Hackers strike out: Recent cases of alleged sports analytics IP theft

Matthew J. Frankel∗1
Nixon Peabody LLP, Boston, MA USA

Abstract. This article discusses recent cases of alleged misappropriation, infringement, and/or theft of sports analytics intellectual property. First, it discusses the federal court case National Football Scouting v. Rang and analyzes the copyright and trade secret disputes at issue in that case. Second, it discusses the recent hacking of and theft from the Houston Astros’ proprietary database and analyzes the potential legal ramifications of the same under trade secret law and the federal Computer Fraud and Abuse Act.

Keywords: Intellectual property, copyright, trade secrets

Over the past several years, the application of trade secret law to sports analytics has received increased attention. Scholarly articles2 and those in the popular press3 have noted that the various elements of the business of sports analytics – statistical compilations, computer programs, player evaluation methods, confidential business information, to name just a few – should be eligible for trade secret protection. As one article notes, with the implementation of new digital video technology for measuring baseball players’ fielding ability, and other sports’ increasing reliance on technology and analytics, new and interesting issues of trade secret and other intellectual property law will continue to proliferate in the sports analytics field.4

Under applicable law, trade secrets are generally defined as information that is competitively valuable and subject to reasonable efforts to maintain secrecy.5 The Uniform Trade Secrets Act (UTSA), which has been enacted (with some variation) in all but a few states, defines trade secrets as including formulas, patterns, compilations, programs, devices, methods, and confidential business information.6

---


4Secret Sabermetrics, 5 Albany Gov’t L. Rev. at 282-84.

5See Uniform Trade Secrets Act, National Conference of Commissioners on Uniform State Laws (amended 1985) (“UTSA”), §1(d); RESTATEMENT (FIRST) OF TORTS §§77 (1939); RESTATEMENT (THIRD) OF UNFAIR COMPETITION §3 (1995).

 ISSN 2215-020X/15/$35.00 © 2015 – IOS Press and the authors. All rights reserved.

This article is published online with Open Access and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
techniques, or processes – all of which are used, to varying degrees, in the development, collection, and application of sports analytics.6 Under the UTSA, in order to qualify as trade secrets, these types of information must derive economic value by virtue of the fact that they are kept secret from others who might gain value from them.5 Sports analytics information will typically meet this requirement. For example, among competitive sports franchises, if one team’s confidential player-evaluation programs were made available to other teams, those teams could use such knowledge to adjust their on-field approaches (e.g., using particular defensive alignments) or off-field approaches (e.g., demanding a greater return for the sale of a player that the selling team knows the buying team rates highly) to gain a competitive advantage. Likewise, among companies that sell sports analytics services, disclosure of their proprietary and confidential data-collection methods, data compilations, and data-analysis tools – all of which required time, effort, and money to develop — might allow competitors to undercut their position in the sports analytics market.

Significantly, the UTSA requires entities seeking to protect trade secrets to take reasonable measures to maintain their secrecy.8 This does not require “heroic” efforts,9 but, depending on the facts, may involve the use of nondisclosure agreements (NDAs), limiting trade secret access on a need-to-know basis among employees or contractors, using computer passwords and firewalls, and/or marking documents and files with confidentiality legends.10

Under the UTSA, if a person misappropriates trade secrets, that person may be held civilly liable for damages or subject to injunctive relief prohibiting that party from using certain information, working for a specific employer or in a specific field, or developing or marketing specific products or services for a period of time.11 Although misappropriation can take many forms, it typically occurs via theft (e.g., by hacking or accessing a computer without authorization and copying trade secret information)12 or through the disclosure or use of trade secret information in a manner that violates a duty of confidentiality (e.g., using Company A’s trade secrets obtained pursuant to a NDA to help Company B develop a competing product).13 Federal laws, including the Computer Fraud and Abuse Act14 (CFAA) and the Economic Espionage Act,15 may provide further grounds for civil and/or criminal liability in cases involving trade secret misappropriation.

Recent developments in the case law and the news elucidate possible intersections of intellectual property law and sports analytics. This article briefly discuss two of those developments: (1) National Football Scouting, Inc. v. Rang,16 a federal district court case in Washington State involving disclosure of confidential football player ratings; and (2) news reports regarding the hacking of the Houston Astros’ proprietary database, “Ground Control,” the publication of “confidential information” from the database regarding trade talks and player evaluations, and the FBI’s investigation of the St. Louis Cardinal’s front office in connection with the hack.17 Both examples provide insight into how courts, law enforcement, sports teams, and other businesses might address intellectual property protection for competitively valuable information.

The Rang case involved a copyright and trade secret dispute between the plaintiff, National Football Scouting, Inc. (NFS), and the defendants, part-time sports writer Robert Rang and the website for which he wrote, Sports Xchange. NFS compiled yearly Scouting Reports in which NFS assigned each player an overall Player Grade, i.e., “a numerical expression representing [NFS’] opinion of the player’s likelihood of success in the NFL.” The Scouting Reports were copyrighted as unpublished works and shared only with twenty-one NFL clubs who paid for the reports for use in the draft. From 2010 to 2011, Rang – ignoring NFS’ cease and desist letters – published eight

5 See UTSA §1(4).
6 See id.
7 See id.
9 Secret Sabermetrics, 5 Albany Gov’t L. Rev. at 253.
10 UTSA §2, 3; see RESTATEMENT (THIRD) OF UNFAIR COMPETITION §44 cmts. c, d, f.
13 UTSA §162, see, e.g., RESTATEMENT (THIRD) OF UNFAIR COMPETITION §40 ill. 2 (1995).
articles discussing Player Grades for eighteen college players.18
Ruling on the parties’ dueling motions, the federal court held that Rang’s Player Grades were “com-

18Nat’l Football Scouting, Inc. v. Rang, 912 F. Supp. 2d 985, 986-89 (W.D. Wash. 2012). The court’s decision does not disclose how Rang obtained Player Grades. This fact would be highly relevant to determining whether he could have ultimately been held liable for misappropriation, since, under these circumstances, establishing misappropriation would likely require evidence that Rang knew or should have known that the information he disclosed belonged to NFS and was confidential. See UTSA §1(2)(ii).

19To determine whether Rang had established a fair use defense, the court applied the controlling test under federal copyright law, which requires consideration of the following factors: “(1) the pur-

pose and character of the use, including whether such a use is of a commercial nature or is for nonprofit educational purposes, (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.” Rang, 912 F. Supp. 2d at 991. While the court found that Rang misappropriated its trade secrets by publish-

20In determining whether Rang had established a fair use defense, the court applied the controlling test under federal copyright law, which requires consideration of the following factors: “(1) the pur-

pose and character of the use, including whether such a use is of a commercial nature or is for nonprofit educational purposes, (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.” Rang, 912 F. Supp. 2d at 991.

21Nat’l Football Scouting, Inc. v. Rang, 912 F. Supp. 2d 985, 986-89 (W.D. Wash. 2012). The court’s decision does not disclose how Rang obtained Player Grades. This fact would be highly relevant to determining whether he could have ultimately been held liable for misappropriation, since, under these circumstances, establishing misappropriation would likely require evidence that Rang knew or should have known that the information he disclosed belonged to NFS and was confidential. See UTSA §1(2)(ii).


23According to the Astros, an “outsider” gained “illegal” access to the Ground Control database, and posted on the internet “proprietary information” from the database consisting mainly of communications with other teams about potential trades.24 In June 2015, newspapers reported that the FBI had subpoenaed the St. Louis Cardinals organization in connection with a pending criminal probe based on “evidence that Cardi-


the Astros’ would have a strong argument that their player evaluations constitute trade secrets – much like the court in Rang held that NFS’ player ratings could be found by a jury to be trade secrets – because they are competitively valuable (inasmuch as the hack likely advantaged Cardinals or disadvantaged the Astros in the trade market) and they were subject to reasonable efforts to maintain secrecy (i.e., were contained in a limited-access, password-protected database).26

The CFAA, which is primarily a criminal statute but permits civil remedies, appears to be tailor-made for this case. In the civil law context, it applies (among other circumstances) where a person hacks into or accesses “without authorization” a “protected computer” – one used in interstate or foreign commerce – in order to obtain data or information from that computer.27 If the person or entity whose computer was hacked or accessed incurs costs of at least $5,000 in a one-year period “to investigate and respond to a computer intrusion” it can sue the perpetrator(s) under the CFAA for recovery of compensatory damages and for injunctive or other equitable relief.28 The hack of the Astros’ Ground Control database and resulting theft of information undoubtedly cost the Astros more than $5,000 to investigate and respond. Thus, if the Astros were to file a civil suit, such suit could likely include a claim for violation of the CFAA. Further, given the FBI’s pending criminal investigation and issuance of subpoenas, it would not be surprising to see criminal charges filed against the perpetrator(s) for trade secret theft under the Economic Espionage Act and/or the CFAA, among other possible charges.

As these examples show, the emergence of analytics as an integral element of success in professional sports, the vast amounts of money at stake, and evolving technologies will continue to present challenges for professional sports clubs, persons and entities whose business is sports analytics, and the lawyers who advise them. Trade secret law, copyright law, and the CFAA, among other sources of law, will continue to provide the owners of this valuable information with important tools to protect against hackers, misappropriators, or others attempting to engage in unfair competition.

---

26Adam Greenberg, Houston Astros hacked, trade conversations posted online, SC Magazine, July 1, 2014, http://www.scmagazine.com/houston-astros-hacked-trade-conversations-posted-online/article/358952/ (noting opinion of technology security researcher that “the kind of insight you could garner from these private sabermetrics would not only help in trade negotiations, it would allow you to frustrate the future trade prospects of the Astros”).

27The CFAA also prohibits incursions that “exceed[] authorized access,” a phrase that has created a split of judicial authority with respect to whether someone who does, in fact, have authorized access to a computer or file, but then uses it for a prohibited purpose, can be held liable under the CFAA. See, e.g., Stuyve Pyne, “The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend,” The Bolt (Berkeley Technology Law Journal), Mar. 31, 2014, http://bdll.org/2014/03/31/the-computer-fraud-and-abuse-act-circuit-split-and-efforts-to-amend/

2818 U.S.C. § 1030(g); see Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 774-76 (S.D. Tex. 2010).