Protecting Your Data: What Are Your Options?

BY MARC LIEBERSTEIN & ASHFORD TUCKER OF KILPATRICK STOCKTON LLP

Marc Lieberstein

Ashford Tucker

Marc Lieberstein *is a partner with Kilpatrick Stockton LLP's Trademark and Copyright practice group and is located in the firm's New York office.* ***Ashford Tucker*** *is an associate with Kilpatrick Stockton LLP's Trademark and Copyright practice group and is located in the firm's New York office.*

Microsoft and News Corp. are discussing an exclusive arrangement for Microsoft's search engine Bing to be the only e-source for News Corp.'s publications. The Wall Street Journal is one of the few publications that charges the public to access its e-publications. The Associated Press (AP) just settled claims, including one for "hot news" missappropriation, that it brought against All Headline News (AHN) for the unauthorized use of AP headlines and news data.[1] In today's information-based economy databases are ubiquitous, but they are also extremely valuable assets. From financial data to real estate to news and weather data, corporations and websites rely on such data to function and profit.

So, what are the options for protecting your database investment from copying or outright theft? It is clear after *Feist Publ'ns v. Rural Telephone Serv.*, 499 U.S. 340 (1991), that the mere investment in a database is no basis for copyright protection. Facts are not protectable in the United States, but if you break a hot news story, can you prevent someone else from reporting the facts before or immediately after you report them? How about time sensitive financial information?

Recent cases are beginning to grant database owners more flexibility to protect a database and prevent unfair misappropriation. In the United States, unlike some other areas of the world,[2] database protection is not governed by statute, but rather falls within several legal areas, i.e., "hot news", copyright/Digital Millennium Copyright Act (DMCA), contract/licensing, trade secret and trespass. This article will review the various database protection options and assess their respective viability in today's digital world.

"Hot News."[3] Making headlines recently was the AP case against AHN, accusing AHN of, among other things, "hot news" misappropriation, i.e., unauthorized taking and dissemination of time sensitive news headlines and data. The AP case settled, so the hot news claim remains untested, but in 1918, the Supreme Court recognized this tort in *Int'l News Serv. (INS) v. Associated Press (AP)*, a case between two major newswires, holding that INS misappropriated the AP's information by publishing AP's news data on the West Coast before or immediately after the AP.

The Second Circuit revisited the hot news tort in *Nat'l Basketball Ass'n (NBA) v. Motorola, Inc.*, crafting a multi-part test to establish the cause of action, the crux of which was the time sensitive nature of the information, the direct competition between the parties and the ability of others to free-ride on the efforts of the plaintiff and/or reduce the incentive to produce the product or service. The Second Circuit denied relief to the NBA because Motorola's instant pager service that published in-game updates to subscribers did not compete with the NBA's broadcasts. Despite the new framework for determining "hot news' misappropriation, since *INS* there has been no reported case decided on this particular claim in favor of a database owner. As a result, with the exception of being used as leverage over a defendant, the hot news claim, while seemingly potent at least for current events, probably lacks the necessary scope and pedigree to provide database owners with meaningful database protection.

Copyright.[4] In contrast to "hot news," despite the fact that most databases are collections of factual information, such databases may be copyrightable as "compilations" under the Copyright Act, 17 U.S.C. 101. Facts themselves are not copyrightable, but it is important to distinguish between the data and the database owner's "selection, coordination, or arrangement" of data. These latter creative elements are copyrightable, as the Copyright Act only requires independent creation and only a "modicum of creativity necessary to transform mere selection into copyrightable expression." *Feist*, 499 U.S. at 362-363 (the Supreme Court refused to extend copyright protection to a telephone book featuring names arranged in alphabetical order).

Accordingly, database owners/creators seeking copyright protection should utilize creative selection and organizational techniques when developing a database, and add editorial content to the underlying data. These embellishments may be superfluous on some functional levels (or even anti-functional), but they are original/creative elements that will distinguish a copyrightable database from uncopyrightable one. The delicate balance between fact and creative expression may be difficult to achieve with databases,[5] but when achieved, this creative balance provides for potent copyright protection for a database.

An early case confirming the value of such a balance was *CCC Info. Servs., Inc. v. Maclean Hunter Market Reports, Inc.* In *CCC Info.*, the district court initially granted summary judgment in favor of CCC, a database provider, permitting it to re-publish information from Maclean Hunter's Red Book car valuation manual database. Citing *Feist*, the Second Circuit reversed because even though the Red Book data were merely factual, CCC's database used Red Book's valuations in combination with another leading valuation estimator to create average valuation estimates. CCC also re-published Red Book valuations. The Second Circuit found that Maclean's Red Book data was not merely unprotectable ideas, but rather were calculated predictions of market value formed from educated opinions of the Maclean editors. Importantly, the Second Circuit stated that Red Book's logical arrangement of data did not render the Red Book uncopyrightable, but rather, was a display of originality, demonstrating "amply sufficient originality to pass the low threshold requirement to earn copyright protection" as a compilation.

Similarly in *Dow Jones & Co. v. Chicago Bd. of Trade*, the Southern District of New York held that Dow's list of stocks was copyrightable due to the subjective judgment exercised in selecting the stocks

to make up the list. But note *Fin. Info., Inc. v. Moody's Inv. Serv., Inc.*, where the Second Circuit affirmed the district court's finding that bond cards listing five basic facts about municipal bonds lacked sufficient creative authorship for copyright due to the objective nature of the compiled facts. Despite the *Moody's* case, the Second Circuit recognized the copyrightable selection and arrangement of facts in a Yellow Pages phone directory targeting New York's Chinese-American community in *Key Publ'ns, Inc. v. Chinatown Today Publ'g Enters. Inc*. But the court found no infringement because the copying party altered its expression of most of the factual similarities at issue.

More recently, in *Proven Methods Seminars, LLC v. Am.Grants & Affordable Housing Inst., LLC*, Proven Methods was granted a preliminary injunction, in part, to stop American Grants' use of compiled public domain data functioning as a guide for navigating government programs. The court stated that Proven Methods' compilation of facts from public domain sources, including websites, possessed the minimum level of creativity necessary to establish copyright protection. By combining editorial input, i.e., "opinions and suggestions" and sufficiently creative organization, the court stated that Proven Methods' combination represented "significant judgment, discretion, and originality" resulting in the copyrightable user-friendly guide.

The Digital Millenium Copyright Act (DMCA). The DMCA is an often overlooked form of copyright protection for databases permitting database owners to use encryption and password technology to prevent unauthorized access to, and copying of, their works.

The DMCA provides a cause of action to database owners who utilize security measures (a) against parties who access copyrighted works by circumvention of those measures, (b) against parties who create technology that circumvents the security measures, and (c) against parties who create technology that circumvents copy protection measures. *See* 17 U.S.C. § 1201 et al.

Accordingly, database owners may seek to use technology and the DMCA to legally protect their databases. For example, in *Ticketmaster L.L.C. v. RMG Techs, Inc.*,[6] the district court granted Ticketmaster's motion for a preliminary injunction against RMG based in part on RMG's violation of the DMCA, because RMG created and made available software which evaded Ticketmaster's website security programs. It bears noting that Ticketmaster's claim under the Computer Fraud and Abuse Act (CFAA) was another basis for the preliminary injunction. The CFAA grants broad protection against unauthorized access, and database owners should consider coupling a DMCA claim with CFAA claims, if possible.

Fair Use.[7] Notably, however, according to the statute, DMCA circumvention claims, like the aforementioned copyright protection, are subject to the fair use limitation imposed by the Copyright Act, 17 U.S.C. § 107. As stated in *Feist*, "[n]otwithstanding a valid copyright, a subsequent compiler remains free to use the facts contained in another's publication to aid in preparing a competing work, so long as the competing work does not feature the same selection and arrangement." Accordingly, some courts have allowed "intermediate copying" as a fair use under the Copyright Act. These courts protect as fair use the copying of a work only to access and extract uncopyrightable material.

For example, in *Sega v. Accolade* and *Sony v. Connectix*, the Ninth Circuit recognized that intermediate copying done by a software competitor to access, engineer, and use a functional hardware or software lockout system is a fair use under the Copyright Act. As a result it may be important to use a combination of copyright and contract law to protect against intermediate copying of uncopyrightable material and limit the fair use defense.

Recently, in *Facebook, Inc. v. Power Ventures, Inc.*, Facebook sued Power for copyright infringement based on Power's unauthorized use of Facebook's proprietary information in the form of cached copies made by Power of entire Facebook pages, including Facebook's copyrightable template arrangement of user data. The district court denied Power's motion to dismiss, and permitted Facebook's claim of copyright infringement based on the fact that Power scraped Facebook users' pages to make cached copies in its creation of a competing website. For the purpose of defeating Power's motion to dismiss, Facebook asserted a sufficient claim that Power's conduct violated Facebook's terms of use.

In rendering its holding, the district court in *Facebook* relied on *Ticketmaster L.L.C. v. RMG Techs, Inc.* and *MAI Sys. Corp. v. Peak Computer, Inc.*, in support of the controversial proposition that an automated program's cache of a website is a fixated copy under the Copyright Act and can be the subject of a copyright infringement action. *Facebook* appears especially noteworthy at first read because it comes from within the Ninth Circuit and seems to run counter to the aforementioned Ninth Circuit decisions in *Sega* and *Sony*, where the court held that intermediate copying was a fair use. Notably, the court did not address any fair use issues, and this remains a case worth watching to see if the copyright/contract combination will work to prevent such competition.

Contract.[8] While copyright has some loop holes (e.g., fair use, validity of copyright), contracts or licensing may offer the best and most consistent protection. Provided that the database terms of use are clear and noticeable to the user, such terms have been generally enforced.

The best terms of use for databases are those that provide for express acceptance prior to allowing access. Thus, the contemporary clickwrap or browsewrap licenses are preferable methods for creating an enforceable contract in the online context. Shrinkwrap licenses, as discussed below, are acceptable for the physical sales of boxed software products. Clickwrap licenses require user assent through an affirmative click, and browsewrap licenses are contract terms merely presented to

users of a web site, i.e., your use is your assent to the web sites terms of use.

It bears noting that all of these licenses are subject to state law, which may vary; and they are each subject to contract defenses, such as unconscionability. Therefore, a conspicuous notice of the terms, or the location of the terms is required for evidence of user assent, e.g., forcing a click or placing notice of the terms and a link to the full contract at the top of the webpage. Also, be aware that courts have recognized the reality that end users do not typically read these licenses, and hence drafters should be forewarned not to insert onerous self-serving terms which would subject the end user to great surprise or hardship; courts are generally dubious of such terms.

The leading case in the early development of end user licensing is *ProCD, Inc. v. Zeidenberg*. In *ProCD*, the court dealt with a shrinkwrap software license: notice of the license at issue appeared on the outside of a box of CD-ROM software, but the full terms of the license were not accessible by the user until the user purchased and opened the product. The terms of the license limited end users to non-commercial uses of the ProCD's CD-ROM SelectPhone database of information – purely factual phone book information which seemed by all accounts uncopyrightable. ProCD sued Matthew Zeidenberg for violating the license when he copied the CD-ROM information and resold it in competition with ProCD.

The Seventh Circuit, in rejecting the district court's holding that there was no valid contract, recognized the viability of "shrinkwrap licenses" as contracts, noting that Zeidenberg was aware of the terms of the license because the outside of the box stated that license terms applied, thus providing notice of ProCD's terms to Zeidenberg. Today, shrinkwrap licenses are still used, and browsewrap and clickwrap contracts are commonplace online, with the problems of notice obviated by the contemporary form of these contracts.

In today's online environment clickwrap, shrinkwrap, and browsewrap licenses generally are practically a prerequisite to accessing data or content. Database owners operating online should establish terms of use, which may differ in treatment of company staff and consumers, among others. And database owners should deploy their terms via some form of license, thereby binding every user who comes into contact with the licensed data. Following these steps should enable a database owner to establish broad protection for its data without copyright.

Trade Secrets. A trade secret is generally defined as information that "(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy", Unif. Trade Secrets Act, 14 U.L.A. 541 (1980) (adopted by 45 states, not including New York).

Trade secret protection may extend to databases used internally, for example by employees of a company, or used externally in limited circumstances subject to "reasonable" efforts to maintain secrecy. These reasonable efforts are often maintained in joint venture agreements, restricted use licenses and non-disclosure agreements. The fundamental drawback for relying on trade secret protection is that it can be forfeited rather easily if the secret becomes known or if a court determines that a party has not made reasonable efforts to maintain a secret. With factual databases, it is more likely than not that the facts will become known, so the shelf like of a trade secret on such factual information might be limited. As such, unless a database is utilized only internally or between a small number of people who are under contract not to disclose, trade secret protection may not be the most formidable form of database protection.

Trespass to Chattels. Surprisingly, use of the trespass to chattels claim in the database protection scenario has been limited, but successful in select situations. Trespass to chattels is a traditional common law tort which provides a property owner with a cause of action against intentional interference with personal property or rights in personal property. Courts have recognized this tort in the online context, analogizing a plaintiff's web site to personal property and holding that unauthorized robotic webcrawling constitutes a trespass to chattels. Thus, this tort provides online database owners with a unique form of relief in some cases, particularly those dealing with unauthorized robotic webcrawling.[9]

Databases are more valuable than ever. The courts appear to understand this value and have made it clear that database owners are not without recourse to protect their investments in compiling factual information and making it available to public and private interests. With careful planning and execution, most databases, even uncopyrightable ones, can be ensured of protection from copying or theft by competitors. IPT

ENDNOTES

1. The Associated Press v. All Headline News Corp., No. 1:2008cv00323 (S.D.N.Y. filed Jan. 14, 2008).
2. The European Union's Database Directive creates a *sui generis* right granted to creators of databases which may not qualify for copyright protection.
3. Case references appear in order in this section as follows: Int'l News Serv. v. Associated Press, 248 U.S. 215 (1918); Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 845 (2nd Cir. 1997).
4. New case references appear in order in this section as follows: Feist Publ'ns v. Rural Telephone Serv., 499 U.S. 340, 362-63 (1991); CCC Info. Servs., Inc. v. Maclean Hunter Market Reports, Inc., 44 F.3d 61, 63-73 (2d. Cir. 1994); Dow Jones & Co. v. Chicago Bd. of Trade, 546 F. Supp. 113, (S.D.N.Y. 1982); Fin. Info., Inc. v. Moody's Inv. Serv., Inc., 808 F.2d 204 (2d Cir. 1986); Key Publ'ns, Inc. v. Chinatown Today Publ'g Enters. Inc., 945 F.2d 509 (2d Cir. 1991); Proven Methods Seminars, LLC v. Am.Grants & Affordable Housing Inst., LLC, 519 F. Supp. 2d 1057, 1064 (E.D. Cal. 2007).
5. U.S. Copyright Office, *Report on Legal Protection for Databases*, 74 (August 1997).
6. 507 F. Supp. 2d 1096 (C.D. Cal. 2007).
7. New case references appear in order in this section as follows: Sega v. Accolade, 977 F.2d 1510 (9th Cir. 1992); Sony v. Connectix, 203 F.3d 596 (9th Cir. 2000); Facebook, Inc. v. Power Ventures, Inc., 91 U.S.P.Q.2d 1430, 1433-34 (N.D. Cal. May 11, 2009), *citing* Ticketmaster L.L.C. v. RMG Techs, Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007); MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993).
8. New case references appear in order in this section as follows: ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1451-53 (7th Cir. 1996). *See* Specht v. Netscape Communications Corp., 306 F.3d 17 (2d. Cir. 2002) (online license agreement held unenforceable because the user could not see the agreement or its terms and thus could not assent to the terms). *See* Register.com v. Verio Inc., 126 F. Supp. 2d 238, *aff'd*, 356 F.3d 393 (2d. Cir. 2004) (license terms enforced to protect a WHOIS database); Ticketmaster L.L.C. v. RMG Techs. Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007) (license terms enforced to protect ticketmaster.com website); Mathew Bender & Co. v. Jurisline.com LLC, 91 F. Supp.2d 677 (S.D.N.Y. 2000) (license terms enforced to protect uncopyrightable legal materials); Bowers v. Baystate Tech., Inc., 320 F.3d 1317 (Fed. Cir. 2003) (license terms enforced to prevent reverse engineering of patented software). Courts have refused to require licenses to access and compile data including player statistics, emphasizing that this information is factual in nature and publicly available. *See* C.B.C. Distrib. and Mktg., Inc., v. Major League Baseball Advanced Media, L.P., 505 F.3d 818 (8th Cir. 2007); CBS Interactive, Inc. v. National Football League Players, 2009 WL 1151982 (D. Minn. April 28, 2009).
9. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp.2d 1058 (N.D. Cal. 2000) (enjoining robotic access); Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2nd Cir. 2004) (enjoining robotic access). *But see* Intel Corp. v. Hamidi 71 P.3d 296 (Cal. 2003) (refusing to enjoin email activity of disgruntled former employee where First Amendment speech concerns raised).