Legal Protection of Software, Practical Law Practice Note 7-575-8965 (2016)

Legal Protection of Software

by Practical Law Intellectual Property & Technology
Maintained • USA

This Practice Note considers the legal protection available for software under US law. It focuses primarily on the law of copyright (including the Digital Millennium Copyright Act (DMCA)), patents and trade secrets, but also considers contractual protections and other common law and statutory rights.

Contents

Legal Protection of Software, Practical Law Practice Note 7-575-8965 (2016)

Proprietary **software** can be among a business's most valuable assets. Whether a company **licenses** software to others or uses software to provide services to customers or for its own internal operations, proprietary software can give the company a competitive edge that may be lost without legal protection.

The owner of rights in software may seek to protect these rights under any one or more of the following:

- **Intellectual property** (IP) laws, including the law of:
    - **copyrights**;
    - **patents**; and
    - **trade secrets**.
- Contractual provisions, such as confidentiality obligations and use restrictions.
- Non-IP statutes.
- Common law tort claims, such as trespass to chattels.

Each form of protection has unique advantages and drawbacks. Some forms are cumulative and others exclusive. Counsel must therefore select the form, or combination of forms, of protection best suited to the client's needs considering such factors as:

- The nature and function of the software product.
- The client's business model, including how and by whom its software will be used or distributed.
- The scope, strength and length of the contemplated form of IP protection.
- The preclusive effect of the chosen type of protection on other modes of protection.
- The levels of difficulty and expense involved in obtaining, maintaining or enforcing the contemplated form of protection.

This Note discusses each of the principal legal theories under which a party may protect its rights in software.

Definition of Software

The US **Copyright Act** defines a computer program as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result" (17 U.S.C. § 101). The program instructions can be fixed in any electronic, print or other medium and are typically set out in human-readable **source code** and machine-readable **object code** form.

However, software rights owners have a strong interest in obtaining protection for more than the computer program's literal code. For example, a program's non-literal elements, such as its user interface, can be more valuable than the literal code itself (see Software as Copyrightable Subject Matter).

"Software" is typically broader in scope than the more narrowly defined "computer program." It includes system software (such as operating system software, which supports basic computer functions), applications software (which carries out specific tasks) and such valuable related articles as the computer program's:

- Documentation, including:
    - user, system administrator and other manuals; and
    - specifications and instructions (including flow charts, block diagrams and texts) that describe or depict the software's architecture, configuration, functionality, testing, operation, interfaces or other features, components or requirements.
- Libraries (code and data that can be used both by a computer program and multiple other, unrelated programs).
- Frameworks (for example, support programs, compilers, code libraries, tool sets and application programming interfaces (APIs)) used to develop the program.

Method and Scope of Analysis

A useful tool for determining the rights that may be asserted in software is to:

- Separate the computer program into literal and non-literal elements (see Software as Copyrightable Subject Matter).
- Determine, on an element-by-element basis, which elements may be protected.
- Identify and evaluate any remaining software components to determine whether they qualify for any of the multiple forms of software protection.

The first two steps of this procedure are part of the abstraction-filtration-comparison test courts frequently apply to determine which elements of a computer program are copyrightable (see Software as Copyrightable Subject Matter). However, this test is also helpful in identifying software elements that may be eligible for other forms of IP protection. This Note therefore adopts an abstraction-filtration analysis to identify, in addition to copyright, the other protections that may apply to these various software elements.

Certain related works are distinguished from software and are beyond the scope of this Note. These include:

- **Computer-generated output** (CGO) (except as embodied by the computer program's code). CGO includes data and data sets, printed or other textual works, audiovisual works, music, sound effects, screen displays and the program's graphical user interface (visual elements, such as buttons, icons, pull-down menus, windows and scroll bars, that enable a user to interact with a computer). (See generally, *Computer Assocs. Int'l v. Altai, Inc.*, 982 F.2d 693, 703 (2d Cir. 1992)* ("These items represent products of computer programs, rather than the programs themselves")). The diverse forms of CGO may be protected under one or more of the following:
  - copyright (for literary, pictorial, musical and audiovisual works, including computer games and characters, derivative works and compilations) (see, for example, *Stem Elecs., Inc. v. Kaufman*, 669 F.2d 852, 855 (2d Cir. 1982)* (computer game sounds and displays may be copyright protected as separate audiovisual works even where there is no copying of the underlying code));
  - trade dress (for the total image and overall appearance of nonfunctional features of a graphical user interface, screen display or other distinctive design);
  - trademark (for screen-displayed or printed names, words, colors, designs, sounds, fictional characters and other distinctive source-identifying marks); or
  - design patents or registered designs (for novel, non-obvious, ornamental icons and screen displays or software-generated product designs) (35 U.S.C. § 171; see also Manual of Patent Examining Procedure (MPEP): ch. 1500 (9th ed. Mar. 2014)).
- **Automated databases** (facts, data, images, music, videos or other information assembled into an organized format that can be accessed by a retrieval program or system). For information on database protection, see Practice Note, Data as IP and Data License Agreements; Registration of Claims to Copyrights, Registration and Deposit of Databases, 54 Fed. Reg. 13,177-178 (Mar. 31, 1989); Compendium of U.S. Copyright Office Practices § 1117: Databases (3d ed. Dec. 22, 2014).

Copyrights

In the US, as in most jurisdictions, copyright law is a favored form of software IP protection.

Legal and Regulatory Authority for Copyrights

Copyrights are regulated in the US by the **US Copyright Office** under the authority of the federal Copyright Act. The

Copyright Office website provides legal and regulatory background information and procedural guidance relating to copyright protection. For more information on copyrights in general, see Practice Note, Copyright: Overview.

Software as Copyrightable Subject Matter

Copyrights attach to original works of authorship fixed in a tangible medium of expression. These include original:

- Literary, musical, pictorial, graphic, dramatic and audiovisual works (17 U.S.C. § 102(a)).
- Compilations of copyrightable or non-copyrightable works (for example, data) (17 U.S.C. § 103).
- Derivative works of or based on any of the foregoing (17 U.S.C. § 103).

Software source code and object code are copyrightable as literary works if they are original and fixed in a tangible medium of expression, such as in print or in a computer hard drive or other electronic, magnetic or optical medium (see *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510, 1520 (9th Cir. 1992*)* and 17 U.S.C. § 102(a)).

However, because computer code is both expressive and functional, deciding which computer program features are eligible for copyright protection is typically more difficult than determining more traditional copyrightable subject matter (*Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1354 (Fed. Cir. 2014)). This is because the Copyright Act expressly excludes from its protection ideas, processes, systems and methods of operation, even if they are described, illustrated or embodied in an otherwise copyrightable work (17 U.S.C. § 102(b)).

As a result, the courts must parse this difficult idea-versus-expression dichotomy to determine a program's protectable, expressive elements and whether a party has infringed any copyrights in these elements. When doing so, the courts take into account the program's literal and non-literal elements, each of which is eligible for copyright protection (see, for example, *Altai*, 982 F.2d at 701).

Literal Elements

A computer program's literal elements are its:

- Source code.
- Object code.

Non-literal Elements

A program's non-literal elements include the structure, sequence and organization of both:

- The program as an integrated whole.
- The program's individual features or components, such as its:
    - modules, subroutines and macros;
    - module substructure (the nesting of one module within another);
    - control flow (the sequence in which modules perform their tasks);
    - files;
    - data flow (the sequence in which data moves through the program and is operated on by the modules); or
    - user interface (data input formats and other non-graphical, internal code that enables the user and computer to communicate with one another, as distinguished from the visible graphical user interface).

(See, for example, *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 9 F.3d 823, 835 (10th Cir. 1993) and *Altai*, 982 F.2d at 702.)

Determining the Copyrightability of Individual Programs

To determine which computer program elements are copyrightable, the federal courts (which have exclusive jurisdiction over US copyright cases) commonly identify and analyze each of the program's literal and non-literal elements under one of three principal tests:

- Abstraction-filtration-comparison (see Abstraction-filtration-comparison).
- Method of operation (see Method of Operation).
- Inherent necessity (see Inherent Necessity).

Abstraction-filtration-comparison

Under this leading test, expressive features of the program's literal and non-literal elements are first examined at multiple levels of abstraction. These levels range from the program's most abstract to its most concrete expression and, as noted by at least one court, can often be parsed into at least six levels of generally declining abstraction: "(i) the main purpose, (ii) the program structure or architecture, (iii) modules, (iv) algorithms and data structures, (v) source code, and (vi) object code" (*Gates*, 9 F.3d at 835).

To identify the remaining core of protectable expression, the contents and structure of each level are then filtered to exclude the following:

- Ideas, procedures, processes, systems, methods of operation, concepts, principles or discoveries (17 U.S.C. § 102(b)).
- Facts, information and data (see *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 350-51 (1991)).
- Under the copyright doctrine of idea-expression merger, elements that are so driven by considerations of efficiency that they can be expressed in only one or a limited number of ways (and are therefore necessarily incidental to the program's ideas).
- Common, standard or stock programming practices, components or usages (*scènes à faire*).
- Features dictated by external constraints or requirements, such as legal compliance, industry demands or hardware or software specifications, standards or compatability requirements.
- Third-party and public-domain materials.
- Other non-protectable elements.

(See *Altai*, 982 F.2d at 706, 709-10.)

First formulated by the US Court of Appeals for the Second Circuit, the abstraction-filtration-comparison test is also controlling in the US Courts of Appeals for the Fourth, Fifth, Sixth, Ninth, Tenth, Eleventh and Federal Circuits (see *Comprehensive Techs. Int'l, Inc. v. Software Artisans, Inc.*, 3 F.3d 730, 734-735 (4th Cir. 1993); *Eng'g Dynamics, Inc. v. Structural Software, Inc.*, 26 F.3d 1335, 1342-43 (5th Cir. 1994); *R.C. Olmstead, Inc. v. CU Interface, LLC*, 606 F.3d 262, 274-75 (6th Cir. 2010); *Sega*, 977 F.2d at 1525; *Gates*, 9 F.3d at 834; *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1543 n.24, 1544 (11th Cir. 1996); *Atari Games Corp. v. Nintendo of Am., Inc.*, 975 F.2d 832, 839 (Fed. Cir. 1992).)

This test has also been adopted, in whole or in part, by district courts in the First, Seventh and Eighth Circuits (see, for example, *ILOG, Inc. v. Bell Logic, LLC*, 181 F. Supp. 2d 3, 11-12 n.4 (D. Mass. 2002); *Tetris Holding, LLC v. Xio Interactive, Inc.*, 863 F. Supp. 2d 394, 402-03 (D. N.J. 2012); *Woods v. Resnick*, 725 F. Supp. 2d 809, 818 (W.D. Wis. 2010); *Control Data Sys., Inc. v. Infoware, Inc.*, 903 F. Supp. 1316, 1322-24 (D. Minn. 1995)).

Method of Operation

Under this First Circuit test, set out in *Lotus Development Corp. v. Borland International, Inc.*, functional program features, such as methods of operation, procedures, systems and other subject matter excluded under Section 102(b) of the Copyright Act, are ineligible for copyright protection no matter how they are, or can be, expressed (49 F.3d 807, 815-16 (1st Cir. 1995); 17 U.S.C. § 102(b)).

Inherent Necessity

Under this standard formulated and adopted by the US Court of Appeals for the Third Circuit in *Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.*, everything that is unnecessary to the purpose or function (the "idea") of the computer program is expressive and therefore eligible for copyright protection (797 F.2d 1222, 1248 (3d Cir. 1986)). Although widely criticized, the test remains controlling in the Third Circuit.

Software Copyright Registration

Copyright protection is formality-free in the US and other member states of the Berne Convention for the Protection of Literary and Artistic Works. A software rights owner need not show any of the following to enjoy copyright protection for the owner's software:

- Publication.
- Affixation of copyright notice.
- Registration.
- Deposit of copies of the software in the US Copyright Office or Library of Congress (17 U.S.C. §§ 409(a) and 407(a) (registration and deposit are not conditions of copyright protection)).

These relaxed standards do not apply to software existing, but not published or registered, before January 1, 1978, or first published between January 1, 1978 and February 28, 1989. However, there are few, if any, software products that remain subject to the old requirements.

While registration is not required, there are substantial benefits to software copyright registration, including:

- The right to sue for infringement (17 U.S.C. § 411).
- The right to recover **statutory damages** and attorneys' fees if the software was registered before the infringement began or has an effective registration date within the sooner to occur of three months after its first publication or one month after the copyright owner learned of the infringement (17 U.S.C. § 412).
- Use of the registration as prima facie evidence of the copyright's validity if made within five years of the software's first publication (17 U.S.C. § 410).
- To stop the importation of infringing copies if the registration is recorded with US Customs (17 U.S.C. § 602; 19 U.S.C. § 1595a(c)(2)(C); 19 C.F.R. §§ 133.31-133.37).

For more information on US copyright registration requirements, see Sections 408 and 409 of the US Copyright Act (17 U.S.C. §§ 408 and 409).

Affixing a copyright notice to or in connection with software also provides substantial benefits, including its use as evidence against a defense of innocent infringement (17 U.S.C. § 401(d)).

Deposit Requirement

An application to the Copyright Office for software copyright registration requires the copyright holder's nonreturnable deposit of a copy or copies of at least a portion of the software being registered.

Because copyright registration requires at least a partial deposit and public disclosure of the software, owners frequently decide not to register the software's source code due to concerns that registration may compromise the source code's confidentiality and trade secret protection (see Securing and Maintaining Trade Secret Rights).

The Copyright Office's registration requirements seek to allay these concerns by permitting the applicant to deposit one of the following:

- The first and last 25 pages of source code, with portions containing trade secrets blocked out.
- The first and last ten pages of source code alone, with no blocked out portions.
- The first and last 25 pages of object code plus any ten or more consecutive pages of source code, with no blocked-out portions.
- For programs of 50 pages or less in length, the entire source code with trade secret portions blocked out.

If portions of the deposited software's code are blocked out:

- The blocked out portions must be proportionately less than the remaining material.
- The remaining material must represent an appreciable amount of original code.

The applicant may also register the software's source code under the Copyright Office's "rule of doubt," if it is unable or unwilling to deposit the source code and confirms in writing that the deposited object code contains copyrightable material. This form of registration does not result in a presumption of copyright validity.

Software Publication and Mandatory Deposit

The Copyright Act also provides for a mandatory deposit, within three months after the date of publication, of two complete copies of the best edition of any work (including software) that is published in the US (17 U.S.C. § 407(a)(1)).

Software is considered published if it is made available to the general public on an unrestricted basis, whether by sale, license, loan, rental or other transfer to an unrestricted group of users. Publication would almost certainly occur, for example, in the distribution of commercial off-the-shelf software to the general public. However, this distribution is almost always limited to the software's object code, with the program's source code left unpublished and therefore beyond the reach of the mandatory deposit requirement.

In addition, it has been argued that because no, or no legally cognizable, publication takes place in the following circumstances, the mandatory deposit requirement does not apply to:

- Limited publications (distributions) of object or source code to a selected class of persons (in the case of custom or enterprise software, for example) for a limited purpose and without the right of reproduction, redistribution or sale (for example, under a license agreement imposing restrictions on distribution and disclosure) (see, generally, *Chi. Bldg. Design, P.C. v. Mongolian House, Inc.*, 770 F.3d 610, 616-17 (7th Cir. 2014) and *Warner Bros. Entm't, Inc. v. X One X Prods.*, 644 F.3d 584, 593 (8th Cir. 2011)).
- Hosting of software to provide **software as a service** (SaaS) or other cloud services.

(See Copyright Registration for Computer Programs, US Copyright Office Circular 61 (08/2012) and Compendium of Copyright Office Practices: §§ 607 and 1509(1)(C) (3d ed. Dec. 2014).)

Scope and Limitations of Software Copyright Protection

General Scope of Copyright Protection
The owner of software copyrights enjoys exclusive rights of:

- Reproduction.
- Modification, adaptation and the preparation of other derivative works (for example, translations, bug fixes, new releases and new versions).
- Distribution, including by license, sale or rental (in electronic file or other form).
- Public display and performance of works generated by the software, including screen displays, graphics and other audio, visual and audiovisual content.

(17 U.S.C. § 106.)

The software copyright owner may exercise these rights itself, assign them to others or license them on an exclusive or non-exclusive basis. Each exclusive right stands on its own, allowing the copyright owner to retain and exploit certain rights while transferring or licensing others. For more information on copyright licensing considerations, see Copyright License Checklist.

Limitations of Copyright Protection: Exceptions, Exemptions and Fair Use
Given software's relatively short economic life, the finite term of software copyright protection is rarely, if ever, a matter of concern (see Comparison Chart: Forms of Software Protection). However, software copyright owners must carefully consider certain other statutory and judicial limitations on copyright protection. These include the right of the purchaser or other owner of a lawfully made copy of a computer program to:

- Sell or otherwise dispose of that copy (other than by rental, lease, lending or similar transactions) (17 U.S.C. §§ 109(a) and 109(b)(1)(A)) (the first sale doctrine).
- Display that copy at the place where the copy is located (17 U.S.C. § 109(c)).
- Make or authorize the making of another copy or adaptation:
  - for archival purposes;
  - as an essential step in the use of the program; or
  - for purposes of maintaining or repairing a device containing the program.

- (17 U.S.C. §§ 117(a) and 117(c).)
- Make fair use of the program by copying and reverse engineering its object code to uncover noncopyrightable methods and ideas for legitimate purposes such as supporting interoperability or creating new software products (17 U.S.C. § 107) (see, for example, *Sony Computer Entertainment, Inc. v. Connectix, Corp.*, 203 F.3d 596, 602 (9th Cir. 2000) and *Atari Games Corp. v. Nintendo of America Inc.*, 975 F.2d 832, 843 (Fed. Cir. 1992)).

However, by careful crafting of their software distribution models and license agreements, software rights owners can contract around these statutory limitations and acquire independently enforceable contract rights (see Contractual Protections).

Ownership of Copyrights in Software

Due to the size and complexity of computer code, software is usually created by a team of programmers. Therefore, ownership rights must be secured from each developer who may have co-authorship rights in the software. This is because copyright ownership automatically vests in the individuals who create the work, unless the work is a **work made for hire**. Under the Copyright Act's work-made-for-hire provisions, a natural or legal person who does not create a work is considered the work's author if it is either:

- The creator's employer, for whom the employee has created the work within the scope of her employment.
- A party that has specially commissioned the work under a written agreement with the work's creator acknowledging that the work is being made for hire.

(17 U.S.C. §§ 201 (copyright ownership) and 101 (definition of work made for hire).)

For specially commissioned software to qualify as a work made for hire, either the commissioning party and creator must have a de facto employer-employee relationship under the common law of agency, or the commissioned software must fall within one of nine specific statutory categories (17 U.S.C. § 101 and *Cmty. for Creative Non-Violence v. Reid*, 490 U.S. 730, 742-43, 751 (1989)).

Because computer programs per se are not included among the nine categories of works that non-employers may commission as works made for hire, a party commissioning an independent contractor to develop software should obtain the contractor's written assignment of the contractor's rights in the resulting work to ensure that the creator's rights in a program are effectively transferred to it. The commissioning party may also seek to qualify commissioned software for work-made-for-hire treatment by obtaining the commissioned contractor's written agreement that the software is a work made for hire and either or both:

- Establishing a de facto employment relationship with the contractor by fulfilling the common law agency requirements set out in *Reid* (490 US at 742-43, 751).
- Framing the software, where applicable, as:
    - part of an audiovisual work (see, for example, *Midway Mfg. Co. v. Arctic Int'l, Inc.*, 704 F.2d 1009, 1012 (7th Cir. 1983) (computer video game copyrightable as an audiovisual work) and Copyright Registration for Computer Programs, US Copyright Office Circular 61 (08/2012) (where applicable, a computer program may be registered as a visual arts work or motion picture/audiovisual work));
    - a translation of another program or program language; or
    - a compilation.

(17 U.S.C. § 101 (works made for hire include parts of an audiovisual work, translations and compilations).)

For more information on copyright ownership, the categories of copyrightable works and the copyright originality and fixation requirements, see Practice Note, Copyright: Overview: Copyright Ownership, Protected Subject Matter and Requirements for Copyright Protection.

Software Protection Under the Digital Millennium Copyright Act

The **Digital Millennium Copyright Act** (DMCA) prohibits third parties from circumventing technological measures the owner uses to prevent unauthorized access to its copyrighted software. Subject to certain express exceptions, the act prescribes criminal liability (17 U.S.C. § 1204) and a civil private right of action (17 U.S.C. § 1203) as remedies for:

- Circumventing a technological measure used to protect against the unauthorized access to software or other copyrighted materials (17 U.S.C. § 1201(a)(1)(A)).
- Trafficking in any technology, product or service that:
    - is primarily designed or produced for circumventing copy-control or other technological measures used to safeguard

against the infringement of copyrights;

- has only a limited commercially significant purpose or use other than to circumvent these copyright protections; or
- is knowingly marketed for use in circumventing these copy controls or other technological copyright protection measures.

- (17 U.S.C. § 1201(b).)
- Tampering with software copyright notices and other copyright digital rights management information (17 U.S.C. § 1202).

(See generally, *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 943-55 (9th Cir. 2010)).

DMCA Limitations

While the DMCA prohibits the circumvention of technological controls to gain unauthorized **access** to copyrighted materials, it does not prohibit the circumvention of technological controls that safeguard against the **copying** of these materials, other than by proscribing the trafficking in technologies and services designed primarily for this purpose (compare 17 U.S.C. §§ 1201(a)(1)(A) with 1201(b)).

DMCA Exceptions

Statutory exceptions to the DMCA's anti-circumvention restrictions include the circumventing of technological access controls for, among other purposes:

- Reverse engineering to achieve interoperability (17 U.S.C. § 1201(f)).
- Encryption research (17 U.S.C. § 1201(g)).
- Security testing (17 U.S.C. § 1201(j)).

Unlike the limited exceptions for permissible copying and modification set out in Section 117 of the Copyright Act (17 U.S.C. § 117), a party need not own a copy of the copyright-protected software, but rather, need only lawfully obtain a copy, or a right to use a copy, for these DMCA exceptions to apply.

DMCA Exemptions

The DMCA grants the Librarian of Congress the rulemaking power to exempt specific classes of works from the act's prohibition against circumvention of access controls. The exemptions last for three years (subject to extension or renewal) and apply to users of any exempted class of works if the DMCA's bar against circumvention is likely to adversely affect the user's noninfringing use of works in that class. (*17 U.S.C. § 1201(a)(1)(B), (C) and (D)* and see US Copyright Office DMCA Rulemaking Page.)

The current DMCA exemptions went into effect on October 28, 2015 and are set out on pages 65,944 through 65,964 of Volume 80 of the Federal Register.

Patents

A utility patent gives its owner the right to exclude others from making, using, offering to sell, selling or importing the

owner's patented invention. Unlike copyrights, patents protect the functional application of a software-implemented invention's underlying inventive idea rather than merely the software's coded expression (see Comparison Chart: Forms of Software Protection).

Legal and Regulatory Authority for Patents

US patents are regulated by the **US Patent and Trademark Office** (USPTO) under the authority of the Patent Act as amended on September 16, 2011 by the **Leahy-Smith America Invents Act** (AIA). For an overview of the AIA, see Practice Note, Leahy-Smith America Invents Act: Overview. For a listing of the effective dates of the act's key provisions, see Leahy-Smith America Invents Act: Key Effective Dates Chart.

For general legal and regulatory information and procedural guidance relating to patents, see the USPTO Patents website and Practice Note, Patent: Overview.

Software as Patent-eligible Subject Matter

The statutory requirements for obtaining patents on software-implemented inventions are the same as for other inventions. For a general discussion of the patent subject matter eligibility, utility, novelty, nonobviousness and definiteness requirements, see Practice Note, Patent: Overview: Patent Requirements.

Patent requirements are considerably more stringent than those governing copyrights and have become even more so as a result of the federal courts' increasing wariness of the patent subject matter eligibility of business method and other software-implemented inventions. Applicants for patents on these inventions typically claim them as novel methods, systems, machines (for example, as pre-programmed, special purpose computers), machine-readable physical media or a combination of these technologies.

The courts closely scrutinize the patent eligibility of these inventions because patent claims directed to them are often drawn so broadly as to cover abstract ideas (for example, mathematical formulas and algorithms) without limitations sufficient to confine the claims to specific applications.

The US Supreme Court most recently addressed this concern in *Alice Corp. Pty. Ltd. v. CLS Bank International* and *Bilski v. Kappos* (134 S.Ct. 2347 (2014); 561 U.S. 593, 604 (2009)). While declining to rule out the patent eligibility of software inventions altogether, the Court formulated strict requirements for their patent eligibility.

Following *Alice* and *Bilski*, the courts scrutinize patent claims drawn to software-implemented inventions as follows:

- Whether the claims are directed to one of the following statutory categories of patent-eligible subject matter under Section 101 of the Patent Act:
  - processes (including methods);
  - machines;
  - articles of manufacture;
  - compositions of matter; or
  - new and useful improvements of any of the above.

- (35 U.S.C. §101.)
- Even if the claimed software-based invention is patent eligible under one of these statutory categories, whether the patent claims are drawn to one of the following judicial exceptions to patent eligibility:

- laws of nature;
- natural phenomena; or
- abstract ideas.

If the software patent claims are directed to an abstract idea or any one or more of the other judicial exceptions to patent-eligible subject matter, the invention:

- Is not patent eligible if an analysis of the claims discloses that they are drawn merely to the abstract idea (or other ineligible subject matter).
- May be patent eligible if the claim's elements, considered individually or as an ordered combination, describe an **inventive concept** sufficient to ensure that the claims are drawn to significantly more than the abstract idea (or other ineligible subject matter).

(See *Alice*, 134 S.Ct. at 2354-55 and 2357 (adopting this two-part framework for distinguishing between patent-eligible and non-patent-eligible claims).)

The inventive concept requirement is not satisfied by patent claims that direct:

- The broad application of a natural law, phenomenon or idea to achieve a specified result without stating limitations sufficient to avoid preempting the use of the concept for all purposes.
- The use of a staple technology such as the internet or a generic or general-purpose computer to implement an abstract idea.
- Field of use limitations.

(See *Alice*, 134 S.Ct. at 2354-60 and *Bilski*, 561 U.S. at 604; see also *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) (software invention patent claims are not drawn to patent eligible subject matter where they instruct the practitioner to implement an abstract idea with routine, conventional activity).)

For more information on patent subject matter eligibility, see Practice Notes, Patent-eligible Subject Matter and Patent: Overview: Patent Requirements; Article, Patenting Business Methods and Software in the US.

Public Disclosure

The USPTO grants patents upon the examination and approval of a patent application that provides a clear and definite description of the claimed invention (35 U.S.C. § 112(b)) and includes information:

- Stating the manner and process of making and using the invention (enablement) (35 U.S.C. § 112(a)).
- Specifying the best mode the inventor contemplates for carrying out the invention (best mode) (35 U.S.C. § 112(a)).

These disclosures become public when the patent application is published and in the patent grant if a patent is ultimately issued. A key concern of software developers therefore is the extent to which they must disclose trade secrets in their source code to obtain patent protection. The Patent Act, USPTO practice and decisions interpreting the act's requirements help mitigate this concern. In particular, the USPTO regularly grants patents on software-implemented inventions without requiring the applicant's disclosure of the software's source code, flow charts or documentation where both:

- The invention is claimed in terms of its functionality.
- The application's disclosure of the invention is sufficient to allow a person having ordinary skill in the art to program the computer disclosed in the application by performing the steps described in the application.

In addition:

- The Patent Act requires the USPTO to hold applications in strict confidence for the later of:
  - the expiration of 18 months after the filing date (35 U.S.C. § 122(a)); or
  - the date a patent issues on the application, if the applicant certifies that the disclosed invention has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires that applications be published 18 months after filing (35 U.S.C. §§ 122(b)(1)(A) and 122(b)(2)(B)(1)).
- If the applicant withdraws its patent application or the application is otherwise no longer pending before the 18-month nondisclosure period expires, the application remains unpublished and confidential (35 U.S.C. § 122(b)(2)(A)(1)).

(See Manual of Patent Examining Procedure Section 2161.01 (citing *Fonar Corp. v. Gen. Elec. Co.*, 107 F.3d 1543, 1549 (Fed. Cir. 1997)).)

For a comparison of the advantages and disadvantages of patent protection relative to other forms of software protection, see Comparison Chart: Forms of Software Protection.

Ownership of Patents in Software Inventions

Traditionally, ownership of a pending US software (like any other) patent application and any patent issuing from it originally vested solely with the inventor or inventors (see MPEP § 301, ¶ I. Ownership (Nov. 2015)). Under the America Invents Act, for applications filed on or after September 16, 2012:

- The patent applicant may be the inventor, a person to whom the inventor assigned or is obligated to assign the invention, or a person who otherwise shows a sufficient proprietary interest in the invention.
- The patent is granted to the real party in interest.

(35 U.S.C. §§ 115(d) and 118, 37 C.F.R. 3.73(a) (2015)).

Trade Secrets

Legal Authority for Trade Secrets

Trade secrets are protected in the US:

- At the federal level under the Economic Espionage Act (EEA) (18 U.S.C. §§ 1831-1839), which was enacted in 1996 and significantly amended on May 11, 2016 by the Defend Trade Secrets Act of 2016 (DTSA), S. 1890, 114th Cong. (2015-2016).
- At the state level by state trade secret statutes.

Every state recognizes some form of trade secrets. The District of Columbia, the US Virgin Islands and all states other than Massachusetts and New York have adopted a version of the **Uniform Trade Secrets Act** (UTSA), in most instances with few or no changes to this model act. For more information on each state's approach, see Trade Secret Laws: State Q&A Tool.

The EEA, as amended by the Theft of Trade Secrets Clarification Act of 2012, provides for federal criminal and civil actions for theft of trade secrets (18 U.S.C. §§ 1832 and 1836). However, the statute did not provide for a private right of action until the DTSA's enactment, before which private enforcement of trade secrets was governed exclusively by state law. The DTSA supplements but does not preempt state law. For an overview of the DTSA, see Legal Update, Are You Ready for the Defend Trade Secrets Act?

Trade Secret Definition and Subject Matter

The DTSA defines "misappropriation" in language that is virtually identical with Section 1(2) of the UTSA and "trade secret" in terms that are also consistent with those set out in the UTSA. Specifically:

- The UTSA defines "trade secret" as follows:
- "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique or process, that:
- (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
- (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
- (UTSA § 1(4) (1985).)
- The EEA, as amended by the DTSA, similarly provides that:
- (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
- (A) the owner thereof has taken reasonable measures to keep such information secret; and
- (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]
- (18 U.S.C. § 1839(3).)

These definitions of trade secrets vary in detail, but commonly provide that protectable trade secrets include any business, financial, technical or other information that:

- Is not generally known or ascertainable through proper means by persons outside the trade secret owner's organization or control.
- Provides economic value or a business advantage to the owner by not being generally known.
- The owner makes reasonable efforts to keep confidential.

(Compare UTSA § 1(4) with 18 U.S.C. § 1839(3).)

Subject matter eligible for trade secret protection includes:

- Ideas, procedures, processes, systems, methods of operation, concepts, principles and discoveries (all of which are expressly excluded from copyright protection under the Copyright Act) (see Software as Copyrightable Subject Matter and 17 U.S.C. § 102(b)).
- Software, if, as is typically the case, the basis of the alleged trade secret misappropriation is not unauthorized copying, but instead a breach of contract, trust, confidence or other duty in acquiring, using or disclosing any confidential form or portion of the software, such as the software's source code (see *Altai,* 982 F.2d at 716-17 (trade secret claims not preempted under the Copyright Act)).

Remedies

The DTSA, like the UTSA, provides for the following remedies for trade secret misappropriation:

- An injunction to preserve evidence and prevent trade secret disclosure, provided that it does not:
  - prevent a person from entering into an employment relationship, and that conditions placed on such employment are based on evidence of threatened misappropriation and not merely on the information the person knows; or

- • otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business.
- • Damages measured by:
  - • actual loss and unjust enrichment, to the extent not accounted for in actual loss calculation; or
  - • a reasonable royalty for the unauthorized disclosure or use of the trade secret.
- • Exemplary damages up to two times the amount of the damages for wilful and malicious misappropriation.
- • Reasonable attorneys' fees for the prevailing party if:
  - • the misappropriation claim is made in bad faith;
  - • a motion to terminate an injunction is made or opposed in bad faith; or
  - • the trade secret was wilfully and maliciously misappropriated.

Unlike the UTSA, the DTSA also allows a trade secret owner to obtain an expedited *ex parte* seizure order in extraordinary circumstances to prevent the propagation or dissemination of the owner's trade secret. For information on the requirements for obtaining a DTSA seizure order, see Legal Update, Are You Ready for the Defend Trade Secrets Act?

Securing and Maintaining Trade Secret Rights

There is no registration requirement or procedure for trade secrets. Trade secret rights are acquired and maintained solely by the owner's reasonable efforts to preserve the secrecy of valuable confidential information:

- • Within the owner's organization (including employees and independent contractors).
- • Among selected third parties that need to use or review the information, such as customers, software developers, suppliers, service providers, lenders, joint venturers, merger partners and prospective acquirers.

This is typically accomplished by applying appropriate security measures at the owner's facilities and in its computer networks and using written confidentiality agreements.

No legal notice need be attached to trade secrets. However, the trade secret owner should mark software and related documentation as "SECRET" or "CONFIDENTIAL" to provide actual notice of the trade secret owner's rights, preserve secrecy and discourage misappropriation.

Rights holders in proprietary software typically safeguard their trade secret rights in source code by both:

- • Maintaining the source code in confidence.
- • Releasing it only selectively (for example, under an escrow arrangement) and under strict restrictions against copying, reverse engineering, transfer and disclosure. (Even though reverse engineering may qualify as a fair use under the Copyright Act, it can still violate the owner's trade secret rights if done in breach of a duty or enforceable contract obligation (see Limitations of Copyright Protection)).

By adopting these measures, the rights holder may preserve its trade secret rights in source code even if it widely sells, licenses and distributes copies of the software's object code to distributors or end users (see Comparison Chart: Forms of Software Protection).

The case for protecting trade secrets in object code is more difficult. The broad distribution of published object code is inconsistent with maintaining confidentiality and trade secret status. However, a software rights holder may seek to retain trade secret rights in object code if it either:

- • Uses the software (both source code and object code):
  - • solely for internal purposes;
  - • with appropriate physical, technical and organizational confidentiality safeguards;
  - • without external distribution; and

- • subject to employee confidentiality obligations.
- • Distributes the software's object code narrowly to a select, identifiable group of end users and subject to restrictions against copying, reverse engineering, transfer and disclosure.

If the software rights holder takes these protective measures, its trade secret rights may extend even to code embodied in a patented software invention. For this to happen, the USPTO must find that the applicant need not disclose the software's code because the statutory patent disclosure requirements are satisfied by the applicant's description of the software's function (see *Fonar, 107 F.3d at 1549*).

(See Comparison Chart: Forms of Software Protection for a comparison with other forms of software protection, including information on trade secret enforcement and remedies).

Contractual Protections

Unlike free and open-source software, most commercial software products are distributed under license solely in object code form. These written, shrinkwrap or clickwrap license agreements typically:

- • Grant narrowly drawn licenses.
- • Include confidentiality obligations and restrictions against copying, modifying, redistributing and, in certain instances, accessing the licensed software.
- • Prohibit reverse engineering and other means of uncovering or reconstructing the software's source code.

By crafting their license and other agreements in this fashion, software rights owners can:

- • Contract around statutory first sale, fair use (including reverse engineering) and essential use rights by licensing, rather than selling, physical copies of the owner's software subject to use restrictions and licensee waivers of these rights (see Limitations of Copyright Protection: Exceptions, Exemptions and Fair Use and *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1326 (Fed. Cir. 2003) (ruling that the First Circuit would find that parties are free to contractually waive the limited right to reverse engineer software under the copyright fair use exemption)).
- • Withhold distribution of tangible copies of the software by adopting a SaaS or other remote service model.

This strategy is based on the reasoning that, under the terms of a software license agreement, the licensee typically licenses rather than owns a copy of the software, and that the statutory limitations on copyright protection therefore do not apply. The software rights owner is then free to impose contractual restrictions on the transfer and use of copies of its software (see, for example, *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1103-04, 1110-13 (9th Cir. 2010)).

The practice of imposing confidentiality, reverse engineering and other contract restrictions on distributed source code makes it generally eligible for contract protection in addition to or in place of any trade secret, copyright or patent rights that may apply. Even though claims to enforce software contract rights may relate to copyrightable subject matter, they are not preempted under Section 301 of the Copyright Act because:

- • A party claiming breach of contract must prove extra elements beyond the infringement of its copyrights under Section 106 of the Copyright Act (17 U.S.C. § 106). These extra elements include, for example, valid consideration and mutual assent.
- • A breach of contract claim asserts rights only against a contractual counterparty, and not against the entire world or public at large.

Claims for breach of contract, therefore, are not equivalent to or preempted by copyright infringement claims (see, for example, *Bowers,* 320 F.3d at 1324-25 (collecting cases) and *ProCD, Inc. v. Zeidenberg,* 86 F.3d 1447, 1454-55 (7th Cir. 1996) (shrinkwrap software license agreement contract rights are not preempted by US copyright law)).

Accordingly, a software licensor may attempt to preserve both contract and statutory IP rights (for example, copyrights and patents) by framing license agreement restrictions as:

- Covenants that, if breached, give rise to an action for breach of contract. These covenants are typically set out in the license agreement's restrictions provision.
- Conditions to the license grant that, if breached, suspend or terminate the license and give rise to an action for copyright or patent infringement. These license conditions are commonly set out at the beginning of the license grant.
- Limitations to the scope of the license grant that also give rise to a claim of infringement if exceeded. These limitations are typically set out in the license grant and may include, for example, territorial, term, permitted use, authorized user, volume of usage and field of use limitations and restrictions.

(See *Graham v. James*, 144 F.3d 229, 236-37 (2d Cir. 1998); *Jacobsen v. Katzer*, 535 F.3d 1373, 1380-83 (Fed. Cir. 2008) and Standard Document, Software License Agreement (Pro-licensor): Section 2.1 (software license grant made "[s]ubject to the terms and conditions of this Agreement, and conditioned on Licensee's and its Authorized Users' compliance therewith").)

Computer Fraud and Abuse Act

The **Computer Fraud and Abuse Act** (CFAA) prohibits the unauthorized access to software and information embedded or stored in certain computers. These computers must either be used:

- In or affecting interstate or foreign commerce (a "protected computer" under 18 U.S.C. § 1030(e)(2)(B)).
- By or for the federal government or a financial institution.

The CFAA prescribes criminal fines, forfeitures and imprisonment for violations of the act (18 U.S.C. § 1030(b), (c), (i) and (j)). The CFAA also provides a private right of action permitting an individual who suffers damages to bring a civil action for damages or injunctive relief for certain of the violations specified in subsection (c)(4)(A)(i) of the act (see 18 U.S.C. § 1030(g) and (c)(4)(A)(i)(I), (II), (III), (IV) and (V)).

The act's precise scope remains the subject of conflicting case law. For a more detailed discussion of the CFAA and key related cases, see Practice Note, Data as IP and Data License Agreements: The Computer Fraud and Abuse Act.

State Law Claims

In addition to claims for breach of contract and trade secret misappropriation, a software rights owner may assert other state law claims to enforce its rights in software. These include, for example:

- Trespass to chattels (the unauthorized access to a computer system, which may house the rights holder's software).
- Unjust enrichment.
- Unfair competition.
- Tortious interference with contract, a prospective business advantage or potential business relations.

These causes of action are often pleaded as supplemental to a contract or federal statutory claim and their pleading and proof requirements vary from state to state.

Comparison Chart: Forms of Software Protection

	Copyright and DMCA	Patent	Trade Secret	Contract
Requirements	Copyright requirements are light: • **Originality** (independent creation and at least minimal creativity). • **Fixation** (in a tangible means of expression). • **Registration** and deposit of portions of the computer program with the Copyright Office required only: • to bring suit for infringement; • to obtain statutory damages; • as prima facie evidence of copyright validity; and • to have the US Customs Service stop importation of infringing copies. • **DMCA** • Software rights holder must use technological access controls to prevent unauthorized access to the software.	Patent requirements are more rigorous than those of any other form of protection: • **Patent eligible subject matter** (process, machine, manufacture, composition of matter or an improvement of any of the foregoing). Does not include any: • abstract ideas; • laws of nature; or • natural phenomena. • (35 U.S.C. § 101.) • **Utility** (35 U.S.C. § 101). • **Novelty** (35 U.S.C. § 102). • **Non-obviousness** (to a person having ordinary skill in the art) (35 U.S.C. § 103). • **Definiteness** (a clear and definite description of the claimed invention), including: • enablement (stating the manner and process of making and using the invention); and • best mode (stating the best mode the inventor knows for carrying out the invention). • (35 U.S.C. § 112(a) and (b).) • **Patent Disadvantages** • Patent requirements create certain disadvantages, including: • Applicant may be required to publicly disclose all or part of the invention's source code if a mere description of the software's function is not enough to satisfy patent disclosure requirements. • Public disclosure may enable third parties to work around the patent claims to develop functionally equivalent non-infringing inventions.	No government grant or registration is required for trade secret protection. Enjoyment of trade secret rights requires only that the information for which trade secret protection is sought: • Is not generally known or ascertainable through proper means. • Provides economic value or a business advantage to the owner from its not being generally known. • Is maintained in confidence by the owner's reasonable efforts to maintain its secrecy. • Protection in the US is governed in the District of Columbia, the US Virgin Islands, and most states (other than New York and Massachuseetss) under a version of the Uniform Trade Secrets Act (UTSA) and under the federal Defense of Trade Secrets Act (DTSA) amendment to the Economic Espionage Act (EEA). • Every state recognizes some form of trade secrets.	No government grant or registration is required for contractual protection. Enjoying the benefits of contract rights and restrictions relating to software requires: • Entry into a legally binding, valid agreement that accords with contract formation requirements of consideration and mutual assent. • Committing the agreement to a writing that is signed and delivered by the parties. • Including in the agreement the desired limitations and restrictions, for example, by: • structuring the agreement as a software license rather than sale; • limiting software transfers under the license to object code only; • drafting a narrow license grant permitting use in object code form only and describing the nature and geographic and temporal scope of permitted use; • including express restrictions against copying, modifying, reverse engineering or transferring the licensed software; and • including licensee confidentiality obligations. • Alternatively, the software rights holder may avoid the risk that end users might copy, modify or reverse engineer its software by adopting a SaaS or other cloud service model under which it provides hosted software services rather than distributing copies of the software.
Cost and Speed	Copyright protection for software	Obtaining a patent on a software-	Trade secret rights:	Contractual protection for software

of Securing Protection	can be obtained more quickly, cheaply and reliably than patent protection. Copyright registration is a relatively quick ministerial process and the costs of obtaining it are low:
	
	• No costs if copyrights in the software are not registered.
	• Minimal costs for copyright registration.
	• The costs of copyright infringement litigation can be high, but typically not as high as patent litigation.
		implemented invention can be lengthy, costly and vulnerable to challenge.
		
		• In 2014 the average time from the application filing date to receipt of a final determination of patent allowance or rejection was 27.4 months (see USPTO 2014 Performance & Accountability Report (Annual Report) at 45).
		• Patent prosecution costs typically include the payment of substantial patent attorneys' or agents' fees for:
		  • conducting a patent search to detect patent-precluding prior art;
		  • drafting the patent application;
		  • steering the application through the USPTO patent filing and prosecution process;
		  • responding to USPTO Office actions and submitting evidence and arguments to counter the examiner's reasons for rejecting the application;
		  • redrafting the application; and
		  • repeating responses and submissions to the USPTO examiner until the applied-for patent claims are finally rejected or allowed.
		  • Patent infringement litigation is typically costly, lengthy and complex.
			• Accrue immediately for qualifying information.
			• Do not require payment of prosecution, registration or maintenance fees to acquire or maintain.
			• Require expenditure of maintenance costs, for example:
			  • the costs of instituting and maintaining technical, physical and organizational security policies and measures; and
			  • the transactional costs of entering into employee and third-party confidentiality agreements.
				accrues upon the software rights holder's entry into a binding license, confidentiality or other agreement relating to the software.
				
				Acquiring and maintaining contractual protection requires the rights holder's expenditure of the:
				
				• Transactional costs (including attorneys' fees) of drafting and, if the contract is negotiated, negotiating the terms of the agreement.
				• The costs of monitoring and auditing licensee use.

Strength and Scope	**Copyright Act Protection** The software copyright owner has exclusive rights of: • **Reproduction**. • **Preparation of Derivative Works** (new versions, updates, adaptations,	**Patent Act Protection** A utility patent owner has the right to exclude others from performing any of the following acts relating to its patented invention: • **Making**. • **Using**.	**Trade Secret Protection** The owner of trade secret rights in confidential software code, documentation, flow charts, programmer note or related materials may bring claims for trade secret misappropriation arising from the unauthorized acquisition, use or disclosure of	**Contractual Protection** Contract rights provide an additional layer of protection that does not preempt or supersede any IP rights the software rights holder may have in the software at any time before, during or after the term of the software agreement.

Legal Protection of Software, Practical Law Practice Note 7-575-8965 (2016)

---

modifications and translations).
- **Distribution** (including by license, sale or rental).
- **Public display and performance** (for example, screen displays, graphics and other software-generated audio, visual and audiovisual content).
- **Copyright Limitations**
- Does not protect against independent creation of identical or substantially similar software.
- Any purchaser or other owner of a lawfully made copy of the copyright holder's computer program has the rights to:
  - sell or transfer that copy outright (but not by rental, lease, lending or similar transactions) (first sale doctrine);
  - display that copy where the copy is located (17 U.S.C. § 109(c));
  - make or authorize the making of another copy or adaptation: for archival purposes; as an essential step in the use of the program; or
  - to maintain or repair a device containing the program.
- Make fair use of the program by copying and reverse engineering its object code to uncover methods and ideas for legitimate purposes, such as providing interoperability or creating new software products.
- **DMCA Protection**
- DMCA prohibits circumvention of technological controls to gain unauthorized access to copyrighted software. Other than specific uses permitted by DMCA exceptions, the act prohibits circumvention even for purposes that qualify as copyright fair use.

- **Offering to sell**.
- **Selling**.
- **Importing into the US**.
- **Supplying** (components of a patented device or product in or from the US intending that they be combined outside the US in a way that would contributorily infringe or induce infringement if the combination occurred in the US).
- (35 U.S.C. § 271.)
- Unlike copyrights, patents protect a software-implemented invention's functional application rather than the software's coded expression. The scope of patent protection can therefore be greater than that of copyright because:
- No proof of access to or copying of the software's code is required to prove infringement.
- Patents, unlike copyrights, protect against the independent creation of functionally equivalent software.
- Because of the considerable time, difficulty and expense of obtaining patents on software-implemented inventions, these patents generally are sought only where:
- Available copyright or trade secret protection make the length of the patent prosecution process a non-material consideration.
- The patent provides a competitive advantage that cannot be achieved by copyright or trade secret protection.
- **Patent Limitations**
- In addition to the risk that the applicant may be required to publicly disclose the object or source code of its invention, a key limitation of patent protection is that the patent owner has only the right to exclude others from practicing the owner's invention. It does have the affirmative right to use its invention, the use of which may

these materials or their embodied ideas, data or information:
- By improper means.
- Under circumstances giving rise to a duty to maintain secrecy or limit use (for example, an employee's duty of loyalty or a valid contractual confidentiality obligation).
- With knowledge or reason to know that the trade secret, or knowledge of the trade secret, was derived from or through a person who:
  - acquired the trade secret by improper means; or
  - owed a duty to maintain its secrecy or limit its use.
- By a person who, before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it was acquired by accident or mistake.
- (See UTSA § 1(2).)
- **Trade Secret Limitations**
- Trade secret protection for any confidential portion of a computer program's code may be lost if the software rights owner:
- Deposits that portion in the Library of Congress or Copyright Office to fulfill copyright mandatory or registration deposit requirements (see Deposit Requirement).
- Applies for a patent, the USPTO requires disclosure of that portion of the code and the patent applicant:
  - discloses this information to the USPTO;
  - prosecutes the application through to the expiration of the 18-month pre-publication period; and
  - the patent application is published disclosing the code.
  - Software trade secret protection may also be lost if:
- The software code or information sought to be protected is:
  - developed by a third

A software licensor may therefore seek to preserve the right to assert both breach of contract and IP infringement claims for a licensee's breach of a software license agreement by including in the agreement:

- Covenants that, if breached, give rise to an action for breach of contract.
- Conditions to the license grant that, if breached, suspend or terminate the license and give rise to a claim for infringement.
- Limitations to the scope of the license grant that, if exceeded, also give rise to a claim for infringement.

Legal Protection of Software, Practical Law Practice Note 7-575-8965 (2016)

• **DMCA Limitations**
• Limitations of DMCA coverage include:
• That it does not prohibit circumvention of technological controls over unauthorized copying.
• It includes statutory exceptions for:
  • reverse engineering to achieve interoperability;
  • encryption research; and
  • security testing.
• It provides three-year exemptions for classes of software designated by the Librarian of Congress.
	infringe a broader, dominant or "blocking" patent.	party;
		• intentionally or accidently disclosed by or on behalf of the owner;
		• not safeguarded by reasonable efforts to keep the code confidential; or
		• otherwise made public without breaching a duty of non-disclosure.
		• A third party obtains the code or other confidential software material without knowing or having reason to know that it was obtained improperly or in violation of a duty of confidence.	

Duration	The term of copyrights in software created on or after January 1, 1978 starts when the software is created and expires:
	
	• 70 years after the author's death, for a work created by an individual developer not as a work made for hire.
	• 70 years after the last author's death, for a work of joint authorship not created as a work made for hire.
	• For works made for hire and pseudonymous and anonymous works, the later of:
	  • 120 years after creation; or
	  • 95 years after first publication.
	  • (17 U.S.C. § 302.)
		For utility patent applications filed on or after June 8, 1995, the maximum duration of a US patent is 20 years from the filing date of the earliest non-provisional US patent application to which priority is claimed, subject to any terminal disclaimers or patent term adjustments for USPTO or FDA delays.	Trade secret protection lasts until the trade secret's subject matter becomes generally available or its owner no longer derives economic value from its secrecy.	Contractual protection lasts during the agreement's term and for any period during which a provision is stated to survive the expiration or termination of the agreement.

Enforcement	A civil action in the appropriate US district court may be brought by: • The legal or beneficial owner of an exclusive copyright in software for direct, contributory or vicarious copyright infringement (17 U.S.C. § 501(b)). • Any person who is injured by a violation of the DMCA anti-circumvention provisions (17 U.S.C. § 1203).	A software patent owner may bring an action for direct, contributory or induced patent infringement in federal district court or, where applicable, the International Trade Commission (ITC).	Trade secret rights may be enforced by claims of trade secret misappropriation filed in either: • State court. • Federal district court if there is federal diversity or supplemental jurisdiction, or jurisdiction based on a substantial and related copyright or patent claim (28 U.S.C. §§ 1332, 1367 and 1338(b)). • For more information on enforcing trade secret rights, see Practice Note, Trade Secrets Litigation.	Contract rights may be enforced by bringing a claim for breach of contract in either: • State court. • Federal district court if there is federal diversity or supplemental jurisdiction, or jurisdiction based on a substantial and related copyright or patent claim (28 U.S.C. §§ 1332, 28 U.S.C. §§ 1367 and 1338(b)).
Remedies	**Copyright Remedies**	**Patent Remedies**	**Trade Secret Remedies**	**Contract Remedies**

Legal Protection of Software, Practical Law Practice Note 7-575-8965 (2016)

• Preliminary and permanent injunctions. • Impoundment and destruction of the infringing articles. • Monetary damages (actual monetary loss). • Accounting of the infringer's profits (to the extent not duplicative of the copyright owner's lost profits). • Statutory damages (instead of direct damages if the copyright owner so elects and timely registers its copyrights in the software). • Costs and attorneys' fees at the court's discretion if the software copyrights are timely registered. • (17 U.S.C. §§ 502, 503, 504, 505 and 412.) • **DMCA Remedies** • Preliminary and permanent injunctions. • Award of: • actual damages and any additional violator profits, including up to treble damages for repeated violations; or • statutory damages. • Impoundment of devices or products involved in the violation. • (17 U.S.C. § 1203.)	• Preliminary and permanent injunctions (35 U.S.C. § 283). • Direct damages, including lost profits or reasonable royalties (35 U.S.C. § 284). • Enhanced (up to treble) damages (35 U.S.C. § 284). • Attorneys' fees in exceptional cases (35 U.S.C. § 284).	Depending on the controlling state law jurisdiction, in addition to any applicable copyright or patent remedies, the owner of trade secrets in software may obtain some or all of the following remedies for the secrets' misappropriation: • Expedited *ex parte* seizure order (under the DTSA). • Preliminary and permanent injunctions against further use or disclosure. • Mandatory and supervisory injunctions, such as the appointment of a special master to observe and report on the duties and activities of an ex-employee in the employee's role with a new enterprise or employer. • Direct damages, lost profits, reasonable royalties or an accounting of the defendant's profits. • Double, treble or other exemplary damages. • Attorneys' fees. • In addition, for violations of the EEA, the US Attorney General may seek: • An injunction for civil violations (18 U.S.C. § 1836). • Penalties of up to ten years of imprisonment and a maximum of $5 million in corporate fines for criminal violations (18 U.S.C. § 1832).	Depending on the controlling state law jurisdiction, in addition to any applicable copyright or patent remedies, the software rights holder may obtain some or all of the following relief for a licensee's breach of the license agreement: • Preliminary and permanent injunctions against further use or disclosure. • Direct damages, lost profits, reasonable royalties or an accounting of the licensee's profits. • Exemplary damages. • Attorneys' fees if provided for in the agreement.