

UIC John Marshall Journal of Information Technology & Privacy Law

Volume 13
Issue 1 *Journal of Computer & Information Law*
- Fall 1994

Article 2

Fall 1994

The Copyright and Trade Secret Protection of Communication Software: Placing a Lock on Interoperability, 13 J. Marshall J. Computer & Info. L. 17 (1994)

Steven N. Dupont

Follow this and additional works at: <https://repository.law.uic.edu/jitpl>



Part of the [Computer Law Commons](#), [Intellectual Property Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Steven N. Dupont, The Copyright and Trade Secret Protection of Communication Software: Placing a Lock on Interoperability, 13 J. Marshall J. Computer & Info. L. 17 (1994)

<https://repository.law.uic.edu/jitpl/vol13/iss1/2>

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

THE COPYRIGHT AND TRADE SECRET PROTECTION OF COMMUNICATION SOFTWARE: PLACING A LOCK ON INTEROPERABILITY

By STEVEN N. DUPONT†

I. INTRODUCTION

There has been a storm of controversy brewing in the contentious area of copyright protection of computer software. The scope and extent of copyright protection in computer software is no stranger to controversy. Unlike the more aesthetic works protected by the copyright laws, software is an area of remarkably rapid change. The federal courts are continually shaping copyright law to better fit both the changing technological and business environments. Consequently, the extent of property rights in such works frequently involves thorny questions of policy that pit the interests of the copyright proprietor against the demands of the software industry. This time, industry demands for compatible and interoperable¹ computing machinery are steering the course of the legal conflict.

Recently, the controversy has come to a head in the seemingly innocuous form of spreadsheets, menu structures and “macros.” In *Lotus Development Corp. v. Borland International, Inc.*,² Judge Keeton ruled that Borland’s “Key Reader” program — a software module that inter-

† Attorney, Intellectual Property and Computer Law Department of Jenner & Block, Chicago, Illinois. The author would like to thank Jerome Roberts for his advice and encouragement, and Kenneth Port for his comments on an earlier draft of this Article.

1. Compatibility ensures that software written for one system will operate identically on another or that one vendor’s software will work with data files or programs written for another vendor’s product. Interoperability ensures that disparate machines or other systems will work together in harmony. Although these are different concepts, they possess a common element: they both require access to some of the secrets of the underlying systems. Thus, the terms are used interchangeably throughout this article.

2. 831 F. Supp. 223 (D. Mass. 1993).

prets macros³ written by users of the Lotus 1-2-3 spreadsheet program so that they can be used with the Borland "Quattro" spreadsheet program — infringes Lotus' copyrights in the Lotus 1-2-3 menu structure.⁴ In so doing, the judge rejected Borland's argument that Lotus' menu structures are uncopyrightable because they are elements that must be copied in order to achieve compatibility with user macros written for the Lotus 1-2-3 program.⁵

Judge Keeton's decision has drawn vociferous protest.⁶ Indeed, a formidable group of law professors and industry organizations have teamed up to attack the decision on appeal.⁷ The position of the defendants and their amicus on appeal goes far beyond a mere attack on the copyright status of certain elements of a spreadsheet program. Rather, they are urging the court to recognize a broad right of competitors (and others) to develop compatible software.

The *Lotus* case has attracted such notables, in part, because it offers a rare opportunity to effect a dramatic change in the law's policy objectives. The debate implicates each of the intellectual property law's twin guiding principles; namely, that the law must encourage invention and innovation while simultaneously promoting the dissemination of ideas and fostering competition.⁸ In the balance, the "property rights" of the individual rightholder are given little weight.⁹ Accordingly, in determining the proper scope of protection enjoyed by computer software, the

3. "Macros" are user-written lists of commands or statements (in this case, lists of spreadsheet commands) that the user wishes to be executed together to perform a given complex function.

4. *Lotus Development*, 831 F. Supp. at 235.

5. This issue was actually decided in an earlier opinion dealing with cross motions for summary judgement by Lotus and Borland. See *Lotus Development Corp. v. Borland International, Inc.*, 799 F. Supp. 203 (D. Mass. 1992).

6. See, e.g., Rob Rossi, *Valley Lines Up Behind Borland*, THE RECORDER Dec. 15, 1993, at 1; John S. McCright, *Computer Experts Ask for New Lotus Decision*, BOSTON BUS. J. Dec. 4, 1993, at 4; Paul Goodman, *Lotus-Gorland Decision Casts Long Shadow on Future of Open Systems*, PC WEEK Sept. 27, 1993; Pamela Addo, *Controversy Clouds Borland/Lotus Suit*, COMPUTER DEALER NEWS Sept. 20, 1993, at 6; Martin Glenn & Dale M. Cendali, *Lotus Case Highlights Copyright Issues and High-Tech Problems*, THE NAT'L L.J. Nov. 1, 1993, at S18.

7. At the time this article was written the *Lotus* decision is on appeal before the First Circuit U.S. Court of Appeals. The American Committee for Interoperable Systems and professors Dennis Karjala and Peter Mennel were among those filing amicus briefs supporting the defendant's position on appeal. See ACIS, *Law Professors Support Borland's Appeal to 1st Circuit*, COMPUTER INDUSTRY LITIG. REP., Jan. 20, 1994, at 18033.

8. See, e.g., *Harper & Row Publishers, Inc. v. Nation Enterprises.*, 471 U.S. 539, 546 (1985) (copyright law); *Loctite Corp. v. Ultraseal, Ltd.*, 781 F.2d 861 (Fed. Cir. 1985) (patent law).

9. See *Mazer v. Stein*, 347 U.S. 201, 219 (1954) (the philosophy behind the constitutional mandate for patent and copyright law is to "advance public welfare through the talents of authors and inventors in 'Science and the useful Arts'"); *Feist Publications, Inc. v.*

courts must pay heed to industry demands for interoperable products. And if compatibility and interoperability is a policy goal that is to be pursued through the courts, it may inevitably affect legal doctrine in areas of the law besides copyright.

What effect would a "compatibility right" have on software developers? The answer depends largely upon the kind of software under development. Within the category of works most affected by such a change are software interfaces.¹⁰ Interfaces — whether internal interfaces or external interfaces, such as communications software — are absolutely vital in achieving compatibility with the systems they connect. Therefore, a court under the sway of compatibility arguments would limit the legal protection it enjoys. On the other hand, interface software generally, and communications software in particular, is an economically vital activity that must be encouraged through legal protection. As a result of this dilemma, the status of intellectual property protection for communications software is at best uncertain.

In an attempt to dispel some of this uncertainty, this article examines the legal status of communications software in the current legal environment. In Part II, this article discusses the technical components of a communications software system in the context of a fictitious software developer. In Part III, the intellectual property protection of communications systems is discussed. The article analyzes the traditional scope of copyright and trade secret protection, and, in particular, how the compatibility debate has affected the scope of legal protection in communication software. Finally, Part IV of the article discusses the antitrust implications faced by the communication software developer and how compatibility concerns affect the analysis of antitrust doctrine. This article concludes that, based on current law, economically adequate legal protection for communication software can still be achieved through a combination of copyright and trade secret protection. However, the protection of such systems is an ever-changing landscape. Talk of "compatibility rights" has taken on a more general and pervasive character in several recent court decisions. As a result of the unique role played by communications software in modern computer systems, the quest for interoperability may soon place what was once protected expression within the public domain.

Rural Telephone Service Co., 499 U.S. 340 (1991) (the main purpose of copyright law is not to reward talent).

10. Generally, interfaces ensure that the software elements within a computer work together efficiently. Communications software is a special kind of interface; it ensures that multi-computer systems work together efficiently.

II. THE COMMUNICATION SOFTWARE ENVIRONMENT¹¹

A. THE COMMERCIAL ENVIRONMENT

Lest one think that communication software is solely the concern of hordes of sneaker-clad "hackers" toiling in front of a computer terminal, consider the plight faced by a fictitious equipment manufacturer, LADIX International, Incorporated. LADIX has developed an innovative hardware and software system designed to allow its process equipment to communicate in an integrated computer network. The system uses a non-standard communication protocol to accomplish its ends. The system also contains a "security" feature which ensures that only authorized equipment will be permitted access to the network. Additionally, LADIX would like to supply applications software packages for use with its communication network. This software would allow display of real-time process information and would store information in a historical database for trending and off-line analysis.

LADIX has a number of business objectives for its new product. First, LADIX wishes to keep its technology proprietary. That is, it wants to bar competing equipment manufacturers from developing compatible equipment unless they are LADIX licensees. Second, LADIX wants only licensed software developers to design and sell compatible applications programs. Note that for LADIX these are not purely profit-driven objectives. In the process control industry, computer glitches can have serious consequences. Therefore, LADIX is very concerned with protecting its customer base from the influence of potentially substandard products.

How is LADIX to accomplish its goals? As we shall see, LADIX's software will qualify for copyright and trade secret protection.¹² However, will the scope of the rights obtained bar a competitor from developing compatible technology (either applications software or process equipment capable of utilizing the LADIX protocol)? Moreover, if LADIX's efforts are particularly successful, and its communication system becomes a *de facto* industry standard, will its rights be curtailed? Before these questions can be answered, a brief digression into the arcane world of communication software programming is necessary.

11. Much of the following discussion is based on the author's experience in the communications software industry.

12. LADIX's software may also qualify for patent protection. Patent protection would cover a distinct aspect of the software not protected under copyright laws, namely, the process or method of operation. 17 U.S.C. § 102(b) (1988). Under the Federal Circuit Court's recent pronouncements in *Arrhythmia Research Tech. v. Corazonix Corp.*, 958 F.2d 1053 (Fed. Cir. 1992), computer programs that are part of a patentable process or device may be patentable. However, few programs satisfy the patent laws rigorous requirements of novelty and nonobviousness. Thus, the limits of patent protection are not affected by the concerns for interoperability. Accordingly, the patent protection of communications software is outside the scope of this article.

B. THE TECHNICAL ENVIRONMENT

Computer systems are essentially a collection of interfaces. At the highest level, applications software creates an interface with the human operator of the computer system.¹³ At the lowest level, usually within the operating system of the computer, are interfaces that permit access to peripheral devices such as disk drives and displays. Communications systems lie at this level. The communications system of a computer permit the error-free exchange of messages between the intelligent devices that comprise the distributed system. Today, high-speed computer networks provide the backbone for this communication.

A distributed system consists of multiple autonomous computers linked in a way that is transparent to the user.¹⁴ The user of a distributed system need not be concerned with the details of the underlying system. The user merely issues a command to send a message to a specified location and the system assures that the addressed device receives the message error free and in a format the device can understand. This transparency is accomplished by using a sophisticated architecture consisting of multiple layers of "protocols" usually implemented in software.¹⁵ Protocols are a set of rules which govern data exchange between the protocol layers.¹⁶ Protocols specify the format, both temporal and spatial, of the data that is transmitted between the protocol layers. A common protocol implementation among all the devices in the system is vital to ensure proper communication.

The tangible significance of a communication system is illustrated by the evolution of IBM's Basic Input-Output System (BIOS) for the IBM-PC. BIOS is a ROM-based¹⁷ program that controls access to the various peripheral devices attached to the PC, *i.e.* disk drives, printers,

13. The copyright protection of computer user interfaces is itself a controversial subject. See cases cited *supra* note 10. The scope of protection in this technology is beyond the scope of this paper.

14. ANDREW S. TANENBAUM, *Computer Networks 2* (1989).

15. *Id.* at 14. The International Standards Organization (OSI) provides a reference model for network designers. The model consists of seven independent layers. Each layer provides specific communication services. At the lowest level is the *physical layer*. This layer is concerned with the actual communication medium and thus is hardware dependent. At the highest level is the *applications layer*. This layer allows applications software a generic, device-independent interface to the distributed system. Interfaces define how data is exchanged between the adjacent layers such that each layer operates independently of the other layers. *Id.*

16. *Id.* at 10.

17. "ROM" is an acronym for "read only memory." These are chips inserted on the circuit board of a computer that contain fixed programs and data that are usually part of the computer's operating system. These programs are often referred to as "firmware."

screen displays and the keyboard.¹⁸ In the IBM-PC environment, the operating system provides user access to these devices by issuing "calls" to the relevant functions within the BIOS program. Consequently, application programs need not be concerned with the particulars of the various devices. BIOS ensures that data is read from or written to the correct locations within the various data sources in proper format.

Programs like BIOS are essential in achieving total machine compatibility. Originally, IBM envisioned that the MS-DOS operating system would provide access to the BIOS program. This would ensure that all MS-DOS applications software would be compatible with all machines capable of running MS-DOS. However, applications software developers found this method of access too inefficient. Accordingly, programmers by-passed the recommended route by issuing calls directly to IBM BIOS. As a result, PC clone manufacturers were forced to duplicate BIOS functions in order to create an IBM-PC compatible machine.¹⁹ The immense popularity of the IBM-PC platform fueled a potent market demand for IBM-PC compatibles. As a result, BIOS has become a *de facto* communication standard for the PC market.²⁰ To achieve such universal appreciation of one's work is a developer's best hope. However, as we shall see, the program's success may be its undoing.

III. COPYRIGHT AND TRADE SECRET PROTECTION OF COMMUNICATION SOFTWARE

A. COPYRIGHT PROTECTION

It is no longer seriously disputed that computer software is protected by copyright law.²¹ Surprisingly, computer programs have been treated within the category of protected works known generally as "literary works."²² Similar to other literary works, a computer program must be

18. NETBIOS is a subset of PC BIOS that controls access to computer networks attached to the PC.

19. Thomas C. Vinje, *The Development of Interoperable Products Under the EC Software Directive*, 8 THE COMPUTER LAW, 1, 3 Nov. 1991.

20. *Id.*

21. See, e.g., *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240 (3d Cir. 1988), *cert. dismissed*, 464 U.S. 1033 (1984); *Whelan Assocs., Inc. v. Jaslow Dental Laboratory, Inc.*, 797 F.2d 1222 (3d Cir. 1986), *cert. denied*, 479 U.S. 1031 (1987). However, agreement is not unanimous, see, e.g., Pamela S. Samuelson, *CONTU Revisited: The Case Against Copyright Protection for Computer Programs in Machine-Readable Form*, 1984 DUKE L.J. 663 (1984).

22. The House Report for the 1976 Act explains that the term "literary work does not connote any criterion of literary merit or qualitative value: it includes . . . computer data bases, and computer programs. . . ." H.R. REP. NO. 1476, 97th Cong., 2d Sess. 54 (1976). Indeed, the recent legislation implementing the NAFTA trade agreement makes explicit that computer programs are to be protected under copyright law as literary works. Pub. L. No. 103-182 (Dec. 8, 1993).

“an original work of authorship” to qualify for copyright protection.²³ Fortunately, copyright’s “originality” requirement demands only some act of independent creation on the part of the author.²⁴ Thus, the great majority of computer programs qualify as original works of authorship and hence are “copyrightable.”²⁵ A far more interesting question, however, is the scope of copyright protection afforded a computer program. Because the unique nature of software makes it so unlike other “literary works,” well-worn copyright principles find difficult application. However, through experience, courts and commentators have become adept at tailoring old principles to new situations and at inventing new principles where necessary.

1. *The Scope of Protection I: The Idea / Expression Dichotomy*

As the Supreme Court recently exclaimed, “the mere fact that a work is copyrighted does not mean that every element of the work may be protected.”²⁶ Section 102(b) of the Copyright Act states that copyright protection does not extend to any “idea, procedure, process, . . . or method of operation.”²⁷ By the teachings of *Baker v. Selden*²⁸ and its progeny, if a particular “element” of a work is necessary to express its underlying idea, or is one of but a limited number of expressions of the idea, that element is uncopyrightable.²⁹ Thus, under the “merger doctrine”, the courts must draw a line between what is copyrightable expression and what are uncopyrightable ideas.

It is, perhaps, not surprising that copyright protection extends to a program’s “literal elements” — its source and object code.³⁰ Yet drawing the line here leaves much of the software designer’s creative input unprotected. Moreover, the courts have long extended copyright protection in literary works beyond the written text to “non-literal elements”, including such amorphous concepts as plot devices and “total concept and

23. 17 U.S.C. § 102(a) (1988).

24. See *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53 (1884); *Alfred Bell & Co. v. Catalda Fine Arts, Inc.* 191 F.2d 99, 103 (2d Cir. 1951); *Feist Publications, Inc. v. Rural Telephone Serv. Co.*, 499 U.S. 340, 345 (1991) (originality requires only some act of independent creation).

25. See RAYMOND T. NIMMER, *THE LAW OF COMPUTER TECHNOLOGY* ¶ 1.02 (1992). See *supra* note 21.

26. Feist, 499 U.S. at 348.

27. 17 U.S.C. § 102(b) (1988).

28. 101 U.S. 99 (1879). In fact, §102(b) of the Copyright Act is a codification of the principle announced by the Supreme Court in *Baker*.

29. See *Id.* at 103. In *Baker*, the court ruled that those elements of an accounting textbook that were “necessary incidents” to the accounting method the book discloses are uncopyrightable ideas. See also *Morrissey v. Proctor & Gamble Co.*, 379 F.2d 675, 678 (1st Cir. 1967).

30. *Franklin*, 714 F.2d at 1246-47.

feel.³¹ In *Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.*,³² the Third Circuit Court of Appeals, reasoning by analogy, found the old principle equally applicable to the new subject matter.³³ According to the court, copyright in computer software protects not only object and source code, but also a program's "structure, sequence and operation," or "SSO."³⁴ SSO, like plot devices in a literary work, represents the many layers of abstractions in a computer program. It extends from detailed structure, such as algorithms and data structure, to the software's main purpose.³⁵

Yet somewhere within this continuum, the line between protected expression and unprotected process or idea must still be drawn. To the *Whelan* court, the line was clearly defined. According to the court, the "idea" of a computer program is its function, or purpose, and everything that is not necessary to that purpose is copyrightable expression.³⁶ This seemed to many to be a rather sweeping pronouncement.³⁷ Recently, courts given the task of fashioning practical tests for copyright infringement have found the *Whelan* formula unworkable.

2. *The Scope of Protection II: Idea/Expression Dichotomy in the Infringement Context*

In order to prove copyright infringement, a plaintiff must demonstrate that the defendant's work is "substantially similar" to his own.³⁸ Substantial similarity is a term of art that is shown to exist only where the similarities between the plaintiff's and defendant's work involve copyrightable elements.³⁹ Here, the principles described above focus on the task of determining whether those elements copied from the plaintiff's work are copyrightable expression or uncopyrightable ideas. The

31. See *Nichols v. Universal Pictures Corp.*, 45 F.2d 119, 121 (2d Cir. 1930), cert. denied, 282 U.S. 902 (1931) (copyright "cannot be limited literally to the text, else a plagiarist would escape by immaterial variations"); *Sid & Marty Krofft Television Prod., Inc. v. McDonald's Corp.*, 562 F.2d 1157, 1167 (9th Cir. 1977) (similarities in "total concept and feel" between H.R. Pufnstuf and McDonaldland characters is basis for infringement).

32. 797 F.2d 1222 (3d Cir. 1986), cert. denied, 479 U.S. 1031 (1987).

33. *Id.* at 1234 ("By analogy to other literary works, it would thus appear that the copyrights of computer programs can be infringed even absent copying of the literal elements of the program.")

34. *Id.* at 1241.

35. *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 9 F.3d 823, 835 (10th Cir. 1993).

36. *Whelan*, 797 F.2d at 1236.

37. See, e.g., Dennis S. Karjala, *Copyright, Computer Software, and the New Protectionism*, 28 JURIMETRICS J. 33 (1987); Peter G. Spivack, *Does Form Follow Function? The Idea/Expression Dichotomy in Copyright Protection*, 35 U.C.L.A. L. REV. 723, 747-55 (1988).

38. *Whelan*, 797 F.2d at 1232.

39. *Id.* See also *Brown Bag Software v. Symantec Corp.*, 960 F.2d 1465, 1475-77 (9th Cir. 1992).

tests designed by the courts for making these determinations are pragmatic rather than dogmatic.⁴⁰ They open the door to the much-loved “policy considerations” that permeate the academic literature on the subject of software copyright.

Recently, the Second Circuit in *Computer Associates International v. Altai, Inc.*,⁴¹ devised such a test for determining copyright infringement of computer software. The court criticized the *Whelan* court’s “meta-physical distinctions” between idea and expression.⁴² Rather than embodying a single idea, the court reasoned that a computer program is composed of many levels of abstraction and thus is composed of several “ideas.”⁴³ Therefore, under the *Computer Associates* analysis the work must first be “dissected” into its structural components; next, those components must be “filtered” in order to separate ideas from the copyrightable expression; and finally, the “core of protectable expression” found in step 2 must be compared with the material within “the structure of the allegedly infringing program” to determine whether the programs at issue are substantially similar.⁴⁴

It is at the second step, or the “filtering” procedure, where the court must reckon with the issue of compatibility. The *Computer Associates* court remarked that certain elements are uncopyrightable if they are “dictated by” certain external factors.⁴⁵ According to the court, these factors include public domain software, program efficiency, computer specifications, compatibility with other programs, and customer and industry demands.⁴⁶ The rationale behind this filtering procedure harkens back to basic copyright principles. Elements “dictated by” things external to the developer cannot be “original” within the meaning of Section 102(a)

40. *Herbert Rosenthal Jewelry Corp. v. Kalpakian*, 446 F.2d 738, 741 (9th Cir. 1971) (tests must consider “the preservation of the balance between competition and protection reflected in the patent and copyright laws.”).

41. 982 F.2d 693 (2d Cir. 1992).

42. *Id.* at 706.

43. *Id.* Interestingly, the *Computer Associates* court, like the *Whelan* court, reasoned by analogy from the field of literary works. The court’s test is actually a modified version of Judge Hand’s “abstraction test” performed upon copyrightable literary works. See *Nichols v. Universal Pictures Corp.*, 45 F.2d 119, 121 (2d Cir. 1930), *cert. denied*, 282 U.S. 902 (1931).

44. *Computer Associates*, 982 F.2d at 706.

45. The *Computer Associates* court adopted a filtering test very similar to that proposed by Professor Melville Nimmer. Nimmer’s approach requires the court to filter out those elements of a program that are: (1) abstract ideas; (2) dictated by logic and efficiency; (3) dictated by external considerations (such as hardware standards, software standards, computer specifications and programming industry standards); and (4) elements taken from the public domain. 3 MELVILLE B. NIMMER & DAVID NIMMER, *NIMMER ON COPYRIGHT* § 13.03[F] (1992).

46. *Computer Associates*, 982 F.2d at 707-10.

of the Copyright Act.⁴⁷ Therefore, where software interfaces are at issue, all those facets of the program that are "necessary" for compatibility with the systems to which they interface are rendered unprotectable. The consequences for communication software are discussed below.

The *Computer Associates* test is gaining wide acceptance.⁴⁸ It is not difficult to see why. The test seeks to balance all interests involved in accordance with the principles of the "merger doctrine." Significantly, the "filtration" step, as it should, considers the alternatives remaining to subsequent software developers and competitors undertaking similar tasks.⁴⁹ However, whether some structural element of a program is "necessary" to compatibility or efficiency is a highly technical question. One may well wonder whether the courts are qualified to undertake such analysis. Significantly, the quality of the court's analysis under the *Computer Associates* test will drastically affect the scope of copyright protection in most computer software.

3. *The Copyright Status of Communication Software*

LADIX's communications software, as a creative and original work, will undoubtedly qualify for copyright protection. However, the application of the copyright principles discussed above to this unique form of software leaves doubt that LADIX's copyright will provide much of an economic benefit. Accordingly, the analysis below focuses on: (a) the copyright status of LADIX's protocol and security system functions; and (b) whether a "right to achieve interoperability" will render much of LADIX's software unprotectable.

a. *The Copyright Status of Communication Protocols*

As discussed above, protocols are the rules and conventions that the software uses to communicate with other devices.⁵⁰ While a particular software implementation of a communication protocol is protected by copyright, does copyright also protect the protocol itself? Here, we are asking whether these protocols, or rules, form part of the program's copyrightable structure, sequence or operation. And if not, whether the pro-

47. In "paraphrasing" the *scènes a faire* doctrine, the court notes that "in many instances it is virtually impossible to write a program . . . without employing standard techniques." *Id.* at 709 (quoting *NIMMER supra* note 45 at § 13.03[F](3)). As the Tenth Circuit Court recently explained, "[u]noriginal elements of a program may be found at any level of abstraction." *Gates Rubber Co.*, 9 F.3d at 838.

48. The Tenth Circuit Court recently adopted the *Computer Associates* test in *Gates Rubber Co.*, 9 F.3d at 834. See also *Engineering Dynamics, Inc. v. Structural Software, Inc.*, 26 F.3d 1335, 1342 (5th Cir. 1994) (endorsing the *Gates Rubber/Computer Associates* abstraction-filtration-comparison test).

49. See *NIMMER, THE LAW OF COMPUTER TECHNOLOGY, supra* note 25 at ¶ 1.03[3][c].

50. See *supra* note 15 and accompanying text.

ocols can be independently copyrightable apart from their software implementation.

In *Secure Services Technology, Inc. v. Time and Space Processing, Inc.*,⁵¹ the court suggested that the plaintiff's facsimile "handshake protocol" could qualify for copyright protection independent of its software implementation if it satisfies the *de minimis* originality requirements of the copyright laws.⁵² In that case, the court ruled that SST's variations on the public domain T.30 protocol were too minor to be an "original work of authorship."⁵³ As a result, the court did not reach certain perplexing questions. For example, what form do SST's protocol variations take and are the protocols "fixed in a tangible medium of expression"⁵⁴ as required by the Copyright Act?

Some of these questions were taken up by the Federal Circuit Court in *Atari Games Corp. v. Nintendo Co.*⁵⁵ In *Atari*, the court reasoned that an original selection and arrangement of data in a signal that unlocks the Nintendo game console could qualify for copyright protection.⁵⁶ Thus, an original combination of data "fixed" in computer memory prior to transmission through a network communication medium might itself be copyrightable. Such a copyright would protect the individual signals, but perhaps not the rules under which those signals were generated. By this reasoning, the protocol is copyright protected, if at all, only through the copyright protection afforded the software that generates the signals.

This dichotomy between what a program "is" and what a program "does" has become an important issue in the compatibility wars being fought in the federal courts. In the appeal of the *Lotus v. Borland* case discussed in the Introduction, counsel for the defense and a host of amicus curiae have argued that Lotus' user interface, including the menu structures at issue in the case, must meet the aesthetic qualifications as

51. 722 F. Supp. 1354 (E.D. Va. 1989).

52. *Id.* at 1362-64.

53. *Id.* at 1363. The court also indicated that the timing characteristics of SST's protocol were uncopyrightable because these are a process, or method of operation which is excluded from copyrightable subject matter under § 102(b) of the Copyright Act. *Id.* at 1363 n. 25.

54. See 17 U.S.C. § 102(a). The 1976 Copyright Act states that a work is "fixed" if it is "otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101.

55. 975 F.2d 832 (Fed. Cir. 1992).

56. *Id.* at 840. However, the *Atari* court did not consider the copyrightability of the signals themselves but rather only the copyrightability of software that generates these signals. See also *Bellsouth Advertising & Pub. v. Donnelly Info. Pub.*, 933 F.2d 952, 957 (11th Cir. 1991) (original selection, coordination, or arrangement of information is copyrightable).

an "audiovisual work" if it is to qualify for copyright protection at all.⁵⁷ The defense's strategy seems to be divide and conquer. If the copyright in the menu structure of Lotus 1-2-3 is divorced from the Lotus program, different copyrightability and infringement rules would apply.

The "is/does" distinction has more than tactical significance in the case of LADIX's copyrights. If protocol copyright protection must exist apart from the copyright protecting the program, in what sense is the protocol expressed? As noted above,⁵⁸ the signals flowing over a communication line, even if copyrightable, in no way embody the protocol that governs their generation. In addition, even if the protocol is expressed in a technical manual or other publication, the copyright in the manual would not extend to the protocol. In *Morrissey v. Proctor & Gamble Co.*⁵⁹, for example, the court held that contest rules "merge" with the underlying idea and hence are not copyrightable.⁶⁰ Written protocols, being the rules governing data transmission, should receive similar treatment.⁶¹

If, on the other hand, the protocol can be considered part of the underlying program's "structure," the arguments for copyright protection face a different challenge. A communication protocol's function in achieving interoperability with other systems jeopardizes its copyright status.

b. Avoiding the "Interoperability" Argument

Compatibility is not an affirmative defense to copyright infringe-

57. See, e.g., *Brief Amicus Curiae of Professor Dennis S. Karjala and Professor Peter S. Menell, Lotus Development Corp. v. Borland International, Inc.*, No. 93-2214, at 4-6, reprinted in *COMPUTER INDUSTRY LITIG. REP.*, Jan. 20, 1994, at 18075.

While the defendant's argument has some intuitive appeal, the great weight of authority is against it. Most courts have treated the copyrights in user interfaces as part of the copyright in the program itself. See, e.g., *Johnson Controls, Inc. v. Phoenix Control Sys., Inc.*, 886 F.2d 1173, 1175 (9th Cir. 1989); *Manufacturers Technologies, Inc. v. Cams, Inc.*, 706 F. Supp. 984, 994 (D. Conn. 1989); *Digital Communications Assocs., Inc. v. Softklone Distrib. Corp.*, 659 F. Supp. 449, 455-56 (N.D. Ga. 1987); *Broderbund Software, Inc. v. Unison World, Inc.*, 648 F. Supp. 1127, 1133 (N.D. Cal. 1986). See also Anthony L. Clapes, Patrick Lynch & Mark R. Steinberg, *Silicon Epics and Binary Bards: Determining the Proper Scope of Copyright Protection for Computer Programs*, 34 U.C.L.A. L. Rev. 1493, 1560-68 (1987).

58. See *supra* note 56 and accompanying text.

59. 379 F.2d 675 (1st Cir. 1967).

60. *Id.* at 678.

61. Of course, because the communication protocol is an intrinsic feature of the underlying program's structure, it could benefit incidentally from the computer program's copyright. However, this is not a copyright in the protocol itself, unless that structure were the only possible structure for implementing the protocol. The possibility of program structure merging with the protocol it implements is discussed in the next section.

ment.⁶² For example, in *Apple Computer v. Franklin Computer*⁶³ the court expressly rejected the defendant's argument that software compatibility with the Apple II computer limited the copyright protection of the Apple BIOS program.⁶⁴ The court remarked that achieving total compatibility is a "commercial and competitive objective which does not enter into the somewhat metaphysical issue of whether particular ideas and expressions have merged."⁶⁵ Instead, according to the court, merger occurs when no other programs could be written which perform the same function as Apple BIOS.⁶⁶

Although there may be no general right to compatibility, the practical limit on the scope of copyright protection still depends upon how uncopyrightable "ideas" are defined.⁶⁷ The *Computer Associates* test, described above, equates certain external factors, including factors governing compatibility, with uncopyrightable ideas.⁶⁸ Whether this creates a compatibility defense depends upon the nature of the work.⁶⁹

Communication protocol design, and the design of software to implement them, are frequently influenced by external technical factors. Thus, communication protocols and data formats, as copyrightable elements, are unlikely to survive the "filtration" step of the *Computer Associates*' infringement test. First, the communication protocol embodied in

62. See, e.g., *Lotus Development*, 799 F. Supp. 203; *Consul Tec, Inc. v. Interface Systems, Inc.*, 22 U.S.P.Q.2d 1538, 1541 (E.D. Mich. 1991).

63. 714 F.2d 1240, 1245 (3d Cir. 1983), cert. dismissed, 464 U.S. 1033 (1984).

64. *Id.* at 1245. Apple BIOS like IBM-PC BIOS is an input-output system program that allows applications software transparent access to peripheral devices. The Apple Bios program is part of the Apple II operating system.

65. *Id.* at 1253.

66. *Id.*

67. See also Clapes, Lynch & Steinberg, *supra* note 57 at 1565.

68. See *supra* note 44 and accompanying text.

69. There are some who argue that the filtration test of *Computer Associates* should be applied to the defendant's rather than the plaintiff's work. In other words, if the elements copied by the defendant from the plaintiff's work were necessary for compatibility with the plaintiff's work, then those elements should merge and hence become uncopyrightable. See Note, Timothy S. Teter, *Merger and the Machines: An Analysis of the Pro-Compatibility Trend in Computer Software Copyright Cases*, STAN. L. REV. 1061, 1075-76 (1993).

This argument loses sight of the purpose of merger analysis. In the infringement context, merger is applied to determine whether the elements of the plaintiff's work that were copied by the defendant meet the requirements of copyrightability. Thus, the plaintiff's expression is not copyrightable where it is so influenced by external factors that the expression is not original to him, or that granting copyright protection would limit a subsequent author access to those external factors. Under the contrary view, elements are rendered uncopyrightable regardless of their originality or their relationship to external factors, but simply because they are needed to be compatible with the plaintiff's work itself. By this reasoning, the characters of Scarlet O'Hara and Rhett Butler would not enjoy protection because these characters would be necessary for a second-comer to write a sequel to "Gone With The Wind."

software is merely a functional element that might be considered to be dictated by efficiency concerns.⁷⁰ Second, the protocol and software design may be dictated by computer manufacturer's design standards or other external factors. Finally, the protocol is undoubtedly necessary for "compatibility with other programs with which a program is designed to operate."⁷¹ The last of these hurdles proves to be the most difficult to clear.

In addition, the *Computer Associates* analysis tends to undermine LADIX's efforts to provide system security through software. As discussed above, LADIX's new system includes security software that will permit devices to access the network only if they issue a predefined coded access message. Usually, the coded sequence of bytes is incorporated directly in the security software source code.⁷² Thus, if this section of the software is itself copyrightable, copying it in order to create a compatible device would constitute infringement.⁷³ Moreover, if the sequence of operations and data is sufficiently complex and there are many ways of generating the security signal, the program's copyright could survive a *Franklin*-style merger analysis.⁷⁴ However, because the design of the software and data sequence was "dictated by" factors that govern access to, and therefore compatibility with, a system, under the *Computer Associates* test, these elements could be readily copied by a competitor.⁷⁵

However, the schism between functionality and compatibility suggests a technical, albeit devious, solution to LADIX's legal problems. Consider the example provided by the case of *Atari Games Corp. v.*

70. See the discussion of external factors in *Computer Assoc.*, 982 F.2d at 709-710.

71. *Id.*

72. Such a technique is used by Nintendo corp in its video game cartridge authorization system. In the Nintendo system, patented microprocessors contain a copyrighted program (the "10NES software"). The "lock" and "key" microprocessors each contain copies of the 10NES software. The lock will fail to operate unless the key performs the same operations at the same time as the lock. See *Atari Games Corp. v. Nintendo of Am.*, 975 F.2d 832 (Fed. Cir. 1992).

73. See *SAS Institute, Inc. v. S & H Computer Sys.*, 605 F. Supp. 816, 832 (M.D. Tenn. 1985).

74. See *supra* notes 63-66 and accompanying text.

75. Another example is provided by *E.F. Johnson Co. v. Uniden Corp. of Am.*, 623 F. Supp. 1485 (D.C. Minn. 1985). In this case, Uniden wrote a software program designed to achieve compatibility with E.F. Johnson's computerized mobile radio system. E.F. Johnson's software contained an "H-matrix", which was necessary to establish communications with the base station. The court reasoned that because there were 32 different configurations of the H-matrix that would ensure compatibility with the EFJ base station, Uniden could not excuse its verbatim copying of the EFJ H-matrix. *Id.* at 1495. It is not entirely certain that the result would be different under the *Computer Associates* merger analysis. However, because the H-matrix was "dictated by" the compatibility requirements of the base station, it is reasonable to assume that it would be rendered uncopyrightable.

*Nintendo of Am., Inc.*⁷⁶ The Nintendo game cartridge security system software⁷⁷ contains several unnecessary instructions and data that are reserved for "future use." Because these instructions currently perform no function, under the *Franklin* analysis they will not merge, and thus are copyrightable expression.⁷⁸ However, by altering the security protocol in future versions, the author could deny access to cartridges whose software does not contain these instructions. The court rejected Atari's argument that these unnecessary instructions were uncopyrightable because they could become functional in future versions.⁷⁹ According to the court, "[t]hings that are admittedly non-functional at the time of copying are not made functional by the infringer's efforts to preempt reactions to its infringement."⁸⁰ Additionally, because these instructions are not influenced by current compatibility concerns, they will not be "filtered out" under the infringement test of *Computer Associates*.

In summary, LADIX's copyright protection in its communication protocol is threatened in the event of a wide acceptance of the *Computer Associates* rationale. Worse for LADIX, given the influence and number of those arguing in favor of the rationale, there is reason to suspect that the courts will go even further and create a general compatibility/interoperability defense to copyright infringement.⁸¹ Moreover, commercial necessity may force future trends in this direction. The demand for communication protocol standardization becomes more important as computing resources become more accessible.⁸² Ironically, the successful software developer may soon find his legal protection undermined by the very popularity of his product.

4. *Compatibility and the Legal Status of Reverse Engineering*

Communications software is especially vulnerable to discovery

76. 18 U.S.P.Q.2d (BNA) 1935 (N.D. Cal. 1991).

77. This refers to the 10NES software discussed *supra*, note 72. See *supra* note 72.

78. See Peter A. Wald, Michael K. Plimack & Matthew J. Viola, *Standards for Interoperability and the Copyright Protection of Computer Programs*, 339 PRAC. L. INST. 701 (1992).

79. *Atari Games*, 18 U.S.P.Q.2d at 1939.

80. *Id.* On appeal, the Federal Circuit Court of Appeals affirmed the lower court's analysis of this point. *Atari Games Corp. v. Nintendo of Am.*, 975 F.2d 832, 845 (Fed. Cir. 1992).

81. See, e.g., Wald, Plimack & Viola, *supra* note 78; Teter, *supra* note 69; Peter S. Menell, An Analysis of the Scope of Copyright Protection For Application Programs, 41 STAN. L. REV. 1045, 1074 (1989); See also *supra* notes 2-7 and accompanying text.

82. The IBM PC phenomenon is a perfect example of this. The IBM PC architecture (including MS-DOS and BIOS) has become a *de facto* standard despite the technical limitations inherent in these products. See *supra* notes 17-20 and accompanying text.

through reverse engineering.⁸³ Reverse engineering of communication protocols could be conducted in either of two ways: (1) uncovering the communication protocol by attaching a protocol analyzer or line monitor to the communication lines;⁸⁴ or (2) by decompiling the object code of the communication program.⁸⁵ The legality of such practices has been the topic of significant recent judicial activity.

Discovery of LADIX's communication protocol through communication line analysis would not violate LADIX's copyrights. As discussed above,⁸⁶ under either a Computer Associates or a Franklin merger analysis, the communication protocol is likely to be held an uncopyrightable aspect of the communication software. Thus, a reverse engineer makes no unauthorized copy of any copyrightable elements by displaying the contents of a communication line.⁸⁷ However, as discussed above, portions of the protocol directly embedded in the software may independently qualify for copyright protection. This would occur, for example, if there were many ways of coding the embedded section.⁸⁸

A much more interesting and hotly-debated topic is the legality of decompilation.⁸⁹ In a strict sense, the legality of decompilation should be non-controversial. Section 106(1) of the copyright act gives the author the exclusive right to reproduce the copyrighted work.⁹⁰ During reverse engineering, several intermediate copies of the copyrighted program are made. Because these copies are made without the authorization of the copyright owner, this should constitute infringement. Indeed, a federal district court so held in *Sega Enterprises Ltd. v. Accolade, Inc.*⁹¹ In *Sega*,

83. The United States Supreme Court has defined "reverse engineering" as "starting with the known product and working backward to divine the process which aided in its development or manufacture." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974).

84. These devices decode signals and contain displays which help the reverse engineer analyze the signal contents and timing characteristics.

85. Decompilation involves translating machine-readable object code into human-readable source code form, which generally is not included with the software when purchased or licensed.

86. See *supra* note 44 and notes 63-66 and accompanying text.

87. But see *Secure Services Technology, Inc. v. Time and Space Processing, Inc.*, 722 F. Supp. 1354, 1364 (E.D. Va. 1989) (suggesting that protocols may be copyrightable along with software if sufficiently original). See also *supra* notes 51-54 and accompanying text.

88. See, e.g., *E.F. Johnson Co.*, 623 F. Supp. at 1502-03. See *supra* note 75.

89. Julie Aguilar, Note, *Sega Enterprises, Ltd v. Accolade, Inc.: Setting the Standard on Software Copying in the Computer Software Industry*, 23 GOLDEN GATE U.L. REV. 269 (1993); Darren J. Carroll, *When More is Less: Controlling the Market for Computer Software Enhancements*, 43 SYRACUSE L. REV. 1321 (1992); Martin Glenn & Dale M. Cendali, *Software Security: Sega Case Suggests Protection Strategies*, THE NAT'L L.J., Jan. 18, 1993, at S2; William S. Coats & Heather D. Rafter, *Accolade and Atari: Reverse Engineering and the Right to Make Compatible Programs*, THE COMPUTER LAW., Oct. 1992, at 1.

90. 17 U.S.C. § 106(1) (1990).

91. 785 F. Supp. 1392 (N.D. Cal. 1992), *rev'd*, 977 F.2d 1510 (9th Cir. 1993).

the court ruled that Accolade infringed Sega's copyrights by making intermediate copies during decompilation of Sega's software in an attempt to break its security code.⁹² Significantly, the court enjoined Accolade's final product even though that product failed to contain a substantial amount of Sega's protected expression.⁹³

The Ninth Circuit Court of Appeals reversed the district court's decision.⁹⁴ The court held that decompilation of software to discover its ideas or functions is a "fair use"⁹⁵ when this is the only practical method of access.⁹⁶ In its fair use analysis, the court remarked that decompilation in an effort to achieve compatibility results in a public benefit and thus is particularly likely to be a fair use.⁹⁷ Additionally, the court pointed out that the need to disassemble is presumed where the software's operation is not visible to the user — as is the case with all system interface programs.⁹⁸

In the wake of the *Sega* decision, LADIX's communication program is particularly vulnerable to the perils of reverse engineering through decompilation. LADIX's software is both a system program that is invisible to the user and a program that is necessary to achieve compatibility. However, *Sega* allows only the discovery of the ideas behind a program through decompilation and not the appropriation of its copyrightable expression.⁹⁹ Therefore, the secret to locking out the competition lies, again, in the copyright status of the protocols themselves. And, as noted above, this gives LADIX but a slender reed of hope. Perhaps even worse for LADIX, the *Sega* decision signals further judicial acceptance of the idea of compatibility as a competitive right. The trend is likely to continue in this direction.

B. TRADE SECRET PROTECTION

Trade secret protection can provide a useful supplement to copyright and patent protection. Unlike copyright and patent law, the subject matter that qualifies for trade secret protection is not rigidly prescribed.

92. *Id.* at 1396.

93. *Id.*

94. *Sega Enter. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1993).

95. See 17 U.S.C. § 107 (1988). Fair use is an equitable doctrine that excuses, under some circumstances, what would otherwise be infringing copying. Section 107 lists four factors that are relevant in determining whether use of a copyrighted work is fair: (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used; and (4) the effect of the use upon the potential market for the copyrighted work.

96. *Sega Enter.*, 977 F.2d at 1513-14.

97. *Id.* at 1523. Almost simultaneously, the Federal Circuit Court reached an identical conclusion in *Atari Games*, as discussed above. *Atari Games Corp.*, 875 F.2d at 943.

98. *Sega Enter.*, 977 F.2d at 1525.

99. *Id.* at 1528.

Processes, techniques, data and ideas, which are uncopyrightable and which do not satisfy the patent law's rigorous novelty and nonobviousness criteria, may nevertheless be protectable trade secrets.¹⁰⁰ On the other hand, trade secret law does not confer any exclusive rights upon the trade secret owner. Rather, trade secret laws protect only the veil of secrecy that the owner has erected to surround his discovery.¹⁰¹ Thus, the roots of trade secret law lie in enforcing standards of commercial ethics rather than in providing a system of incentives for art and innovation.

According to the Restatement of Torts, a trade secret is defined as: "[a]ny formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."¹⁰² Despite this rather clear pronouncement, the concept of a "trade secret" is flexible and invites the consideration of a number of factors.¹⁰³ Significantly, however, all trade secret laws require the owner to undertake active measures to maintain secrecy.¹⁰⁴

LADIX's communication protocols and security methods themselves, like formulas and patterns, can be protectable trade secrets provided that they are not generally known to others and provided that LADIX undertake sufficient security measures.¹⁰⁵ However, the unique nature of LADIX's trade secrets raises two issues. First, whether the trade secrets can be lawfully discovered through reverse engineering; and second, whether trade secret protection can be limited by claims that use of trade secrets is required to achieve interoperability.¹⁰⁶ Below, the dis-

100. See NIMMER, *THE LAW OF COMPUTER TECHNOLOGY*, *supra* note 25 at ¶ 3.02.

101. *Id.*

102. RESTATEMENT (SECOND) OF TORTS § 757 cmt. b (1974). Unlike copyright protection which is governed by federal laws, trade secret protection is governed by state laws. There is, however, considerable uniformity in state trade secret laws. More than 30 states have adopted the Uniform Trade Secrets Act. See Uniform Trade Secrets Act, 14 U.L.A. 537 (Supp. 1989).

103. See *Gates Rubber Co. v. Bando Chemical Industries*, 9 F.3d 823, 848 (10th Cir. 1993)(under Colorado law, factors include: extent of knowledge outside business; extent known inside business; precautions taken to guard secrecy; savings effected in protecting the information; amount of effort expended; amount of time and expense required to duplicate).

104. See Uniform Trade Secrets Act, 14 U.L.A. 369 (Supp. 1989).

105. See *Secure Services Technology, Inc. v. Time and Space Processing, Inc.*, 722 F. Supp. 1354, 1360 (E.D. Va. 1989); *Telerate Systems, Inc. v. Caro*, 689 F. Supp. 221, 232 (S.D.N.Y. 1988) (plaintiff's communication protocol "would appear to be the type of 'process or device' typically considered a trade secret").

106. A trade secret claim may also be vulnerable to preemption under the Copyright Act. See 17 U.S.C. § 301 (1988). Preemption is mandated where a trade secret claim asserts rights equivalent to those delineated in § 106 of the Copyright Act. *Gates Rubber*, 9 F.3d at 847. However, there is no preemption where the claim asserts an additional ele-

cussion examines whether these are real or only perceived dangers.

1. *Permissible Reverse Engineering of Trade Secrets*

Trade secret laws protect owners of valuable trade secrets against "misappropriation." A prototype example of trade secret misappropriation is where a former employee violates a confidentiality agreement by disclosing trade secrets to a competitor of the former employer.¹⁰⁷ However, misappropriation can also occur where one uses some "improper means" to discover the owners secrets.¹⁰⁸ Could LADIX proceed against a reverse engineer under the trade secret laws? The answer may well depend on the LADIX's sales or licensing policies.

In *Kewanee Oil Co. v. Bicron Corp.*,¹⁰⁹ the Supreme Court stated that trade secret laws do not prevent discovery by proper means including "so-called reverse engineering."¹¹⁰

In *Secure Services Technology v. Time and Space Processing*,¹¹¹ the plaintiff alleged that the defendant misappropriated trade secrets when it reverse engineered the plaintiff's facsimile protocol by analyzing a machine loaned to them by the plaintiff's customer.¹¹² The court held that the defendant's methods were a proper means of discovery because the machine was not acquired by improper means.¹¹³ Additionally, the court held that the plaintiff waived its trade secret protection by failing to take adequate steps to maintain the secrecy of its protocol. According to the court, "by selling its machine without reserving proprietary rights, SST effectively disclosed its protocol variations."¹¹⁴

The terms of the license or sales agreement can limit the extent of a competitor's proper means of discovery. For example, in *Telerate Systems, Inc. v. Caro*,¹¹⁵ Telerate sustained its trade secret claim against a defendant who discovered its communication protocol by attaching a protocol analyzer to equipment obtained from a Telerate licensee.¹¹⁶ In this case, the defendant's actions were an improper means of discovery because the Telerate licensing agreement specifically prohibited attaching

ment beyond that needed to prove copyright infringement. *Id.* A trade secret claim is liable to assert such an additional element namely, a breach of confidence. Thus, LADIX's potential trade secret claims should survive a preemption challenge.

107. *See, e.g.,* *Head Ski Co. v. Kam Ski Co.*, 158 F. Supp. 919 (D. Md. 1958).

108. *E.I. duPont de Nemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970), *cert. denied*, 400 U.S. 1024 (1971) (discovery by aerial photography is misappropriation).

109. 416 U.S. 470 (1974).

110. *Id.* at 476.

111. 722 F. Supp. 1354 (E.D. Va. 1989).

112. *Id.* at 1359.

113. *Id.* at 1360.

114. *Id.* at 1361.

115. 689 F. Supp. 221 (S.D.N.Y. 1988).

116. *Id.* at 233.

an analyzer without Telerate's consent.¹¹⁷ According to the court, "the term 'reverse engineering' is not a talisman that may immunize theft of trade secrets."¹¹⁸

Thus, LADIX's best hope of maintaining the secrecy of its proprietary interface lies in its ability to control access to the interface design. Accordingly, LADIX's license and sales agreements must insist on the confidentiality of any trade secret disclosed in the transaction. Moreover, to the extent possible, LADIX sales agreements should forbid unauthorized access to data interface ports.¹¹⁹ This may preclude any claim that reverse engineering the protocol or security features is a lawful means of discovery.

2. *Trade Secrets Necessary to Achieve Interoperability*

As discussed above, copyright protection of communications software is often circumscribed due to its vital role in permitting interoperability with other systems.¹²⁰ One suspects that trade secret protection of communication protocols could face the same scrutiny. However, to date no court has limited the scope of a trade secret because of its necessity in achieving interoperability.¹²¹ The reason lies in the very different footing in which trade secret law stands. As noted above, trade secret law does not grant the owner a monopoly as a means of encouraging innovation. Rather, trade secret laws protect the owner of commercially-valuable secrets against unlawful or "improper" disclosure and discovery. Within these narrow limits, the trade secret owner's rights are absolute.¹²²

In sum, trade secret protection serves a complimentary function for creators of communication software. Copyright laws protect the source code and structure of the program but do not protect the communication protocol itself. Trade secret laws protect the interface specifications and communications protocols provided the owners (LADIX in our case) take

117. *Id.*

118. *Id.*

119. Note that the ability to control access to data ports becomes impractical for widely distributed systems that are based on standard platforms. This, in effect, places an inherent limit on the ability of trade secret owners to prevent the development of interoperable systems.

120. See *supra* Part II, Section A.3 of this Article.

121. Several commentators have noted this discrepancy. These commentators suggests that the courts should recognize a general "right to be compatible." See David Bender, *Protection of Computer Programs: The Copyright/Trade Secret Interface*, 47 U. PITT. L. REV. 907, 923 (1986); Duncan M. Davidson, *The Future of Software Protection: Common Law, Uncommon Software*, 47 U. PITT. L. REV. 1037, 1099 (1986).

122. However, federal antitrust laws do limit the ability of trade secret owners to extend their power in the marketplace. The antitrust impact on the marketing policies of communication software vendors is considered in Part III below.

adequate steps to protect their secrets. Thus, if LADIX is vigilant in maintaining the secrecy of its protocols and in scrutinizing its licensing and sales agreements, trade secret protection fills the large void between copyright protection and adequate protection.

IV. THE ANTITRUST IMPLICATIONS OF COMMUNICATION SOFTWARE

At first glance, antitrust laws would seem wholly at odds with intellectual property laws: the former protect consumers against impediments to free competition while the latter grant authors and inventors monopoly rights. However, as the Federal Circuit Court has pointed out, the two bodies of law are complimentary in that they both "are aimed at encouraging innovation, industry and competition."¹²³ In order to maintain a proper balance between innovation and competition, antitrust laws guard against improper extensions of market power by owners of intellectual property rights.¹²⁴ Typically, antitrust claims against intellectual property rightholders come in two forms: (A) claims that the rightholder engaged in illegal tying arrangements; and (B) claims that the rightholder maintains an illegal monopoly. In each case, the rightholder's market power is the dominant consideration. And, as we shall see, a rightholder's power to control interoperability may create sufficient market power to raise antitrust concerns.¹²⁵

A. ILLEGAL TYING ARRANGEMENTS

Under § 1 of the Sherman Act, an illegal tying arrangement occurs when a rightholder uses its dominance in the market for a "tying product" to coerce buyers into accepting a "tied product" resulting in an anticompetitive effect in the market for the tied product.¹²⁶ Illegal tying arrangements have been found where a rightholder's market power

123. *Atari Games Corp. v. Nintendo of Am.*, 897 F.2d 1572, 1576 (Fed. Cir. 1990).

124. *Id.*

125. Recently, the moribund Antitrust Division of the Justice Department has shown signs of life. Assistant Attorney General Anne K. Bingaman has indicated that, in her opinion, overly broad intellectual property protection and vigorous enforcement of intellectual property rights can threaten free competition. See *Trustbusters Go Gunning For High Tech*, BUS. WEEK, March 7, 1994, at 64. Ominously (for LADIX), she has singled out the *Lotus v. Borland* case as an example of this phenomenon. *Id.*

126. 15 U.S.C. §§ 1, 3 (1988). See also § 3 of the Clayton Act. 15 U.S.C. § 14 (1988). The Supreme Court has stated that:

[T]he essential characteristic of an invalid tying arrangement lies in the seller's exploitation of its control over the tying product to force the buyer into the purchase of a tied product that the buyer either did not want at all, or might have preferred to purchase elsewhere on different terms.

Jefferson Parish Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 12 (1983). The tying relationship must also result in a "not insubstantial" effect on interstate commerce. *Id.* However, this

stems from its holding the keys to compatibility. For example in *Digidyne v. Data General Corp.*,¹²⁷ the court found an illegal tying arrangement in Data General's practice of refusing to license its RDOS operating system to all except purchasers of its NOVA hardware.¹²⁸ In effect, DG's market dominance in RDOS created by its copyright and trade secret protection gave them coercive power over DG customers who were locked into RDOS because of previous investments in applications software.¹²⁹ The court held that DG's practices forced its customers to buy NOVA hardware resulting in an illegal restriction on competition in the computer hardware market.¹³⁰

The successful antitrust plaintiff must prove more than a market power in an interoperable product. Illegal tying occurs only if there is a separate market demand in the tying and the tied products. In *Telerate Systems*, the defendant alleged that the plaintiff's sale of database access coupled with its sale of display terminals amounted to an illegal tying arrangement.¹³¹ The court reasoned that the character of the demand for the two products, rather than the function of the two products, determines whether an illegal tying arrangement exists.¹³² According to the court, no illegal tying arrangement existed because the demand for Telerate's database could not be distinguished from the demand for its protocol-compatible display terminals.¹³³

Additionally, a tying claim requires proof that the accused undertook coercive marketing policies. That is, the defendant must *condition* the availability of one product (usually the tying product) on the purchase of another product (usually the tied product).¹³⁴ In *Telerate Systems*, the court noted that, unlike the defendant in *Digidyne*, Telerate did not condition access of its database (the tying product) upon the purchase of protocol-compatible terminals (the tied product).¹³⁵ Instead,

requirement is of a *de minimis* nature. See *United States v. Loew's, Inc.*, 371 U.S. 38, 49 (1962).

127. 734 F.2d 1336 (9th Cir. 1984), *cert. denied*, 473 U.S. 908 (1985).

128. *Id.* at 1338.

129. *Id.* at 1344.

130. Commentators have harshly criticized the reasoning of the *Data General* court. They have argued that a copyright cannot achieve sufficient market power because a copyright grants a monopoly in expression, not functionality. Thus, others may develop RDOS-compatible operating systems without violating DG's rights. See Reback, *Further Reflections on Data General and the Law of Pricing Unbundled Products*, THE COMPUTER LAW. Nov. 1984, at 4. However, as the discussion above points out, the combination of trade secret and copyright law may make it very difficult for a competitor to develop compatible products legally.

131. *Telerate Systems*, 689 F. Supp. at 234.

132. *Telerate Systems*, 689 F. Supp. at 234.

133. *Id.* at 236.

134. *Northern Pacific Ry. v. United States*, 356 U.S. 1, 6 n.4 (1958).

135. *Telerate Systems*, 689 F. Supp. at 236.

Telerate customers could choose among several methods of access.¹³⁶

The cases point out that a rightholder in interoperable products, such as communications software, must be wary of violating the anti-trust laws. Because of LADIX's copyright and trade secret protection of its communications software, LADIX can attain a dominant position in the market for access to real-time data from LADIX machines. Thus, by bundling the sale of its manufacturing equipment with the sale of communication software to enable data access, LADIX invites antitrust scrutiny. But the demand for LADIX machine data cannot be separated from the demand for the machines themselves. Moreover, LADIX does not condition use of its proprietary network on the purchase of specific computing hardware — many kinds of computers can be attached to the LADIX network.

On the other hand, LADIX's sale of applications software may raise some antitrust concerns. Applications software may be treated as a distinct product if consumers might wish to purchase it separately from the LADIX's real-time data access.¹³⁷ This would occur only if the software had value as a general display package apart from its value as an integrated part of the LADIX system. If so, LADIX may not condition the sale of its real-time access software on the purchase of LADIX application software and *visa versa*.

B. ILLEGAL MONOPOLIES

One also violates the Sherman Act by monopolizing or attempting to monopolize a market in U.S. commerce.¹³⁸ This provision has special relevance for those who have been granted legal monopolies under copyright, trade secret or patent laws. In the words of the Federal Circuit Court, intellectual property rights cannot be used as a "sword to eviscerate competition unfairly."¹³⁹ For example, certain clauses found in licensing agreements may result in a violation of the antitrust laws.¹⁴⁰ However, antitrust problems arise only where there is no active competition for the product or where the licensor or seller possesses a large section of the relevant market.¹⁴¹

136. *Id.* at 236.

137. *Jefferson Parish*, 466 U.S. at 39 ("for products to be treated as distinct, the tied product must, at a minimum, be one that some consumers might wish to purchase separately without also purchasing the tying product").

138. 15 U.S.C. § 2 (1988).

139. *Atari Games Corp. v. Nintendo of Am.*, 897 F.2d 1572, 1576 (Fed. Cir. 1990).

140. *See Albrecht v. Herald Co.*, 390 U.S. 145 (1968) (agreements concerning resale prices are *per se* illegal); *Continental T.V., Inc. v. GTE Sylvania, Inc.*, 433 U.S. 36, 57 (1977) (non-price vertical restrictions to be judged under a "rule of reason").

141. *Atari Games Corp.*, 897 F.2d at 1576.

Vendors who wish to maintain closed systems or proprietary networks may face antitrust scrutiny if their actions disrupt the market for peripheral devices.¹⁴² This can arise, for example, where the system vendor changes product specifications or access protocols, thereby rendering third-party products incompatible.¹⁴³ However, the successful antitrust plaintiff must demonstrate the defendant's actions were predatory or evidence some other anticompetitive assault on the secondary market.¹⁴⁴ The courts are unlikely to risk chilling innovation by assuming malevolent intent on the part of an innovator.

Moreover, the successful antitrust plaintiff must demonstrate that the defendant's actions had an adverse affect in a defined "relevant market."¹⁴⁵ In the case of the integrated system, the plaintiff must succeed in defining the relevant market narrowly to include only the defendant's system and associated peripherals. The courts are also unlikely to embrace such a definition. Rather, the courts are more likely to define the relevant market broadly to include all of the defendant's competitors within the primary market.¹⁴⁶ Under the "reasonable interchangeability" test, if other products that perform the same functions are readily available, the "relevant market" is unlikely to be seriously affected by the defendant's actions.¹⁴⁷ Therefore, no antitrust violations arise where a proprietary network vendor limits access to a single data source if there are similar data sources on the market.¹⁴⁸

Strong copyright and trade secret protection of communication software raises antitrust concerns due to its power to control interoperability. We have seen, however, that the antitrust laws give the product innovator the benefit of the doubt. Thus, assuming LADIX has no monopoly on process equipment and acts without manifest intent to damage its competitors, LADIX should not run afoul of the antitrust laws through its efforts in developing a proprietary data interface.

142. See NIMMER, *THE LAW OF COMPUTER TECHNOLOGY*, *supra* note 25, at ¶ 4.11.

143. See, e.g., *Telex Corp. v. International Business Mach. Corp.*, 510 F.2d 894 (10th Cir. 1975).

144. See *Berkey Photo, Inc. v. Eastman Kodak Co.*, 603 F.2d 263 (2d Cir. 1979); *Telex Corp.*, 510 F.2d at 927.

145. *United States v. Grinnell Corp.*, 384 U.S. 563, 571 (1966).

146. NIMMER, *THE LAW OF COMPUTER TECHNOLOGY*, *supra* note 25, at ¶ 4.11[2].

147. See *United States v. E.I. DuPont de Nemours & Co.*, 351 U.S. 377, 380-81 (1956). A detailed analysis of the "reasonable interchangeability" test is beyond the scope of this article. In brief, the test also requires the claimant to prove "demand interchangeability" and "supply interchangeability." These are economic terms that measure the effect of price changes on demand and supply for the product.

148. See, e.g., *Telerate Systems, Inc.*, 689 F. Supp. at 239.

V. CONCLUSIONS

LADIX's communications software will be protected under copyright laws. However, recent copyright decisions indicate that competitors may have a right to use portions of a copyrighted program that are necessary to achieve interoperability with other systems. Moreover, recent U.S. developments in copyright law recognize a competitor's right to decompile software in an effort to discover the keys to compatibility. Because communications software serves the vital function of providing interoperability among disparate systems, its legal protection under modern copyright law may be significantly curtailed.

Trade secret protection for communications software supplements copyright protection in a number of ways. For example, unlike copyright laws, trade secret laws will protect LADIX's protocol specifications provided LADIX undertake steps to maintain their secrecy. Moreover, by using licensing policies that prohibit unauthorized access to data ports, LADIX can prevent the loss of its secrets through reverse engineering. However, LADIX must be wary of any licensing policies which may result in an illegal tying arrangement under U.S. antitrust laws.

To date, U.S. intellectual property law does not recognize a general right to achieve compatibility. There are, however, indications that the courts may soon recognize such a right. The necessity or desirability of such rights can certainly be debated. Significantly, IBM's rights in its BIOS program has not prevented competitors from lawfully discovering its secrets through reverse engineering. Indeed, the developers of widely distributed systems will probably find it in their best interests to permit access to their products. However, the recognition of a general right to interoperability may work to the extreme disadvantage of developers of small, closed systems like LADIX. The courts would be wise to heed the warnings of Judge Edelstein in *Telerate Systems*,¹⁴⁹ lest interoperability become a talisman that excuses piracy.

149. See *supra* note 118.

