922).

[77] Flood v. Kuhn, 407 U.S. 258 (1972).

[78] *Id.* at 282. Though it would likely not be difficult to prove that, despite the antitrust language, the business of baseball is connected to interstate commerce, the fact that this question may be less straightforward and that case law like *Aleynikov* illustrates that this requirement is not something courts are willing to simply look past, prosecutors may be more reluctant to bring charges under the EEA in the context of baseball.

(iii) *knowingly* misappropriate the trade secret through one of the delineated unauthorized acts.[79] Each element requires a fact-specific inquiry.

D. The EEA as Applied to Correa's Case

As suggested above, Correa's case provides an illustration as to how the EEA could apply to trade secrets in baseball. Correa was charged with violating five counts of the CFAA. The application of criminal law to the sports world is neither novel nor extreme, and there have been many other instances in which the government has taken a keen interest in criminal activity in the sports industry. For example, the federal government extensively investigated and prosecuted the use of performance enhancing drugs.[80] The New England Patriots' involvement in the so-called "Spygate" incident garnered significant political interest, with many calling for criminal prosecution.[81] Currently, the Department of Justice is investigating MLB's international signing practices.[82]

Correa worked for the Cardinals from 2009 until he was charged in 2015. During the beginning of his tenure with the Cardinals, Correa worked closely with Jeff Luhnow and Sig Mejdal. His relationship with Mejdal, in particular, was contentious—the two were considered "rivals" who engaged in "heated disputes."[83]

In December of 2011, the Astros hired Luhnow as General Manager. In January of 2012, Luhnow brought Mejdal along to head the Astros' analytics department.[84] Mejdal, a NASA engineer, was brought in to "make sense of all the

---

[79] 18 U.S. Code § 1832(a) ("Whoever, with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly" misappropriates a trade secret through an enumerated act shall be subject to punishment).

[80] *See, e.g.*, *Congress Asks DOJ to Prove Whether Clemens Lied Under Oath*, ASSOCIATED PRESS (Feb. 27, 2008), http://www.espn.com/mlb/news/story?id=3267163; Del Quentin Wilber & Ann E. Marimow, *Roger Clemens Acquitted of All Charges*, WASH. POST (June 18, 2012), https://www.washingtonpost.com/local/crime/roger-clemens-trial-verdict-reached/2012/06/18/gJQAQxvzlV_story.html?noredirect=on&utm_term=.9ee2ce9e4c42.

[81] Horovitz, *supra* note 65, at 324 n.101 ("Given the level of Congressional attention Spygate and other sports stories have received recently, the notion of federal prosecution hardly seems farfetched.").

[82] Jon Werthem, *Exclusive: The Evidence that Persuaded U.S. Department of Justice to Investigate MLB Recruitment of Foreign Players*, SPORTS ILLUSTRATED (Oct. 2, 2018), https:/www.si.com/mlb/2018/10/02/fbi-investigation-mlb-atlanta-braves-los-angeles-dodgers.

[83] *See* Sentencing Memo of the United States at 4, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016).

[84] Brian McTaggert, *Astros Hire Luhnow as General Manager*, MLB (Dec. 8, 2011, 12:10 AM), http://wap.mlb.com/hou/news/article/2011120826126688/; Brian McTaggert, *Analyze This:*

new data that [was] becoming available for assessing ballplayers."[85] When Mejdal left the Cardinals, he was directed to hand over his computer and password to Correa.[86] At the time, the Astros and Cardinals were division rivals.[87] While Luhnow and Mejdal were with the Cardinals, the analytics staff used a database tool called "Red Bird Dog," and Luhnow and Mejdal "had clear ideas of what they wanted after using [that] system."[88] At the Astros, the two went on to build Ground Control, which housed "a variety of confidential data, including scouting reports, statistics, and contract information, all to improve the team's scouting, communication, and decision-making for every baseball-related decision."[89] The system, which takes "variables and weights them according to the values determined by the team's statisticians, physicist, doctors, scouts and coaches," was referred to as the "repository of the organization's collective baseball knowledge—the Astros' brain."[90]

When Mejdal left to join the Astros, he used a password similar to the one he had used while working at the Cardinals.[91] Correa guessed the new password and accessed Mejdal's Ground Control and email accounts.[92] In March of 2013, Correa viewed scouting information, including the Astros' scouts' rankings of all players eligible for the 2013 Amateur Draft, a weekly digest page which listed statistics and notes on the performance and injuries of players whom the Astros were considering drafting, other web pages containing the Astros' evaluations of the Cardinals' prospects, and notes on trade discussions.[93] In June of 2013, the day before the 2013 Amateur Draft, Correa sorted the Astros' draft page to see which prospects the Astros rated highest, as well as other scouting reports.[94] Before day three of the Draft, Correa viewed the draft page to look for players not yet drafted, including the page of Adam Nelubowich, whom the Cardinals drafted later that day, and three players

---

Astros' Mejdal Takes on Unique Role, MLB (Jan. 31, 2012, 11:37 AM), http://wap.mlb.com/hou/news/article/2012013126525316/.

[85] Green, *supra* note 67.

[86] Sentencing Memo, *supra* note 83, at 2.

[87] The Astros and Cardinals were both members of the National League Central division before the Astros moved to the American League in 2013.

[88] Drellich, *supra* note 2.

[89] Plea Agreement at 7, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016).

[90] Green, *supra* note 67.

[91] Plea Agreement, *supra* note 89, at 8.

[92] *Id.*

[93] *Id.*

[94] Sentencing Memo, *supra* note 83, at 3.

the Cardinals had drafted the day before.[95] On July 31, 2013, the day of the non-waiver trade deadline, Correa again accessed Ground Control to view trade discussions between the Astros and other teams.[96]

On March 8, 2014, the *Houston Chronicle* published an in-depth article about Ground Control.[97] In response, the Astros enhanced their security precautions by changing Ground Control's URL and requiring Ground Control users to change their passwords. The team reset the database to a system-wide default password, which was emailed to users. However, since Correa had access to Mejdal's email, he also gained access to the new URL and default password. Correa used this information to access Luhnow's account, viewing 118 web pages containing confidential information specifically relating to players the Astros were targeting in the 2014 Amateur Draft. Correa also viewed the "task page" for the Astros' analytics department, which "listed the projects that the department was researching."[98] In March of 2014, Correa allegedly leaked embarrassing confidential information about the Astros' trade discussions to *Deadspin*, a sports blog. In so doing, Correa allegedly sought retaliation for a recent *Sports Illustrated* article, which praised Luhnow and Mejdal's reportedly outstanding analytical methods and predicted that the Astros would win the 2017 World Series.[99] During these unauthorized intrusions, Correa used software to conceal his identity, his location, and the type of device he was using.

In December of 2014, Correa was promoted to Director of Scouting, where his duties involved scouting and the amateur draft—areas in which his access to Ground Control would have been particularly relevant. Though the government only charged Correa with accessing Ground Control on five occasions, the prosecution's sentencing memo alleges that Correa in fact accessed Ground Control on forty-eight occasions, using the accounts of five different Astros employees.[100] The sentencing memo further states that Correa improperly accessed Mejdal's email account over a two-and-a-half-year span.[101]

Correa claimed he was looking at Ground Control because he believed that the Cardinals' proprietary data had been "improperly transferred to the Astros'

---

[95] *Id.* at 4.
[96] Plea Agreement, *supra* note 89, at 9.
[97] Drellich, *supra* note 2.
[98] Plea Agreement, *supra* note 89, at 10.
[99] *See* Sentencing Memo, *supra* note 83, at 6 (describing the *Deadspin* leak).
[100] *Id.* at 1.
[101] *Id.*

system by former Cardinals employees who had been hired by the Astros"[102] and asserted the Astros had replicated "key algorithms and decisions tools" created by the Cardinals.[103] No charges were ever brought against the Astros.

Correa waived indictment and pleaded guilty to five counts of "Unauthorized Access of a Protected Computer" under the CFAA for intrusively accessing the Astros' database from March 2013 to June 2014.[104] Correa was sentenced to forty-six months in prison and ordered to pay criminal monetary penalties, including over $279,000 in restitution to the Astros.[105] In addition, the MLB Commissioner ordered the Cardinals to give the Astros their top two draft picks in the 2017 Draft and pay the Astros $2,000,000, the maximum punitive fine that the MLB Commissioner has the authority to direct pursuant to the MLB Constitution.[106]

While Correa pleaded guilty under the CFAA, could he have also been convicted under the EEA? Correa did not appropriate the operational code of Ground Control itself, nor did he appropriate Ground Control's algorithms used to evaluate input data. Instead, he took the analytical conclusions generated by Ground Control—that is, the *results* produced by the system. It seems clear that such results would fit the EEA's definition of a "trade secret."

First, the content which Correa accessed falls within the types of information listed in section 1839(3). The rankings which the Astros assigned to players whom they were interested in drafting are analogous to those provided in *Rang*, and the scouting reports, trade discussions, and medical reports that Correa accessed would qualify as "business information" within the meaning of the EEA.

---

[102] *Ex Parte* Motion for Issuance of Subpoena & Prehearing Production of Materials at 1, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016) (recounting Correa's statement made at rearraignment); *see also* Rearraignment at 9:8-24, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016).

[103] Derrick Goold, *Correa Gives His Account of Hacking Case*, ST. LOUIS POST-DISPATCH, Feb. 1, 2017, at B1.

[104] Plea Agreement, *supra* note 89, at 1.

[105] Judgment in a Criminal Case, *supra* note 1, at 3, 6.

[106] Tom Verducci, *Lax Hack Smack: MLB, Rob Manfred Let Cardinals off Easy in Hacking Scandal*, SPORTS ILLUSTRATED (Jan. 30, 2017), https://www.si.com/mlb/2017/01/30/cardinals-astros-hacking-chris-correa. *See generally* MAJOR LEAGUE CONST. art. II, § 3, *available at* http://www.law.uh.edu/assignments/summer2009/25691-b.pdf ("In the case of conduct by Major League Clubs, owners, officers, employees or players that is deemed by the Commissioner not to be in the best interests of Baseball, punitive action by the Commissioner for each offense may include . . . a fine, not to exceed $2,000,000 . . . .").

Second, the Astros took several "reasonable measures" to keep their information secret, as required by section 1839(3). Ground Control was not only protected by a password, but this password was reset after the *Houston Chronicle* article, showing that the organization was actively vigilant in protecting its system. Additionally, certain functions were only permitted to be used by certain employees. For example, Correa's bouts of unauthorized access involved intruding into the accounts of two minor league players who, according to the government's sentencing memorandum, had more limited access than other personnel.[107] Prior to Correa's hacking, Luhnow said that the team was taking "as many measures as we can to protect the information," such as walling off access, inhibiting the ability to download the data, and logging users' activity on the system.[108]

Third, the information in Ground Control derived "independent economic value" from not being generally known or ascertainable through "proper means." The government argued, and the court agreed, that "the deliverable from all of [the scouting] expenses was the information that they put in" Ground Control.[109] As the government noted, in order to diminish the strong likelihood that years and money will be fruitlessly invested in talented individuals who never end up graduating to major-league caliber, teams have poured increasingly massive amounts of resources into the consideration of which players to acquire.[110] The Astros' proprietary data that was stored in Ground Control was only economically valuable because it was not generally known to other baseball teams. By developing its own tools and metrics, the Astros were able to better evaluate talent, thereby gaining a competitive edge over other teams. Analogizing the secrecy-based value of proprietary sabermetrics, one journalist contended that Correa's actions were "tantamount to stealing the secret formula for Coke."[111] The plea agreement asserts that the intended loss to the Astros was $1.7 million.[112]

---

[107] Sentencing Memo, *supra* note 83, at 5.

[108] Joshua Green, *My Time with the Architect of the Astros' 'Ground Control,'* BLOOMBERG BUSINESSWEEK (June 16, 2015, 3:47 PM), https://www.bloomberg.com/news/articles/2015-06-16/my-time-with-the-architect-of-the-astros-ground-control-database.

[109] Rearraignment, *supra* note 102, at 11:8-9.

[110] Responses to Defendant's PSR Objections at 6, United States v. Correa, No. 4:15-CR-00679 (S.D. Tex. July 21, 2016).

[111] Green, *supra* note 108.

[112] Plea Agreement, *supra* note 89, at 4. The prosecution reached the $1.7 million figure by taking the number of players Correa viewed "by 200," dividing that by the number of players that were eligible to be drafted and multiplying by the scouting budget of the Astros that year. *See* Rearraignment, *supra* note 102, at 10:22-11:4. The actual monetary loss incurred by Correa's

Further, the data Correa accessed related to a product intended for use in interstate commerce. As discussed above, baseball, as a form of viewable entertainment in which tickets are sold and marketing is conducted throughout the country, is a product of interstate commerce.[113]

Compared to satisfying section 1839's definition of a "trade secret" and section 1832's interstate commerce requirement, the EEA's mens rea element would likely be more difficult to prove. This may explain why the government refrained from pursuing charges under the EEA. Correa proffered that his intent was not to injure the Astros for his own benefit but to assess whether the Astros had stolen information from the Cardinals.[114] Had the government prosecuted Correa under the EEA and had his case proceeded to trial, Correa may have argued that he did not intend to injure the Astros or convert it for his or the Cardinals' benefit.[115] There may have been no conclusive evidence that Correa intended to injure the Astros.

That said, such intent could be inferred from the fact that Correa allegedly leaked the Astros' confidential trade discussions to *Deadspin*—a move which inflicted foreseeable reputational damage on the Astros and seemed to serve no purpose other than to injure and embarrass. Also, as the government pointed out in its sentencing memorandum, the information Correa looked at did not relate to the Cardinals, but rather included the Astros' trade discussions with other teams. Such trade discussions had no bearing on whether the Astros stole information from the Cardinals, suggesting that Correa's intent was to injure the Astros (and not to assess whether the Astros had stolen information from the Cardinals).

Moreover, Correa personally benefited from the hack insofar as he was promoted to Director of Scouting in 2014. The specific content Correa accessed in the Astros' Ground Control database was directly related to drafting and scouting, which were areas core to Correa's new job responsibilities. As the prosecution highlighted in its court filings, Correa's access to Ground Control gave him the

---

victims was established as just over $279,000, and this substantially smaller figure was pertinent to the determination of Correa's sentence pursuant to the U.S. Sentencing Guidelines.

[113] *See* Flood v. Kuhn, 407 U.S. 258, 282 (1972) ("Professional baseball is a business and it is engaged in interstate commerce.").

[114] Goold, *supra* note 103.

[115] In his guilty plea, Correa conceded that he acted with intent to injure the Astros. *See* Plea Agreement, *supra* note 89, at 10 ("The Parties agree that the defendant's intended loss under the U.S. Sentencing Guidelines definition for all of his intrusions is $1.7 million."). Conceding that he acted with intent may have been a condition of his guilty plea. However, it does not bear on how Correa would have argued had his case proceeded to trial.

ability to "corroborate his judgment calls" by "check[ing] what another analytics-minded organization thought."[116] In addition, Ground Control enabled Correa to know which projects the Astros found promising and which they discarded.

Two principle questions remain. First, why did the prosecution not bring charges against the Cardinals as well? The Commissioner clearly saw it fit to sanction the organization through a fine and loss of draft picks. Further, it would have been possible to introduce evidence that Correa acted within the scope of his employment, thus making the Cardinals liable pursuant to the doctrine of respondeat superior. Perhaps because the government knew that MLB had its own internal mechanisms for disciplining and fining clubs, there was less of a need for the government to impose its own sanctions.

Second, why did the government not prosecute Correa under the EEA? Certainly, the CFAA charge was the more straightforward claim to pursue since the EEA has a more intricate mens rea requirement. As previously mentioned, to succeed on an EEA charge, the prosecution would need to establish that the defendant (i) *intended* to convert the trade secret for the benefit of someone other than the owner; (ii) *intentionally* or *knowingly* injured the owner; and (iii) *knowingly* misappropriated the trade secret through one of the delineated unauthorized acts.[117] Further, the prosecution would have had to prove that the content which Correa accessed on the Astros' Ground Control constituted a trade secret. It is possible that the Astros were reluctant to reveal information about Ground Control, especially given the media scrutiny. Indeed, the prosecution "agreed to a more restrained sentence," including the decision not to add additional charges such as aggravated identity theft,[118] and noted that the plea agreement was "the product of extended negotiations between the parties, both of whom made concessions over several months."[119] While the prosecution specifically noted that they chose not to charge Correa with aggravated identity theft, there is no discussion of the EEA. Declining to charge Correa under the EEA may have been part of the prosecution's strategy of taking a lenient posture in order to reach a plea deal.

---

[116] Responses to Defendant's PSR Objections, *supra* note 110, at 6.

[117] 18 U.S.C. § 1832(a) (2012).

[118] Responses to Defendant's PSR Objections, *supra* note 110, at 7 ("[T]he parties agreed that a more restrained sentence was appropriate, so they agreed on the loss calculations and the sophisticated means enhancement, and to not charge aggravated identity theft.").

[119] *Id.*

II.
THERE ARE POLICY REASONS TO APPLY THE ECONOMIC ESPIONAGE ACT TO TRADE SECRET THEFT IN BASEBALL

Ground Control is not the exception in the baseball industry. Many teams have similar databases that house information used to make player-related decisions, including the Cardinals (who have since moved on from Red Bird Dog but refuse to disclose the name of their new system),[120] the Boston Red Sox (Beacon),[121] and the Cleveland Indians (DiamondView).[122]

Correa was charged under the CFAA for accessing the Astros' database "without authorization." In so doing, the prosecution neglected the heart of the wrong Correa committed. The prosecution failed to address the true focus of Correa's misdeeds—not the *means* of accessing the information (a problem which brings to mind questions of password sharing discussed in *United States v. Nosal*[123]), but the proprietary nature and *use* of the information itself. This point is underscored by the fact that Correa accessed Ground Control not via the use of technical skill but rather by receiving Mejdal's password when Mejdal turned over his computer upon leaving the Cardinals. Because Mejdal failed to significantly change his password, Correa had an easy means of entry.

Correa's case provides an important lesson concerning the nature of the intellectual property risks which baseball teams face. The main threat is not from "outside" hackers who illicitly *access* computer databases but from those already embedded within the industry who impermissibly *use* secret information.

---

[120] *See* Derrick Goold, *MLB Commissioner: Teams Need to Protect Intellectual Property*, ST. LOUIS POST-DISPATCH (Nov. 10, 2015), https://www.stltoday.com/sports/baseball/professional/birdland/mlb-commissioner-teams-need-to-protect-intellectual-property/article_4c2ed647-65e6-5edd-b17a-e3cdcf510fd3.html ("The Cardinals have long since abandoned 'Red Bird Dog' for an internal database whose nickname they don't even want to share.").

[121] Alex Speier, *Red Sox to Retire 'Carmine,'* BOS. GLOBE, Feb. 23, 2017, at D.1.

[122] Alex Kaufman, *Moneyball, Before Moneyball Was Cool*, ESPN: SWEETSPOT (June 7, 2014), http://www.espn.com/blog/sweetspot/print?id=48166.

[123] United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016). In *Nosal*, an employee gave former employees her password so they could continue to access the company's confidential database. Nosal was convicted under the CFAA, and as Judge Reinhardt noted in his dissent, the application of the CFAA to this scenario had the potential to criminalize broader types of password sharing. *Nosal*, 844 F.3d at 1048 (Reinhardt, J., dissenting).

Accordingly, the EEA, which focusses on the impermissible *use* of secret information, addresses the risks faced by baseball teams more directly than does the CFAA, which focusses on the illicit *access* from outside hackers. The importance of this shift is driven home by a few considerations.

A. The Fluidity of Personnel in Baseball Creates a High Risk for Misappropriation

While employee turnover is a common feature of many industries, the fluidity of baseball operations staff is practically a definitional feature of the baseball industry.[124] Just as a player is traded from team to team, front office staff routinely move from team to team as well. The Milwaukee Brewers' baseball operations department provides one example. The team's current General Manager, David Stearns, joined the Brewers from the Houston Astros, and he had previously worked for the Cleveland Indians, New York Mets, and Pittsburgh Pirates. The team's Assistant General Manager, Matt Arnold, had stints with the Tampa Bay Rays, Los Angeles Dodgers, Texas Rangers, and Cincinnati Reds. The team's senior advisor, Doug Melvin, had prior experience with the Rangers, Baltimore Orioles, and New York Yankees. Taken together, Stearns, Arnold, and Melvin alone have inside experience with one third of the league, including two division rivals.[125]

An examination of the thirty General Managers at the start of the 2018 season reveals that nine have worked for four or more teams, and thirteen have worked for two or three teams.[126] While that leaves eight General Managers who have only worked for one franchise, every team has baseball operations department staff with experience working for multiple teams.[127]

This "incestuous shuffling of scouting and front office talent" poses a serious risk to teams that have developed proprietary data systems.[128] The information one team has in assessing players is directly applicable to the core business of a competitor team.

---

[124] *See* Dean Pelletier, *Trade Secrets: Extra Edges on the Diamond*, PELLETIER L. (Mar. 8, 2015), http://www.pelletier-ip.com/?p=197 (calling employee mobility "part of the fabric of all professional sports").

[125] 2018 MILWAUKEE BREWERS MEDIA GUIDE 10-12 (Mike Vassallo et al. eds.).

[126] *See infra* Appendix.

[127] Data was compiled using each team's 2018 Media Guide. Employees holding the title of "General Manager" were included in this study. The Boston Red Sox's Dave Dombrowski, the Miami Marlins' Michael Hill, and the Baltimore Orioles' Dan Duquette were included in this study, as those three teams do not employ anyone with the title "General Manager."

[128] Ben Lindbergh, *Baseball's Ever-Expiring Secrets*, RINGER (Feb. 6, 2017, 11:49 AM), https://www.theringer.com/2017/2/6/16036642.

At first glance, increasing criminal enforcement of trade secret laws produces undesirable consequences, such as a restricting employee mobility. Limits on employee movement within an industry can have "detrimental effects on innovation, market competition, and economic growth,"[129] because preventing "talented individuals from standing upon the shoulder of giants, sharing knowledge, and making use of their human capital," harms innovation.[130] Thus, perhaps using the CFAA would be less detrimental to employee mobility and the cross-pollination of ideas because the CFAA focuses on the access to that information rather than how it is used. However, as discussed above, Correa's case illustrates why the CFAA is inadequate on other grounds. The statute's vague notions of what constitutes "hacking" fails to address what society wishes to express as the true harm of Correa's actions. We do not want to punish Correa solely because he guessed a password. Rather, we want to punish Correa because he used that password to give his team an illicit and illegal competitive advantage.

Further, concerns over the EEA restricting employee mobility in baseball are overstated. First, because the EEA includes such a high mens rea requirement, trade secret prosecutions would be brought sparingly in baseball. Under the EEA, the prosecution must establish as to each element of the crime that the defendant (i) intended to convert a trade secret to the economic benefit of someone other than the owner, (ii) intended or knew that such conversion would injure the owner of the trade secret, and (iii) knowingly misappropriated the trade secret through one of the delineated unauthorized acts.[131] Given the EEA's demanding mens rea requirement, prosecutors will likely only go after those with a truly "evil-meaning mind."[132] That is, employees moving between organizations without "evil-meaning minds" will not have to fear prosecution. Still, as with any criminal statute, prosecutorial discretion will ultimately reign supreme on when and whether these cases will be brought.

---

[129] Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 TEX. L. REV. 789, 835 (2015).

[130] *Id.*; *see also* Cohen, *supra* note 57, at 229 ("Diminished labor mobility is costly not only for individual workers, but for the nation as a whole. The economy is at its most efficient when workers are able to take their labor where the market would value it most highly." (internal citations omitted)).

[131] 18 U.S.C. Code § 1832(a) (2012) ("Whoever, with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly" misappropriates a trade secret through an enumerated act shall be subject to punishment).

[132] Morissette v. United States, 342 U.S. 246, 251 (1952).

Second, baseball teams already have internal mechanisms in place to stifle employee fluidity and movement, meaning that any chilling effect on employee mobility from the EEA would be relatively unpronounced. Among other mechanisms, teams require employees to ask for permission before interviewing with another MLB team. These rules stem from the prohibition against tampering "with negotiations or dealings respecting employment" found in the Official Professional Baseball Rules Book.[133] The rule reads:

> [T]here shall be no negotiations or dealings respecting employment, either present or prospective, between any player, coach or manager and any Major or Minor League Club . . . unless the Club or baseball employer with which the person is connected shall have, in writing, expressly authorized such negotiations or dealings prior to their commencement.[134]

On its face, the provision extends to "managers," a term which, along with individual team policies, could be and has been broadly interpreted to encompass a host of employees.[135] Although individual teams' employee policies are generally not public information, there have been some media reports of teams amending their employee policies in response to employees getting poached by other teams. For example, in 2011, the Toronto Blue Jays amended their employee policy so that employees in their baseball operations department would not be granted permission to interview with other teams for positions that did not represent a promotion from their current position.[136] Teams generally have a "widely observed policy of letting other clubs interview their employees for positions that would represent promotions."[137] Even so, in some rare cases teams have exercised this power in restricting employees from interviewing with other teams even if the employee

---

[133] OFFICE OF THE COMM'R OF BASEBALL, THE OFFICIAL PROFESSIONAL BASEBALL RULES BOOK, R. 3(k) (2018) [hereinafter MLB RULES BOOK], https://registration.mlbpa.org/pdf/MajorLeagueRules.pdf.

[134] *Id.*

[135] For an example of an investigation into tampering regarding a team's manager, see Associated Press, *MLB Rules No Tampering Found in Cubs' Hiring of Joe Maddon*, ESPN (Apr. 29, 2015), http://www.espn.com/chicago/mlb/story/_/id/12787877.

[136] Doug Harrison, *Jays Amend Employee Policy to Quell Farrell Rumours*, CBC SPORTS (Oct. 25, 2011, 12:39 PM), http://www.cbc.ca/sports/baseball/mlb/jays-amend-employee-policy-to-quell-farrell-rumours-1.1050694.

[137] Lindbergh, *supra* note 128.

would be offered a promotion.[138] Given the general trend of vast movement of executives between teams, this system still seems largely perfunctory. Nonetheless, the system shows that the industry is trying to put its thumb on the scale against employee movement, thereby overshadowing any theoretical chilling effect the EEA may have on employee mobility.

Third, even assuming that the EEA would stymie employee mobility, this would not necessarily harm the baseball industry. Limiting employee fluidity may in fact be healthy for the industry. Sports are built on the notion of discovering who has the best competitive strategy and advantage. Sharing ideas between teams breaks down the fundamental competitive fabric and function of the system. Unlike industries which may provide for a more concrete connection to economic growth, public utility, or the public good, sports are a gratuitous demonstration of who can outcompete whom, who can come up with the best strategy, and who can win a game. Professional sports are built on the fundamental idea of secret gamesmanship. Unlike in other industries where employees working together across companies may enhance the public good, employees sharing secrets in sports undermines the gamesmanship of the sport, harms the public's confidence in the integrity of the game, and reeks of collusion. Furthermore, the confined and unique nature of the sports industry lessens costs to innovation that may be more harmful in other settings.

The Correa case is one example of the effects of employee turnover, both from a psychological and competitive perspective. Correa's psychological paranoia resulting from Luhnow and Mejdal's departure allegedly led him to access Ground Control. It was not ludicrous of Correa to worry that Luhnow and Mejdal may have taken proprietary information with them—as one commentator noted, "the secrets were inside their heads."[139] Even a *Houston Chronicle* article that predated the Correa case alluded to this phenomenon, noting that "were a member of the Astros front office to leave, some of the team's operating secrets would leave with them."[140]

Moreover, the Correa case illustrates what a competitor can do once this type of data is acquired. Among numerous occasions, Correa accessed Ground Control on three key instances: right before and during the 2013 Amateur Draft and the day of the non-waiver trade deadline. By accessing Ground Control on these dates,

---

[138] For example, the Chicago White Sox denied then Assistant General Manager Rick Hahn permission to interview for General Manager of the Seattle Mariners.

[139] Lindbergh, *supra* note 128.

[140] Drellich, *supra* note 2.

Correa was able to see the players in which the Astros were interested as well as gain more information in assessing the Cardinals' own picks. For example, Correa accessed scouting information for a pitcher, Marco Gonzales, who was the Cardinals' first-round draft pick.[141]

It remains to be seen whether teams will take the Correa case as a cautionary tale. The Commissioner, Rob Manfred, insinuated that there must be a shift in the way teams think about guarding proprietary data, noting that "30 years ago intellectual property in this business was what some GM carried around in his head and he was going to take it with him when he left . . . . There wasn't much you could do about that. Today the business has changed."[142] Implicit in the Commissioner's statement is an acknowledgment that some secrets cannot be kept simply due to the fluidity of the industry. His statement points to a worry of hackers accessing data, not leaks from a team's own employees. However, the idea that the threat does not come from employees changing teams is misguided, as Correa was only able to gain access to the Astros' database because Mejdal gave Correa his old password.

Luhnow himself condoned some type of misappropriation, saying "if someone leaves, they're allowed to take . . . anything they remember in their head." [143] The Director of Baseball Research for the Minnesota Twins echoed this sentiment, saying "if they can remember it you cannot stop them from taking it."[144]

Accordingly, some argue that the EEA does criminalize "theft by memory."[145] The idea of theft of trade secrets by memory is not wholly foreign. Under state law, several state courts have held that memorizing trade secrets constitutes a basis for civil liability.[146] For example, in *Stampede Tool Warehouse, Inc. v. May*,[147] former employees of an automotive equipment distributor argued their "taking" of the company's customer list could not be a violation of the Illinois Trade Secrets Act[148]

---

[141] Responses to Defendant's PSR Objections, *supra* note 110, at 4.

[142] Bill Shaikin, *Former Cardinals Executive Pleads Guilty, Admits Hacking Astros' Computers*, L.A. TIMES (Jan. 8, 2016, 6:54 PM), http://www.latimes.com/sports/sportsnow/la-sp-sn-cardinals-chris-correa-astros-20160108-story.html.

[143] Drellich, *supra* note 2.

[144] Lindbergh, *supra* note 128.

[145] Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 878 (2002) ("The EEA may be read to protect trade secrets that exist only in the mind of the holders against misappropriation through memorization of another.").

[146] *See, e.g.*, Allen v. Johar, Inc., 823 S.W.2d 824 (Ark. 1992); *see also* Ed Nowogroski Ins. v. Rucker, 971 P.2d 936 (Wash. 1999).

[147] Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d 209 (Ill. App. Ct. 1995).

[148] 765 ILL. COMP. STAT. ANN. 1065/1-9 (West 2017).

because they memorized the list instead of physically or digitally taking the information. The court disagreed, holding: "[a] trade secret can be misappropriated by physical copying or by memorization. . . . Using memorization to rebuild a trade secret does not transform that trade secret from confidential information into non-confidential information."[149] Though state courts, under state trade secret laws, have imposed civil sanctions on those who misappropriate trade secrets via memorization, to date, criminal liability has been mostly limited to theft of information in a tangible medium.[150]

Nonetheless, the literal language of the EEA suggests that prosecuting theft by memorization could be even easier than prosecution under most state trade secret laws. First, the definition of trade secrets under the EEA is broader than that of the UTSA. The EEA says information can be a trade secret "*whether* or how stored, compiled, or memorialized,"[151] whereas the UTSA lacks such elaboration.[152] The fact that a trade secret need not be stored or memorialized under the EEA points to an expansive definition of intangible objects as trade secrets. Further, the EEA provides that one who "communicates[] or conveys such information" without authorization, has committed a prohibited activity.[153] This suggests there is no requirement that a person must physically or electronically take trade secrets to be prosecuted under the EEA. The UTSA contains no such language. Thus, the EEA seems to contemplate the risk of misappropriation via memorization more than state laws do. Further, despite the fact that the statute has undergone numerous amendments since its enactment, Congress has done nothing to clarify this potential ambiguity.

Still, although the language of the EEA is amenable to criminalizing the memorization and disclosure of trade secrets, the EEA—in practice—has not been used to prosecute such conduct (perhaps because criminal sanctions for this type of misappropriation would "unduly endanger legitimate and desirable economic behavior"[154]). Turning to the EEA's legislative history, theft by memory was not the

---

[149] *Stampede Tool Warehouse, Inc.*, 651 N.E.2d at 217.

[150] Cohen, *supra* note 57, at 227 ("[M]ost [states] appear to limit criminal liability to cases in which there has been some kind of physical taking and do not require employees to wipe clean the slates of their memories." (internal quotation marks omitted)).

[151] 18 U.S.C. § 1839(3) (2012) (emphasis added).

[152] UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 438 (1990) ("'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process . . . .").

[153] 18 U.S.C. 1832(a)(2).

[154] 142 CONG. REC. S12,213 (daily ed. Oct. 2, 1996) (Managers' Statement for H.R. 3723, The Economic Espionage Bill).

type of misappropriation Congress had in mind.[155] Although a section of the EEA was removed during reconciliation which said that "the general knowledge and experience that a person gains from working at a job is not covered,"[156] this language was removed because Congress found it "unnecessary and redundant."[157] Remembering information from one's previous job is often an incidental fact to employee movement, and society may not view this behavior as culpable enough to warrant criminal sanctions.

Coupled with the lack of prosecution under the EEA for trade secret theft by memorization, baseball industry executives have taken a seemingly permissive attitude towards such conduct, thereby creating uncertainty as to when society should deem this behavior wrongful. Limited information sharing is tolerated in baseball culture. For example, one unnamed R&D Director noted that scouts often trade advance reports in exchange for favors or simply as an act of kindness among industry friends.[158] Teams openly admit that the reason they hire analysts is often because of the projects said analysts have worked on with a competitor.[159] While baseball executives have deemed some information sharing impermissible, where they seem to draw the line (as to what trade secret misappropriation they consider wrongful versus what they consider permissible), they seem to do so arbitrarily with no grounding in any legal framework. For example, while one unnamed executive said that copying source code to a Dropbox would constitute prosecutable behavior, they opined that if a developer still had access to code in his or her email and used that for a new team, that would be a "gray area."[160]

This permissive approach is misguided. Uncertainty as to conduct that companies deem improper has a detrimental effect on ex ante behavior and destroys any prospect for notice or ability to shape expectations as to what type of information teams value, what type of conduct is permitted, and what employees can take with them should they—or perhaps more accurately, when they—switch employers. The necessary normative guidance that shapes employee behavior is lacking in the baseball industry, so the threat of criminal prosecutions may be necessary to

---

[155] *Id.* at S12,212 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl) ("[W]e do not want this law used to stifle the free flow of information or of people from job to job.").

[156] *Id.*

[157] *Id.* at S12,213 (Managers' Statement for H.R. 3723, The Economic Espionage Bill).

[158] Lindbergh, *supra* note 128.

[159] *Id.* ("Most of the time in offices that are more inclusive by nature you will be exposed to the development and actual usage of the systems you develop and as such when you leave you take that with you. In fact, in most cases that is part of the reason you are being hired to begin with." (quoting the former General Manager of the Colorado Rockies, Dan O'Dowd)).

[160] *Id.*

discourage misconduct that harms competition and fair play, on and off the field. Accordingly, the EEA can and should provide guidance to employees over what type of behavior should be considered wrongful.

B. How Disputes Are Resolved in the Absence of Criminal Sanctions

A wide variety of internal disputes in MLB are subject to arbitration clauses. If the controversy involves disciplining a player, the league is required to go to arbitration as prescribed in the collective bargaining agreement with the MLB Players Association.[161] For disputes involving two teams, the Major League Baseball Constitution ("MLB Constitution") sets forth arbitration procedures. The latter is more applicable for cases of trade secret theft. The MLB Constitution states:

> All disputes and controversies related in any way to professional baseball between Clubs . . . (including . . . owners, officers, directors, employees and players) . . . shall be submitted to the Commissioner, as arbitrator, who, after hearing, shall have the sole and exclusive right to decide such disputes and controversies and whose decision shall be final and unappealable.[162]

The Commissioner also has the separate power to impose punitive action on "Major League Clubs, owners, officers, employees or players" for any conduct "deemed by the Commissioner not to be in the best interests of Baseball."[163]

Any action a team might seek to take against another team for the misappropriation of trade secrets by a former employee (i.e., under a state trade secrets law) would be subject to the arbitration clause of the MLB Constitution. Because teams are precluded from entering the courts to adjudicate these disputes, criminal law, where appropriate, could fill the gap. The fact that there is a separate system for internal discipline may lead some to believe that the need for criminal prosecution is reduced (or perhaps completely eliminated), as the league has come up with its own way for handling these types of disputes. However, the record of punishments imposed upon teams under the arbitration framework is sparse and

---

[161] 2017–2021 Collective Bargaining Agreement Between Thirty Major League Clubs and the Major League Baseball Players Association art. XIII (Dec. 21, 2016), http://www.mlbplayers.com/pdf9/5450407.pdf.

[162] MAJOR LEAGUE CONST. art. VI, § 1, *available at* http://www.law.uh.edu/assignments/summer2009/25691-b.pdf.

[163] *Id.* art. II, § 3.

opaque,[164] and the Commissioner is under no duty to disclose the punishments imposed.[165] Arbitration eliminates the advantage of the public process and transparency the legal system brings to the resolution of these disputes. Further, the standards in a criminal trial (i.e., beyond a reasonable doubt) in conjunction with the extensive mens rea requirements (especially for the EEA) allow for a more rigorous and thorough investigation of the issue than does private arbitration between teams.

Unlike civil disputes which fall within MLB's mandatory arbitration rules, criminal prosecutions under the EEA would be adjudicated in the courts. In failing to prosecute EEA violations in the context of baseball, prosecutors have, in effect, empowered MLB to define the scope of trade secret law in baseball and to relegate such disputes to private arbitration. This is contrary to the will of the legislature, which has elected to make trade secret theft a crime. As discussed above, baseball teams—many which feel powerless to stop the sharing of proprietary information in the face of the industry's employee fluidity—generally take a permissive attitude towards information leaving an organization when employees move teams. Where a private industry feels powerless to stop wrongful behavior is precisely where the criminal law should step in, not where the criminal law should stand down. Section 1832 of the EEA was written with this kind of misappropriation in mind. The importance of this information was underscored by Senator Herbert H. Kohl, when he said: "[B]usinesses spend huge amounts of money, time, and thought developing proprietary economic information . . . . This information is literally a business's lifeblood. And stealing it is the equivalent of shooting a company in the head."[166] Teams should not resign to letting their trade secrets, into which they have invested time and money, be taken to other teams. There may be more of a "league-think" attitude in baseball as opposed to other industries since each team is part of a larger collective, but undermining the competitive nature of the sport by allowing employees to bring proprietary information with them when they leave a team will eventually disincentivize teams from investing in these types of program and harm the league more than help it.

---

[164] Michael McCann, *Breaking Down Chris Correa's Prison Sentence For Hacking Astros*, SPORTS ILLUSTRATED (July 18, 2016), https://www.si.com/mlb/2016/07/18/cardinals-chris-correa-hacks-astros-prison-sentence ("The record of team punishments is fairly barren.").

[165] *See, e.g.*, Matt Snyder, *MLB Rules on Red Sox-Yankees Sign Stealing and Fines Both Teams*, CBS SPORTS (Sep. 15, 2017), https://www.cbssports.com/mlb/news/mlb-rules-on-red-sox-yankees-sign-stealing-and-fines-both-teams/ (discussing fines of an "undisclosed amount" levied on the Red Sox and Yankees in a recent dispute over sign-stealing).

[166] 142 CONG. REC. S740 (daily ed. Feb. 1, 1996) (statement of Sen. Kohl).

Finally, the reality is that prosecutors tend to use the EEA sparingly, often only in "egregious and 'open-and-shut' cases."[167] The Correa case likely meets the elements set out by the EEA and would have been a good opportunity for the government to use the EEA in a high-profile case to both publicize the EEA and more concretely broaden trade secret protection in sports.

C. Conventional Methods of Protecting Trade Secrets Are Ineffective

Though teams use many conventional tactics which qualify as reasonable precautions to keep information secret under the EEA, such methods are inadequate to stop the misappropriation of proprietary information on their own. One tactic that teams take is walling off certain information from certain employees.[168] This approach has several pitfalls. First, it does nothing to address what occurs when the General Manager, who is not walled off from any information, moves teams (which, as discussed above, is common practice). Second, creating "information silos" is bad for cooperation and employee morale.[169] It also leads to fewer people making more decisions and increases the likelihood of error.[170] Third, the baseball industry is highly reliant on the use of interns. The sheer number of low level analysts who cycle through an organization makes walling off difficult. As one former Yankees baseball operations intern noted, the number of interns was often so high that there were "more interns than office space."[171] Further, as fewer (or no) criminal prosecutions are brought, the onus will be on the team to come up with more effective ways to prevent the misappropriation of proprietary information. As a result, teams may wall off more data from certain employees, stifling an organization's synergy and ability to perform to its full potential.

Alternatively, teams may turn to contract law. The two types of contractual provisions generally used to protect trade secrets—non-disclosure agreements and non-compete agreements—may be inadequate in the context of professional

---

[167] Halligan, *supra* note 32, at 499.

[168] Drellich, *supra* note 2 ("There are ways to protect yourself by making sure that people have access to the data that they only need to make the decisions in the area." (quoting Luhnow)).

[169] Lindbergh, *supra* note 128 ("It creates real morale issues in the staff if they are walled off from things, particularly once you get into director and higher levels. Everyone doesn't need to know every piece of information, but if you start excluding department heads from certain things in the fear that they might leave, you are sort of inviting them to leave for somewhere else where they will be more involved and more trusted." (quoting an unnamed executive)).

[170] *Id.* ("A walled-off employee can't make as many direct contributions, and the smaller the pool of potential peer reviewers, the more likely it is that mistakes will survive.").

[171] *Id.*

baseball. Non-competes are especially problematic since they receive vastly different treatment from state to state. This could put teams in states which generally prohibit non-competes, such as California (where five teams, or one sixth of the league, are located), at a significant disadvantage.[172] Further, a breach of these agreements would not be adjudicated in the courts. As mentioned above, disputes between teams (for example, an employee disclosing a trade secret in violation of a non-disclosure agreement) are subject to the MLB Constitution's mandatory arbitration clause. Accordingly, inter-team disputes over non-disclosure agreements would not receive the protections and additional sanctions available through the legal system.

III.
ON-FIELD TACTICS

One commentator called Correa's actions a "high-tech version of what's been going on forever in baseball—stealing signals."[173] This comment illustrates the potential for complex legal questions to arise if the government more aggressively prosecutes the misappropriation of information in this context. In baseball, the ubiquity of sign-stealing has essentially been baked into the game.[174] In baseball, a sign is when a manager, coach, or player performs a series of physical movements (i.e., touching his hat, nose, or ear) to instruct the player to run a certain play (i.e., stealing a base or putting down a bunt).[175] Though in some situations, stealing signs could technically meet the standard under the EEA or other trade secret statutes, such on-field tactics should not be subject to adjudication in the courts.

---

[172] Grow & Grow, *supra* note 4, at 1618.

[173] Tyler Kepner, *Former Cardinals Executive Pleads Guilty to Hacking Astros*, N.Y. TIMES (Jan. 8, 2016), https://nyti.ms/1OVuZDk.

[174] *See, e.g.*, Tim Kurkjian, *Sign-Language Hidden Cameras, Phony Signals, Double-Dealing Espionage. No This Isn't the CIA—We're Talking About the Game Within the Game of Baseball*, SPORTS ILLUSTRATED (July 28, 1997), https://www.si.com/vault/1997/07/28/8115901/sign-language-hidden-cameras-phony-signals-doubledealing-espionage-no-this-isnt-the-ciawere-talking-about-the-game-within-the-game-of-baseball (quoting former Minnesota Twins Manager Tom Kelly saying that "stealing signs is part of the job"); Scott Lauber, *Dustin Pedroia Downplays Scandal: 'Don't Think This Should Be News,'* ESPN (Sept. 6, 2017), http://www.espn.com/mlb/story/_/id/20609320/dustin-pedroia-boston-red-sox-insists-sign-stealing-part-game (quoting the Boston Red Sox's Dustin Pedroia calling sign-stealing "part of the game").

[175] For a more thorough explanation of the history and different variations of signs in baseball, as well as how each element of the UTSA and EEA may be applied to sign-stealing, see Andrew G. Barna, Note, *Stealing Signs: Could Baseball's Common Practice Lead to Liability for Corporate Espionage?*, 8 BERKELEY J. ENT. & SPORTS L. (forthcoming 2019).

A. Non-Verbal Signals Could Meet the Definition of a Trade Secret

The EEA definition specifically provides that the information does not have to be tangible. Though this was likely added to address digital forms of information, hand signals used during a game are a type of intangible business information. Although the signal is displayed in public, the meaning of the signal is not public information nor is the timing as to when the play will be deployed. The secrecy is key to the successful implementation. If a team knows what is coming, it can prepare to counteract that move. Some coaches create decoy signs in which they add a slight variation to the sign so the player knows that play should not actually be implemented. This can help assess the extent to which the signs have been compromised. The timing is also imperative. Even if a player can anticipate what type of pitch will be thrown, the timing of knowing exactly when that pitch will be thrown is where the value of the secret lies. Teams "closely guard . . . the various signals (hand, verbal, or otherwise) used by coaches to relay play calls to players during a game."[176]

Does a team stealing an opposing team's signs constitute misappropriation of a trade secret within the meaning of the EEA? If the player notices that a change-up is thrown every time the catcher puts down four fingers and communicates that to the batter while he is standing on second base, did he knowingly steal information? This scenario likely fails to meet the requirement of misappropriation. Rather, it is more akin to reverse engineering. Reverse engineering is when one "start[s] with [a] known product and work[s] backward to divine the process which aided in its development or manufacture."[177] Here, the player used public information and decoded what the signal meant based on his powers of observation, thereby not acquiring the secret by improper means.[178] Although stealing signs in the manner described is technically "sign-stealing," it is very common and is not something the criminal law or government should have a hand in.

However, a distinction must be made between signs that are stolen via the naked eye and signs stolen via the aid of other devices. There have been several

---

[176] *See* Grow & Grow, *supra* note 4, at 1579; *see also*, Barna, *supra* note 175, at 19-20 ("Per industry practice, MLB teams take many measures to protect their signs. They use false signs, change signs throughout the game, change signs after players get traded, ensure the pitcher is not 'tipping' his signs, and speed up the pitcher's delivery.").

[177] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

[178] Delineating the line between misappropriation and superior knowledge or an educated guess is a common difficulty in the criminal law, especially in the insider trading context. *See, e.g.*, SEC v. Steffes, 805 F. Supp. 2d 601 (N.D. Ill. 2011).

cases of "sign-stealing" in which teams used more sophisticated means of acquiring the signs than merely observing signals and their outcomes. Teams have used various technologies and devices to decode or intercept signs, such as the use of video cameras or binoculars. In football, where teams communicate plays via electronic headsets, some teams have used electronic means of eavesdropping on these conversations. While non-video sign-stealing is an accepted part of the game, the use of other devices has been treated more seriously. In fact, while there is no official rule against sign-stealing in the MLB Rulebook, MLB issued a memo to clubs in 2001 specifically prohibiting the use of electronic equipment in connection with sign-stealing[179] (and the MLB Commissioner can punish teams for any conduct that is not in the "best interests" of baseball under the Rule Book[180]). This prohibition against the use of other devices in connection with sign-stealing was reiterated by Commissioner Manfred in 2017.[181] Another example comes from professional football, where the New England Patriots videotaped New York Jets coaches sending signals to their players during a game. It was not the stealing of the signs that got the Patriots in trouble but the fact that they did so using a camera.[182]

In 2017, the Yankees filed a claim with the Commissioner alleging that members of the Red Sox staff watching the game in the clubhouse used Apple Watches to communicate with training staff in the dugout about what signs the Yankees were using. Through a series of signals, the Yankees further alleged, the Red Sox training staff in the dugout then communicated this information to their players at the plate. The Red Sox filed a claim in response alleging that the Yankees used its camera from its regional sports network, YES, to steal signs during the game as well. Both teams were fined an "undisclosed amount" by the Commissioner.[183]

---

[179] Ken Rosenthal, *Red Sox Crossed a Line and Baseball's Response Must Be Firm*, ATHLETIC (Sept. 5, 2017), https://theathletic.com/94995/2017/09/05/red-sox-crossed-a-line-and-baseballs-response-must-be-firm/.

[180] MLB RULES BOOK, *supra* note 133, at R. 21(f).

[181] Robert D. Manfred, Jr., *Commissioner's Statement Regarding Red Sox-Yankees Violations*, MLB (Sept. 15, 2017), https://www.mlb.com/news/c-254435818.

[182] *See generally* Horovitz, *supra* note 65.

[183] Scott Lauber, *Red Sox, Yankees Fined Separate as Part of MLB Investigation Into Sign-Stealing*, ESPN (Sept. 15, 2017), http://www.espn.com/mlb/story/_/id/20716110/boston-red-sox-new-york-yankees-fined-separately-part-mlb-investigation-sign-stealing (discussing the Commissioner's determination that there was "insufficient evidence" to back the Red Sox claim against the Yankees, but nonetheless fined the Yankees after uncovering evidence that the Yankees had engaged in improper conduct in connection with the use of a dugout phone in a previous season).

B. The Legal System Should Not Be Involved in Adjudicating Disputes over On-Field Misappropriation

On-field tactics like sign-stealing should not be subject to the criminal law, whether it is done with the naked eye or with the help of an electronic device. This is because there is a difference between illegal behavior and "gamesmanship."[184] Unlike the stealing of sabermetric data or scouting reports, which have a corollary to the broader business world and are akin to the types of material Congress sought to protect when enacting the EEA, policing what is "against the rules" in a sporting event is no place for the judiciary. Sign-stealing is not only a common practice but has also been "lauded as good coaching."[185] As one law professor argues, "nothing done on the field of play is cheating. What happens on the field, even if it violates the rules of the game, is still the game."[186]

Questionable on-field tactics—even when done through sophisticated means like cameras or other equipment—are more appropriate for the disciplinary mechanisms built into the league's arbitration forums. As it relates to on-field play, some level of "cheating" is accepted, and it should be up to those in charge of policing the sport, not judges, to delineate what is proper.[187]

Additionally, the sign must "derive[] independent economic value."[188] While stealing signs can give teams a meaningful competitive edge[189] and some commentators believe "a sports play can be just as valuable to a sports team as a product, design, formula, or process may be to a manufacturing corporation or product developer,"[190] it would be more difficult to quantify how much a specific play is "worth" to the business. In contrast, the time, money and effort put in to creating analytical databases is easier to calculate and more congruent to what trade secret law was designed to protect.[191] Thus, a line should be drawn between "conduct primarily affect[ing] the integrity of the game" and conduct relating to the business

---

[184] Horovitz, *supra* note 65, at 327 ("The blurring of the cheating-gamesmanship line is of paramount legal importance—the former is intuitively misappropriation, the latter proper.").

[185] *Id.* at 318 (internal quotation marks omitted).

[186] *Id.*

[187] *Id.* at 328-29 ("It would be difficult for courts to accurately determine what is proper or improper in a world governed by unwritten laws that are hardly unanimous.").

[188] 18 U.S.C. § 1839(3)(B) (2012).

[189] Barna, *supra* note 175, at 5.

[190] Ferrelle, *supra* note 40, at 167.

[191] Horovitz, *supra* note 65, at 329 ("[T]he core focus of trade secret law is still the business world.").

of the enterprise and the information and programs a team creates, which "more closely align with business concerns."[192] In his note, Andrew Barna puts forth several other policy reasons against adjudicating sign-stealing in the courts, including the fact that signs can be changed easily and at a minimal cost, the customary nature of sign-stealing within the game, and the Commissioner's ability to impose penalties—such as loss of draft picks—which courts may not impose.[193]

IV.
THE FUTURE OF SPORTS DATA

The data that Correa accessed included several players' private medical records. Though keeping medical records is nothing new, teams have been pouring more resources into refining and leveraging this type of data. Every team now has in-house sabermetricians,[194] meaning the competitive advantage teams once gained from using sabermetrics has been reduced. As one consultant noted, "by the time someone has taken a statistical method elsewhere, has been able to implement it and is in a position to use that information to influence the decision-making of other teams, we would probably be onto the next thing."[195] While sabermetric analysis has become the lifeblood of every team, injury avoidance mechanisms have become a greater priority.[196] To that end, teams have turned to biometric data to recapture the competitive edge that was once secured through the early adoption of statistical analysis.

If teams can better harness data to identify the factors that put players at risk for injury, they will have a significant advantage. As injuries derail careers (and cost teams millions of dollars), any informational edge in preventing them is coveted. One focus has been on the jarring increase in tears in the ulnar collateral ligament ("UCL") of pitchers.[197] UCL tears take on average a period of twelve to sixteen

---

[192] *Id.* at 330. ("[T]he more conduct is directly related to business (that is, the more it is removed from pure athletic competition), it not only more closely aligns itself with the core justifications for trade secret protection but it also becomes easier and more natural for courts to classify as proper or improper.").

[193] Barna, *supra* note 175, at 22.

[194] Ben Lindbergh & Rob Arthur, *Statheads Are the Best Free Agent Bargains in Baseball*, FIVETHIRTYEIGHT (Apr. 26, 2016, 11:04 AM), https://fivethirtyeight.com/features/statheads-are-the-best-free-agent-bargains-in-baseball/.

[195] Lindbergh, *supra* note 128 (quoting director of analytics Jesse Smith).

[196] Associated Press, *Putting Data Science on the Pitcher's Sleeve*, N.Y. TIMES (Apr. 2, 2016), https://www.nytimes.com/2016/04/03/sports/baseball/putting-data-science-on-a-players-sleeve.html (quoting Glenn Fleisig calling biometric data collection "the next sabermetrics").

[197] Jonah Keri, *The Tommy John Epidemic: What's Behind the Rapid Increase of Pitchers Undergoing Elbow Surgery*, GRANTLAND (March 10, 2015), http://grantland.com/the-

months for recovery, but they can take as many as thirty months.[198] These injuries "keep a tremendous amount of money in the dugout."[199]

The monitoring systems many teams are beginning to use are extensive and invasive. For example, the Seattle Mariners work with Fatigue Science to monitor player sleeping habits. Players wear wristbands, which were originally developed by the U.S. military to measure fatigue in pilots and soldiers.[200] Teams "speak only in vague terms about their efforts, fearful of publicizing any experiment that could become a competitive advantage," which shows that teams are taking steps to keep these procedures secret and see some economic value in them.[201] Other examples include the use of harnesses to document "heart rate variability, respiration rate, activity and calories burned"[202] and arm sleeves embedded with 3D sensors to measure the force on the elbow joint of each throw.[203]

The collection and analysis of athletes' biometric data raises ethical and privacy questions that are outside the scope of this paper.[204] For example, should employers be allowed to keep this kind of information private if it could lead to innovative breakthroughs in preventing injury in the future? If a team discovers a way to minimize or completely avoid the prevalence of a certain kind of injury, should there be a duty to disclose this information so players can protect themselves?[205] What are the ramifications if this information gets stolen? Should the precautions employers take to maintain the secrecy of this data differ from those

---

triangle/tommy-john-epidemic-elbow-surgery-glenn-fleisig-yu-darvish/ (twenty-five percent of major league pitchers and fifteen percent of minor league pitchers in 2015 had Tommy John Surgery to repair the ulnar collateral ligament, and more pitchers had the surgery in 2014 than all of the 1990s).

[198] *Tommy John FAQ*, MLB: PITCH SMART, http://m.mlb.com/pitchsmart/tommy-john-faq/ (last visited Dec. 20, 2017).

[199] Joe Greenberg, *Q&A: New Cubs 'Saberist' Tom Tango*, ESPN (Jan. 30, 2013), http://www.espn.com/blog/chicagocubs/print?id=14619.

[200] Brian Costa, *Baseball's Fight with Fatigue*, WALL ST. J. (Feb. 23, 2015, 12:45 PM), https://www.wsj.com/articles/baseballs-fight-with-fatigue-1424710560.

[201] *Id.*

[202] *The Sports Industry's New Power Play: Athlete Biometric Data Domination*, SPORTTECHIE (March 3, 2017), https://www.sporttechie.com/the-sports-industrys-new-power-play-athlete-biometric-data-domination/.

[203] Grow & Grow, *supra* note 4, at 1578.

[204] For a discussion of the ethical and privacy issues surrounding the collection of athletes' biometric data, see *id.* at 1619-20.

[205] *See id.* at 1620.

taken for their normal statistical talent evaluations given the private nature of the data collected?

The collection, disclosure, and storage of biometric data would likely implicate other federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[206] and the Genetic Information Non-Discrimination Act of 2008 (GINA).[207] Further, some states, such as Illinois, have enacted laws relating to employer collection of biometric data. The Illinois Biometric Information Privacy Act (BIPA) requires private entities to "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry."[208] BIPA and similar laws could require teams to implement higher safeguards for the protection of player biometric data than merely protecting their databases with passwords, lest they be subject to liability for inadequately securing biometric data. As long as medical information is housed in the same place as other player data,[209] as was the case with Ground Control, teams should be motivated to strengthen the precautions they take for all their collectively-stored property. As the gathering of this data becomes more widespread and the benefits of its collection become clearer, the law will need to confront novel questions relating to protecting biometric data.

CONCLUSION

Although Correa was not charged under the EEA, he was ultimately sentenced to a significant amount of time in prison. Nonetheless, the changes over the last two decades in baseball—which have transformed the industry into one obsessed with the collection and analysis of data—show the need for greater legal protection of expensive and labor-intensive proprietary systems, such as Ground Control. Though teams take a somewhat relaxed attitude toward the realities of information sharing when employees switch teams, stronger trade secret protection in baseball is necessary to maintain the public's confidence in the integrity of the game. The EEA provides one way for the government to stop the misappropriation of this kind of

---

[206] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26, 29, and 42 U.S.C.).

[207] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110- 233, 122 Stat. 881 (codified in scattered sections of 26, 29, and 42 U.S.C.).

[208] 740 ILL. COMP. STAT. ANN. 14/15 (West 2017).

[209] For example, Correa viewed medical pages that were housed in Ground Control for 1B/DH/LF Conrad Gregor and 1B Chase McDonald. *See* Responses to Defendant's PSR Objections, *supra* note 110, at 1.

information as personnel move from team to team. The criminal law may not have a place on the baseball field, but it certainly has a place inside the office.

APPENDIX[210]

[210] Thank you to Mike Passanisi for helping design this image.


BASEBALL'S FLUID TALENT POOL
General managers generally move from team to team, usually having spent many years working around the league, bringing with them that team's institutional knowledge and strategy.
FIVE TEAMS
These three general managers have each worked for five different organizations.
DAVE DOMBROWSKI
President of Baseball Operations
Boston Red Sox
JERRY DIPOTO
General Manager
Seattle Mariners
DAVID STEARNS
General Manager
Milwaukee Brewers
FOUR TEAMS
An additional six general managers have each worked for four different organizations over their baseball tenures.
Alex Anthopoulos
General Manager
Atlanta Braves
Dan Duquette
General Manager
Baltimore Orioles
Matt Klentak
General Manager
Philadelphia Phillies
Thad Levine
General Manager
Minnesota Twins
A.J. Preller
General Manager
San Diego Padres
Mike Rizzo
General Manager
Washington Nationals
QUICK FACTS...
26.6%
(EIGHT OF 30)
Percentage of current GMs that have worked for only one team or organization
30%
(NINE OF 30)
Percentage of current GMs that have worked for at least four teams
43.3%
(13 OF 30)
Percentage of current GMs that have worked for two to three different teams