Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

IP Protection Still Elusive For Data Compilations In US And EU

By **Richard Assmus, Nickolas Card, Brad Peterson and Mark Prinsley**
(July 16, 2019, 4:16 PM EDT)


Richard Assmus


Nickolas Card


Brad Peterson


Mark Prinsley

In many areas of research and development, businesses justifiably expect to be able to protect their innovations. In data projects, businesses today often pay dearly to license third-party data, collect data from their customers and business partners, organize that data into useful databases, improve the quality of the data and analyze those databases for business gain.

For example, International Data Corporation reported in a study dated Sept. 19, 2018, that spending on AI systems will reach $77.6 billion in 2022, up from approximately $24 billion in 2018. Of that amount, an estimated 40% will be dedicated to the development of AI software. This raises a question for lawyers of what those businesses will own as a result.[1] Here, we explore the availability of copyright and trade secret protection for data compilations under U.S. law and under the European Union's Directive 96/9/EC (on the legal protection of databases).

Copyright

The U.S. Copyright Act protects original expression, not the underlying ideas or facts embodied in that expression.[2] Still, the U.S. Copyright Act recognizes rights in compilations, which are defined as "a work formed by the collection and assembling of preexisting materials *or of data* that are selected, coordinated or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."[3]

Courts have grappled with the level of selection, coordination and arrangement required before finding original expression and, accordingly, granting copyright protection. Importantly, the underlying facts themselves need not be protectable for the compilation as a whole to be accorded protection.

The most cited case on this question, as it relates to databases, is Feist Publications Inc. v. Rural Telephone Service Company Inc.,[4] in which the U.S. Supreme Court reversed a ruling in favor of a phone book company against a competitor that had copied most of an entire phone book. The Supreme Court held that, in spite of the effort ("sweat of the brow") required to compile a phone book, the standard

alphabetical listing of basic phone directory information was not sufficiently original to merit copyright protection. The Supreme Court noted, however, that "the originality requirement is not particularly stringent" and that "[p]resumably, the vast majority of compilations will pass this test."

Although Feist is often presented as the death knell for copyright protections in databases under U.S. law, some cases applying the originality requirement soon after Feist actually found that particular data compilations merit protection, albeit narrow.[5] We have not, however, seen a case fully testing this proposition for a modern database in which data scientists made specific decisions about the selection, coordination or arrangement of the database or the particular data to compile for use in analysis.

A company that makes numerous choices with respect to consumer data it collects — for example, by deciding to collect specific data fields regarding a consumer's habits — may successfully argue that its database should enjoy copyright protection, at least against large-scale verbatim copying. Certainly such a company would also benefit by documenting its innovation process throughout, including any creative decisions made by the company.

A further copyright issue arises in the context of artificial intelligence. AI tools may produce creative works as they analyze a company's data or in other contexts. However, these works are unlikely to be eligible for copyright protection, as current U.S. copyright law requires "an original work of authorship."[6] Although the definition of "author" is not fixed by the U.S. Copyright Act, courts have found a human authorship as a requirement for copyright protection. In Naruto v. Slater, for example, the court required that a "person" or "human being" is required for authorship under the Copyright Act.[7] There would thus be benefit in involving humans in any creative process using AI and documenting the human contribution to the work.

Trade Secret

The U.S. Defend Trade Secrets Act defines "trade secret" as:

… all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, *compilations*, …, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –

(a) the owner thereof has taken reasonable measures to keep such information secret; and

(b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[8]

Unlike copyright, trade secrets do not require an original act of authorship. Instead, trade secret protection requires the owner to take "reasonable measures to keep such information secret."[9] Like copyright, an intentional program of documented efforts to meet the legal standard will help to ensure protection.

Courts look to affirmative acts of the plaintiff during this evaluation and may consider whether the plaintiff: (1) tracked database access and listed all employees, contractors, licensors, business partners or other third parties who could have misappropriated the plaintiff's compiled information; (2) reviewed any agreements with employees, vendors, subcontractors and other service providers for confidentiality clauses and restrictions on use of the plaintiff's data; and (3) evaluated its database security measures and other internal confidentiality precautions at the start of the project and periodically thereafter.

To preserve trade secrets, companies should limit exposure to trade secrets (both within the company and outside of the organization) to those who need access. Companies can reduce the risk in any necessary access through confidentiality and other language in employee and independent contractor agreements. Courts often look for contract language between the parties to indicate that the disclosing company clearly communicated disclosure restrictions to the people receiving the trade secret and may consider nondisclosure agreements or noncompete language in services contracts as evidence in support of protecting a trade secret.[10]

Companies should perform a similar analysis with respect to vendors, subcontractors, data licensees and other agreements under which they allow another company to access data. Each third-party agreement that exposes a company's prospective trade secrets could threaten the company's claim for trade secret protection. In order to show that the company took "reasonable measures" to ensure secrecy, any such agreement should include clauses that require such reasonable measures from the licensee (such as a confidentiality clause) and specifically list the information to be protected (see Events Media Network Inc. v. Weather Channel Interactive Inc., where a general restriction on disclosure of "Confidential Information" was not sufficient to show that the plaintiff intended licensed information to remain confidential).[11]

Finally, a company may be required to prove the reasonability of its security measures in order to make a successful claim for trade secret protection. Though this requirement is open to interpretation, courts agree with respect to a few best practices, including implementing password protections and restricting access to sensitive areas of facilities.[12] Of course, what is reasonable depends on the facts (the requirement is often stated as "reasonable under the circumstances"[13]). For example, companies that rely on software databases may be required to prove spending on database testing and maintenance.

European Union

In the European Union, there were historically a variety of approaches to the copyright problem of the "simple database" (as in the Feist case). The United Kingdom, for example, found it possible to protect a list of football fixtures as a copyright work. However, in the continental European countries, "sweat of the brow" did not necessarily result in the creation of a protectable work. In the interest of harmonizing intellectual property rights in database creation, the European Union expanded copyright law with a new database right specifically to protect and encourage database creation within the European Union.[14] The EU database right offers protections for databases by reference to the investment in selection or arrangement of the contents of the database.

In practice, the EU database right has perhaps not been as successful as its architects may have hoped. In British Horseracing Board Ltd. And Others v. William Hill Organisation Ltd.[15], the European Court of Justice established that the database right in the information used to create the database is distinct from investment in the selection or arrangement of the contents of the database and found it insufficient to garner database protection through the EU database right.

In many of the likely use cases, the investment would be tied to the company's collection of data, and not in its selection or arrangement. In these cases, the database would not be protected by the EU database right, even if the database had been created in Europe.

The European countries also recognize the concepts of trade secrets and confidentiality obligations. In the United Kingdom, for example, information could be protected from unauthorized use or disclosure under longstanding common law principles, which have recently been codified in the U.K. domestic law

regulations aimed at harmonizing trade secret laws across the European Union, if it can be shown that the information:

- Is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;

- Has commercial value because it is secret; and

- Has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[16]

So, in the United Kingdom, a victim of potential misappropriation could act to protect against the misuse of confidential information or trade secrets that had fallen into the hands of a third party through the wrongful actions of a former employee, even if the employment contract had been imprecise regarding the confidentiality obligations to which the employee had been subject.

Conclusion

Intellectual property laws were enacted before data became a substantial area of investment, and it remains difficult to obtain copyright protection for databases. Trade secret protection is more readily available, although it requires policies and procedures to establish those rights. To maximize the opportunities for legal protection, investors in data innovation should structure their projects with an eye to putting in place and continuing to maintain the best possible case for copyright and trade secret protections under the unique circumstances of the projects.

Richard Assmus, Brad Peterson and Mark Prinsley are partners and Nickolas Card is an associate at Mayer Brown LLP.

[1] https://www.idc.com/getdoc.jsp?containerId=prUS44291818

[2] 17 USC § 102(b).

[3] 17 USC § 101 (emphasis added).

[4] 499 U.S. 340 (1991).

[5] See Key Publications, Inc. v. Chinatown Today Publishing Enterprises Inc., 945 F.2d 509 (2d Cir. 1991), regarding a yellow pages directory and Kregos v. Associated Press regarding a baseball pitching form, 3 F.3d 656 (2d Cir. 1993).

[6] 17 USC § 102(a).

[7] Naruto v. Slater, 2016 WL 362231, at *1 (N.D. Cal. Jan. 28, 2016).

[8] 18 USCS § 1839(3) (emphasis added). In meaning, this definition is very similar to the Uniform Trade Secrets Act adopted in almost all U.S. states.

[9] 18 USCS § 1839(3)(B)

[10] Duggan v. Am. Family Mut. Ins. Co., 2010 WL 1268175 (E.D. Wis. Mar. 30, 2010).

[11] Events Media Network Inc. v. Weather Channel Interactive Inc., 2015 WL 457047, at *7 (D.N.J. Feb. 3, 2015).

[12] Deepa Varadarajan,The Trade Secret-Contract Interface, 103 Iowa L. Rev. 1543, 1557 (2018).

[13] GSI Tech., Inc. v. United Memories, Inc., 2015 WL 1802616, at *4 (N.D. Cal. Apr. 20, 2015).

[14] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[15] C-203/02, November 9, 2004.

[16] Trade Secrets (Enforcement, etc.) Regulations 2018, § 2.