DR. DAVID G. HUGLEY
NATIONAL INSTRUMENTS, AUSTIN.

CONTRACTS RESTRICTING THE USE OF IDEAS

1. Would the ultimate contractual power be the ability to control ideas by contract? Of all the things in which to have contractual rights, would ideas be the most valuable?

The purpose of this article is to shed some light on certain contract practices in the United States that have developed as recently as during the last 20 years, wherein contracting parties attempt to agree upon the restriction of ideas, perhaps in excess of what the intellectual property laws or interests of society may allow.

Two topics in this area are addressed. The first is the prevalent attempted use of trade secret law in contracts, far overreaching reasonable limitations. The second area involves contracting parties' efforts to control competitive use of those ideas which may be demonstrated in software.

Trade secret law in the United States allows for a juridical person to legally protect from disclosure, or collect damages for the disclosure of, information which the person has maintained in secrecy. Physical and informational barriers must have been established and maintained in order for information to qualify as a trade secret and to be qualified for the benefit of legal protection. For example, information needs to have been closely held within a company and not disclosed to others without their agreement to maintain the secret. If the information has been disclosed to others without such agreement, it no longer qualifies as a trade secret. Therefore, if it is necessary for the person or firm to share the information with another party in order to achieve the firm's business objectives, the discloser and recipient contract, with the recipient engaging in a contractual promise not to release the information to others. These contracts, often referred to as "non-disclosure agreements," "confidential disclosure agreements," or "proprietary information agreements" should identify in some way the nature of the secrets to be

disclosed. Freedom of contract allows for a variety of provisions in these contracts, and disclosers often include a provision limiting the uses to which the recipient can put the information, operating almost as a limited license for its use. Most often these "purpose" provisions provide that the only purpose for which recipient can use the information is in furtherance of the business collaboration between the parties, for the benefit of the discloser.

Such contracts prohibiting disclosure can be employed to prevent the publication or communication of the data of the disclosure. A good example would be the prevention of the disclosure of a company's customer mailing list or wage information regarding each of the company's employees. Clearly the company would share that information only with a trusted supplier who would not leak the information to others, and this is a traditional and understandable use of such a contract.

It seems logical that a discloser would include a provision in the contract that the recipient could not utilized the information in furtherance of the recipient's own business.

In the current evolution of this form of contract in the United States, the contracting party playing the role of "discloser" is changing the clauses identifying the "secrets" to be disclosed. Now we observe and encounter provisions entirely vague as to the information to be disclosed. Take, for example, a contract proposed to cover the content of a meeting between two parties. The "information" to be disclosed is then described as "any and all information, whether written or oral, disclosed to Recipient." Suppose, in furtherance of this example, that the Discloser will describe his method of manufacturing goods or the design of a new product. This "information," disclosed orally, in fact may well comprise ideas themselves, perhaps devoid of data.

Recipient, if he has signed the contract, is now forbidden from disclosing any such idea to others. Also, if the contract contains the standard clause providing that Recipient cannot use what is disclosed for any purpose other than his collaboration with the Discloser, Recipient is now under a contractual obligation to forego the use of an entire idea.

These contracts have become pervasive in commercial practice.

A normal firm will be asked to sign many such forms every year. In fact, in many places of business, persons wishing to be admitted to the physical facilities will be "required" to sign, on behalf of his own firm and himself, such a form contract. The contractual effect is that the visitor has agreed to quash, for his own use or even for his own discussion with others, all ideas which may be discussed or in evidence within that facility. Signing such a contract, prior to admission to a facility or meeting, when in ignorance of the ideas which may be proposed, opens the possibility that ideas which are otherwise available in society are quashed by contract. The ubiquitous nature of these contracts in commerce today in the United States leads to the probable consequence that ideas not otherwise legitimately protected by other forms of intellectual property are removed from open circulation in commerce and society through the operation of contracts.

Traditional trade secret law provides limited defenses against accusations of breach of such a contract. If the defendant can prove that the idea was available to him prior to that time from another source, this may provide a defense. The problem then becomes one of proof. Ideas that could never attain the protection of patent law, for example due to lack of novelty or due to obviousness, still may not be presentable from other sources in a form sufficient to provide proof. Obviousness of the idea does not provide a defense to the allegation of breach of contract.

The implied intent of such overreaching non-disclosure contracts is clearly to quell competition. Upon the success of a new product, competitors can search their files in order to ascertain whether the successful company has ever entered into one such vague non-disclosure agreement with them. Then the competitor can allege that the idea was at one time orally disclosed under the contract and that the contract has been breached.

One may ask, "Could not the defendant in this situation simply prove that the idea was not in fact disclosed to them?" In cases where this evidence is provable, the defense has value. However, as noted above, the contracts in practice today regularly provide for no identification of the subject matter at the time of the agreement and

provide that the obligation attains even in the absence of any objective proof or written evidence.

This web of contractual entanglements between firms is intended to subdue competition. The vague and overreaching obligations create an uncertain threat upon the introduction of new products and services. Firms must check their numerous non-disclosure and non-use contracts in an attempt to ascertain their freedom to introduce new products and services. The net social benefit of this contractual expansion of trade secret intellectual property law is called into question.

Traditional forms of intellectual property law are not effectively providing boundaries on this expansion. In the United States, neither patent nor copyright law impairs the spread of restrictions on the use of ideas through the power of this freedom to contract.

So freedom to contract has wrought a restriction on the free use of ideas.

2. In the area of contracting for software programs, the relationship of contract law to intellectual property law has received more judicial attention, although the overall state of the law at this time is not clear.

Software providers originally used contracts to govern the use of their products in the U.S., because Congress and the courts were not sure that software was a proper subject of copyright law.[1] The value of software is in its utility and its object code function rather than a particular work's nonfunctional expressive elements, so copyright seemed questionable as the properly applicable law. The software industry sought contract protection for their programs.[2] Software authors utilized contracts privately to specify what rights were granted or transferred, and which were excluded, using their own definitions. They described the products they offered, and controlled their liability. „Bargained agreements" were used for software developed specifically for a user; „unbargained shrinkwrap agreements" were utilized for mass market distribution of software.[3] The National Commission on New Technological Uses of Copyrighted Works recommended software copyrightability to the Congress, and in addressing the problem for the first time, the copyrightability of software became law in the 1976 Copyright Act.[4]

Protection of software as a copyrighted literary work by the courts then occurred.[5] Copyright law is now computer software's primary source of legal protection in the United States, and unbargained shrinkwrap licenses on mass market software are prevalent.[6]

Copyright law, however, is rich with a history spanning hundreds of years when software did not exist. The U.S. Constitution provides that the purpose of copyright law is „to promote the progress of science and the useful arts."[7] Section 102(B) of the Copyright Act states, „in no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle or discovery regardless of the form in which it is described, illustrated or embodied in such work."[8]

The United States Supreme Court noted in *Sony Corp. of America v. Universal Studios, Inc.*, that copyright law seeks to achieve a balance between „the interest of authors...in the control and exploitation of their writings...on the one hand, and society's competing interest in the free flow of ideas...on the other."[9] An important part of the balance is permitting or encouraging the public to copy unoriginal material. When courts were dealing with ordinary text writings, they attempted to strike this balance by distinguishing between ideas and expression. Ideas remained in the public domain. Courts recognized that if an idea could be protected, intellectual progress would be slowed. Requiring payment for a certain author's expression of the idea still left opportunity for others to express the idea in their own creative ways.

Courts then faced this same policy issue after 1976, with regard to software programs. Courts promptly diverged in this analysis, with a confusing set of tests to be applied to software, including „the abstractions test," the „successive filtering method" and even implementing (and then reversing) the „look and feel" test. It is not the purpose of this discussion to analyze these confusing attempts to define copyright coverage of software. The point here is that software vendors were (and still are) uncertain what is protected. Software licensors are returning to contract law to secure greater rights than those afforded by copyright law.

One important area in this regard is the subject of reverse engi-

neering. Software vendors structure contracts to circumvent an important limitation on their rights as copyright holders.[10]

A software programmer writes his program in human readable „source code." A compiler program translates the source code into object code, which is only machine-readable. Commercial programs are then distributed in object code only. Therefore, the uncopyrightable elements and ideas are only available through the derivation of the software's human readable source code through „decompilation" and „disassembly" reverse engineering processes.[11] Even though intermediate-copies or translations are made in this process, United States courts have uniformly held that decompilation and disassembly are permitted under copyright law if they are undertaken for the purpose of obtaining specifications needed to make interoperable or competitive products, and if this is the only means to access the uncopyrightable elements.[12] Thus copyright, balanced with a reasonable scope of fair use, protects the „fair use" of ascertaining the ideas behind the expression to allow the creation of compatible and competitive products.

As a response to this Fair Use Doctrine allowing reverse engineering under copyright law, firms attempt to prohibit reverse engineering of their software by employing contractual devices which include prohibitions against reverse engineering in most off-the-shelf open market software shrinkwrap licenses. (Beneath a clear outer wrapping is a visible license agreement, which states that by removing the plastic shrinkwrap enclosing the software, the end user agrees to the terms of the license.[13]) This license almost always includes a prohibition on reverse engineering.[14]

The U.S. Supreme Court found these shrinkwrap agreements to be generally enforceable.[15] However, the debate regarding a shrinkwrap license prohibiting reverse engineering has created tension between state contract law and copyright law.[16] In the case of *Bowers v. Baystate Technologies*, the U.S. Court of Appeals for the Federal Circuit upheld the conclusion that a shrinkwrap license can bar reverse engineering of a software program, adopting a blanket rule that such restrictions should never be preempted by the Federal Intellectual Property Laws.[17]

IP Laws grant certain exclusive rights or monopoly privileges to

authors, but the privileges are ultimately associated with public interests. Courts and legislatures saw the need to limit the scope of the IP monopoly. Copyright „fair use" doctrine reflects this need for limitations on copyrights. The Fair Use Doctrine exempts a reverse engineer from liability for certain decompilation that would otherwise infringe in an attempt to limit a copyright holder's exclusive right in order not to stifle creative efforts by competitors through exploring information committed to the public domain through copyright. Effective competition requires software developed by competitors to be compatible with existing standard systems. So reverse engineering should be allowed in order to accomplish compatibility. In the case of *Eichel v. Marsan*, the Court held that: if an author, by originating a new arrangement and form of expression of certain ideas or conceptions, could withdraw these ideas or conceptions from the stock of materials to be used by other authors, each copyright would narrow the field of thought open for development and exploitation in science, poetry, narrative and dramatic fiction, and other branches of literature would be hindered by copyright instead of being promoted.[18]

Justice Brandeis said that „the noblest of human productions-knowledge, truths ascertained, conceptions and ideas – become, after voluntary communication to others, free as the air to common use."[19] In terms of economic efficiency, ideas or concepts, because they are basic building blocks of creation, should be free for use. If decompilation is not allowed, this results in a de facto monopoly by the owner of the copyright over the functional aspects of the works.

The Copyright Act was intended to promote growth and creative expression based on the dissemination of other creative works and the unprotected ideas contained in those works.[20] The ultimate aim of the Copyright Act is to benefit the public through the distribution of knowledge, rather than to reward individual authors.[21] Even though copyright law grants an author certain exclusive rights, the author should not use these rights to maintain its dominance and control in a manner adverse to public policy.

Uncertainty of freedom to contract in this area is serious. A shrinkwrap license can impose very restrictive terms, or a prohibi-

tion on reverse engineering, eliminating the right to create a compatible or competitive product.

Restrictions on software reverse engineering through anticompetitive conduct or copyright license agreements may constitute copyright misuse or a violation of antitrust laws. The Copyright Misuse Doctrine was first established in the case of *Lasercomb America, Inc., v. Reynolds*, which expressly upheld the defense against an infringement action.[22] Lasercomb, the copyright owner, included in its license agreement contractual provisions, which precluded licensees from developing competitive software for a period of 99 years.[23] The Court held that the underlying restrictive license agreement went further than protecting against copying and was used in a manner adverse to the public policy embodied in a copyright grant.[24]

Copyright misuse is a defense against an allegation of copyright infringement. Conduct underlying a copyright misuse defense in an infringement case may serve as a basis for antitrust liability. However, an antitrust claim requires proof of additional elements: market power, competitive injury, anticompetitive intent, etc. However, proof of an antitrust violation can often serve to establish copyright misuse.[25] An antitrust claim gives rise to damages, whereas copyright misuse is an absolute defense against a claim of copyright infringement.

In some cases, a contract prohibiting software reverse engineering is subject to copyright misuse or antitrust liability. In the case of *Alcatel U.S.A., Inc., v. DGI Technologies, Inc.*, the United States Court of Appeals for the Fifth Circuit ruled that a license agreement prohibiting reverse engineering constituted copyright misuse.[26] If a license, in order to extend copyright protection beyond its proper scope, prevents competitors from detecting or understanding unprotected ideas or functional elements embodied in a computer program and from developing competing or interoperable products, it constitutes anticompetitive use of the copyright. This finding requires also a finding that federal copyright law preempts state contract law. Alternatively, the state court could find that the term in shrinkwrap license is unconscionable in this contract of adhesion. The 50 states vary in their contract law as to the enforceabili-

ty of all terms of shrinkwrap license. The „Uniform Computer Information Transaction Act" is proposed model legislation for the states in the law of software contracting, but has only been adopted by two states: Maryland and Virginia. It provides for enforceability of all terms of a shrinkwrap license including prohibition of reverse engineering and restrictions on interoperability.

A shrinkwrap contract in a mass market application program is not negotiated and is a standard form contract. As such, it may be unenforceable under the contract doctrine of unconscionability. Courts could choose not to enforce certain terms. The contract is a subject of state law. State common and statutory laws have often clashed with federal laws regarding patents and copyrights. A state law rule or contract term may be invalidated by federal preemption. A contract term that varies the effect of a federal law that cannot be varied by agreement under the Copyright Act may be unenforceable. Therefore, an antireverse engineering provision under a licensing contract may be unenforceable if it denies federally created fair use. Section 301(A) of the Copyright Act is intended to preempt common law or statutes of any state which are equivalent to the exclusive federal copyright. A contractual restriction on reverse engineering expressly narrows the scope of fair use rights, which places an arbitrary power in the hands of the copyright holder going far beyond the protection provided by law.[27] In *Symantec Corp. v. McAfee Associates, Inc.*, the Court held that a software license prohibiting reverse engineering was preempted by Section 301 of the Copyright Act.

In *Vault Corp. v. Quaid Software, Limited*, the United States Court of Appeals for the Fifth Circuit used the Supremacy Clause of the U.S. Constitution to set aside a contractual prohibition upon reverse engineering, noting that the prohibition „conflicts with the rights of computer program owners under Section 117" of the Copyright Act and „touches upon an area of federal copyright law."[28]

Contract terms prohibiting reverse engineering may be unenforceable because they are unconscionable. As explained in the official comments to the "Uniform Computer Information Transaction Act" (the model act mentioned earlier), the basic test is whether, in

light of the general commercial background and the commercial needs of the particular trade or case, the terms involved are so one-sided as to be unconscionable under the circumstances existing at the time the contract was made. The principle is one of prevention of oppression and unfair surprise and not of disturbance of alloca-tion of risks because of superior bargaining power.

Procedural unconscionability particularly applies in the context of adhesion contracts, as it has been defined in the model act as "the lack of a meaningful choice, considering all the circumstances sur-rounding the transaction including the manner in which the cont-ract was entered, and whether each party had a reasonable oppor-tunity to understand the terms of the contract, and whether the important terms were hidden. If a Court finds a contract or term thereof to be unconscionable, the Court may refuse to enforce the contract, enforce it without the unconscionable term, or limit the application of the term in order to avoid an unconscionable result in order to prevent oppression and unfair surprise, and because of superior bargaining power.[29] Basically, the question is whether the term involved is so one-sided and unfair as to be unconscionable. Also, a contract of adhesion is one to which one of the parties must adhere to the powers of a monopolist on a take-it or leave-it basis. In *Vault Corp. v. Quaid Software, Ltd.*, the Court found the shrinkwrap license to be unenforceable as a contract of adhesion.

The *Bowers v. Baystate Technologies* decision by the Court of Appeals for the Federal Circuit is in conflict with other Federal Courts of Appeals decisions. A shrinkwrap license attempting to bind the purchaser to the vendor's terms offers only the choice of not buying the software. This self-proclaimed contract provides a copyright owner the superior power to override public law with a contract of adhesion.[30]

Software producers now go even further than prohibiting reverse engineering. They attempt to go so far as using the contract to prohibit the licensee from "attempting to determine the method of operation" of the software; and also contain provisions prohibit-ing the creation of competitive products and the creation of com-patible products without the licensor's approval.

Please consider this example clause taken from the license for a

software product currently shipping in the United States, which states:

"NONCOMPETITION. Licensee agrees not to use the Program ...to distribute its own or a Third Party's Application, a principal purpose of which, as reasonably determined by [Licensor] is to perform the same or similar functions as Programs licensed by [Licensor] or which replaces any component of the Programs. Licensee shall not otherwise use the Programs to compete with the products or businesses of [Licensor] ..."

These provisions, as well as a prohibition on reverse engineering, may be subject to antitrust scrutiny under 1 of the Sherman Act. Though no claim regarding an anti-reverse-engineering provision has been brought as of now, a number of potential antitrust issues arise. Section 1 forbids any contract in restraint of trade. Anti-reverse engineering clauses restrain trade within the meaning of the statute since they limit the ability to develop comparable products, if the nature of the restraint would be characterized as unreasonable under either "per se illegality" or the "rule of reason." The "rule of reason" would most likely be applied, weighing a broad inquiry into the nature of the defendant's intent and purpose, justifications for the restrictions, competitor's competitive position, and the effect of the challenged restrictions.

IN CONCLUSION,

The various legal doctrines analyzed above do not offer any clear guidance as to how the issue of the conflict between copyright law and contract law will be resolved. None of these doctrines define, within a predictable system, on the basis of what criteria contractual provisions will be held unenforceable despite the fact that they excessively restrict the users' rights in the context of copyright law. For example, the copyright misuse doctrine could potentially be used to invalidate contractual provisions that are anticompetitive, but little guidance currently exists as to its scope of application. The doctrines of public policy and unconscionability, considered as two general doctrines of contract law, are not specific enough to

deal with the issue. These doctrines could only be helpful if the courts adapted them to the specific characteristics of software licensing transactions. However, even though the doctrine of unconscionability is overbroad, this doctrine might be helpful in showing that a contract will be considered oppressive, and thus likely to be unconscionable, because it is offered on a take-it-or-leave-it basis.

The Uniform Computer Information Transactions Act "Fundamental Public Policy Exception" provides that: "if a term of a contract violates a fundamental public policy, the court may refuse to enforce the contract, enforce the remainder of the contract without the impermissible term, or limit the application of the impermissible term so as to avoid a result contrary to public policy, in each case to the extent that the interest in enforcement is clearly outweighed by a public policy against enforcement of the term."

The Uniform Computer Information Transactions Act does not further define what is meant by fundamental public policy. The official commentary identifies three concepts which may qualify as fundamental public policy: innovation, competition, and freedom of expression (fair comment and fair use). It states:

"Innovation policy recognizes the need for a balance between protecting property interests in information to encourage its creation, and the importance of a rich public domain upon which most innovation ultimately depends. Competition policy prevents unreasonable restraints on publicly available information in order to protect competition. . . . Free expression and the public interest in supporting public domain use of published information also underlie fair use as a restraint on information property rights."

There is no clear public policy that prevents parties from contracting around the limitations of copyright law. The identification of innovation, competition and freedom of expression as the key values that are potentially threatened by excessively restrictive contracts should be particularly considered.

Indeed, these are the same fundamental policies that courts in the United States should creatively learn to apply to the unbridled use of overreaching non-disclosure agreements identified in Section 1.

NOTES

1 Brett Frischmann and Dan Moylan, *The Evolving Common Law Doctrine of Copyright Misuse: A Unified Theory and Its Application to Software*, 15 Berkeley Technology Law Journal, 865 (2000).

2 Maureen A. O'Rourke, *Drawing the Boundary Between Copyright and Contract, Copyright Preemption of License Terms*, 45 Duke Law Journal, 479 (1995).

3 Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 Southern California Law Review, 1239 (1995).

4 Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 Stanford Law Review, 1045 (1989).

5 Frischmann and Moylan, supra note 1.

6 Lemley, supra note 3.

7 U.S. Constitution, Article 1, Section 8, Clause 8.

8 17 U.S.C. 102(B) 2000.

9 464 U.S. 417 (1984).

10 Dennis S. Karjala, *Copyright Owners' Rights and Users' Privileges on the Internet, Federal Preemption of Shrinkwrap and Online Licenses*, 22 University of Dayton Law Review, 511 (1997).

11 Peter S. Menell, *Envisioning Copyright Laws Digital Future*, 46 New York Law School, Law Review, 63 (2003).

12 *Sega v. Accolade,* 977 F.2d 1510 (9th Cir. 1992); *Atari v. Nintendo,* 975 F.2d 832 (Fed. Cir. 1992).

13 Greg Weiner, *Reverse Engineering as a Method of Achieving Compatibility in the Computer Industry*, 6 University of Baltimore Intellectual Property Law Journal, 1 (1997).

14 Jonathan Band Masanobu Katoh, *Interfaces on Trial; Intellectual Property and Interoperability in the Global Software Industry*, 220 (Westview Press, 1995).

15 *ProCD v. Zeidenberg*, 86 F.3d 1447 (Seventh Circuit, 1996).

16 *Bowers v. Baystate Technology, Inc.*, 32 F.3d 1317, (Fed. Circuit, 2003).

17 Mark Lemley brief amicus curiae in support of petitioning for a panel rehearing in *Bowers v. Baystate Technologies*, 9 (September 2002).

18 *Eichel v. Marsan*, 241 F. 404 (Southern District of New York, 1913).

19 *International News Service v. Associated Press*, 248 U.S. 215 (1918) (Brandeis, J., Dissenting).

20 *Sega v. Accolade*

21 *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

22 911 F.2d 970 (Fourth Circuit, 1990).

23 See id. at 973.

24 See id. at 978.

25 See Robert H. Land and Sturges M. Sopen, *Reverse Engineering of Computer Software and U.S. Antitrust Law*, 9, Harvard Journal of Law and Technology, 237 (1996).

26 166 F.3d 772 at 793 (Fifth Circuit, 1999).

27 953 F.2d 731 at 741 (Second Circuit, 1991).

28 847 F.2d 255 (Fifth Circuit, 1998).

29 *Intel Corp. v. Intergraph Corp.*, 195 F3d 1346 (Fed. Circuit, 1999).

30 See L. Ray Patterson and Stanley W. Lindberg, *The Nature of Copyright: A Law of Users' Rights* (1991).