Source

Open for Business

A Practical Guide to Open Source Software Licensing

Heather Meeker

Second Edition
Table of Contents

Preface........................................................................................................................................... i

Part I: A Foundation.......................................................................................................................... 1
   Chapter 1: The Philosophy of Free and Open Source Software.................................................. 3
   Chapter 2: A Tutorial on Computer Software ............................................................................. 11

Part II: Basic Open Source Theory and Compliance........................................................................ 31
   Chapter 3: Common Open Source Licenses .................................................................................. 33
   Chapter 4: License Compatibility.................................................................................................. 51
   Chapter 5: Conditional Licensing................................................................................................ 61
   Chapter 6: What Is Distribution?.................................................................................................. 71
   Chapter 7: Notice Requirements .................................................................................................. 85

Part III: Advanced Compliance.......................................................................................................... 93
   Chapter 8: The GPL 2 Border Dispute ......................................................................................... 95
   Chapter 9: LGPL 2.1 Compliance ............................................................................................... 121
   Chapter 10: GPL 3 and Affero GPL 3 ......................................................................................... 125
   Chapter 11: Open Source Policies .............................................................................................. 139
   Chapter 12: Audits and Due Diligence ....................................................................................... 143

Part IV: Intersection with Patents and Trademarks....................................................................... 151
   Chapter 13: Open Source and Patents (Grants, Defensive Termination)................................. 153
   Chapter 14: Open Source and Patent Litigation Strategy............................................................ 179
   Chapter 15: Trademarks ............................................................................................................. 183

Part V: Contributions and Code Releases....................................................................................... 187
   Chapter 16: Open Source Releases ............................................................................................ 189

Part VI: Additional Topics ............................................................................................................... 201
   Chapter 17: Mergers & Acquisitions and Other Transactions .................................................... 203
   Chapter 18: Government Regulation ......................................................................................... 213
   Chapter 19: Enforcement and Obstacles to Enforcement ............................................................ 219
   Chapter 20: Open Standards and Open Source ........................................................................ 253
   Chapter 21: Open Hardware and Data ....................................................................................... 257
   Forms and Checklists .................................................................................................................. 261
   Glossary and Index ..................................................................................................................... 263
   Case Index ................................................................................................................................. 269
The conditions of open source licenses—requirements to deliver notices, make source code available, or relicense on the same terms—are triggered by distribution. For almost all open source licenses, if you don’t redistribute the software, you need not meet any conditions to exercise the license. But what is distribution? Twenty years ago, the answer to this question was easy, but it gets more difficult every year.

**An American Term of Art**

The GPL is in essence a conditional copyright license, and it has no choice-of-law provision. Therefore, theoretically, only an action regulated by the applicable copyright law can trigger application of its copyleft conditions. In the United States, the core commercial right of copyright is called distribution or publication. Therefore, in the United States, the question of what triggers copyleft conditions is identical to the question of what constitutes distribution under copyright law.

GPL 3, which was released in 2007, attempted to internationalize the license to fit with local variations on this concept by using neutral words such as “propagate” and “convey.” Unlike its successor, GPL 2 specifically named distribution as the trigger for copyleft requirements. GPL 2 remains in wide use—and it particularly is the license applicable to the Linux kernel—so the question of what constitutes distribution under GPL 2 is still alive and well in the open source world.

Distribution, though one of the enumerated rights of copyright under US law, is not defined in the Copyright Act (Title 17 of the United States Code). Title 17 grants a copyright owner the exclusive right to “distribute copies … of the copyrighted work to the public by sale or other transfer of ownership, or by

---

rental, lease, or lending.” The Act states that “offering to distribute copies … to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication.” But this does not define distribution. Where a statute’s terms are ambiguous on their face, the rules of statutory interpretation allow us to look to the statute’s legislative history. The 1976 House Report also does not define distribution but defines publication in the negative by saying, “[A]ny form of dissemination in which a material object does not change hands—performances or displays on television, for example—is not publication.” Later case law equated distribution with publication.

Section 106(3) of the Copyright Act accords to the copyright owner the exclusive right “to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending.” Put differently, the copyright owner has the exclusive right to publicly sell, give away, rent, or lend any material embodiment of his work. As the legislative history of this section shows, the definition of distribution is “virtually identical with that in the definition of publication in section 101.” Thus, in essence, exclusive right of distribution is a right to control the work’s publication.

**Determining When Distribution Has Occurred**

In the United States, therefore, distribution means providing a tangible copy to another person. The question of what constitutes distribution therefore devolves to two questions: What is a tangible copy, and what is another person?

The transfer of the work must be made “to the public” to trigger the definition of distribution under the Copyright Act. In the absence of a statutory definition of the phrase to the public, courts have held that a “limited” distribution that “communicates the contents of a manuscript to a definitely selected group and for

---

2 17 U.S.C. Section 106(3).
a limited purpose, and without the right of diffusion, reproduction, distribution or sale,” is not distribution to the public.9

In other words, a distribution is a “general” publication if it is not made (1) to a limited group; (2) for a limited purpose; and (3) “without the right of diffusion, reproduction, distribution or sale.” The legislative history of the Copyright Act makes it clear that, “when copies or phonorecords are offered to a group of wholesalers, broadcasters, motion picture theaters, etc., publication takes place if the purpose is further distribution, public performance, or public display.”10 Thus, even if the work is distributed to a single person or entity, the publication would be general if the recipient is free to diffuse, reproduce, distribute, or sell copies of the work.

In the contemporary world of information technology, many activities stray close enough to the transfer of a copy to challenge the boundaries of this definition of distribution. It is these activities that make the question of what is distribution under GPL of such great interest to companies implementing day-to-day strategies for GPL compliance.

Starting at the baseline, the most obvious business case is that of a distributed product. Whether the product is software alone or a hardware product as well, businesspeople understand what it means to sell a product and for it to change hands. Companies trying to comply with open source licenses like GPL 2 therefore have more difficulty assessing activities that they do not consider to be the business case of commercial distribution but that may nevertheless constitute distribution under the law. This chapter discusses those other business cases, from the clearest to the murkiest, as a matter of law.

A Clear Case in the Clouds

Companies often wonder whether software transmissions or remote use—sometimes called the ASP or SAAS model, or cloud computing—constitute distribution.

While this is one of the most controversial aspects of free software licensing, it is not a difficult interpretation question under US law for GPL 2. Advocates of

---


free software have long recognized that if the trigger for copyleft requirements is
distribution, increasingly popular cloud computing models will circumvent those
requirements. This is sometimes referred to as the “ASP loophole.”

During the drafting of GPL version 3, this issue engendered significant con-
troversy. At one point, a variation on GPL 3 was proposed to allow the author to
select an option that would cause online use to trigger copyleft requirements. Ulti-
mately, this variation was removed from GPL 3 and memorialized in an alternative
form of the license known as the “Affero GPL.” The basic form of GPL 3 makes
it clear that ASP or SAAS use does not trigger copyleft requirements. In GPL 3,
copyleft is triggered by conveying rather than by distribution, and “[t]o ‘convey’ a
work means any kind of propagation that enables other parties to make or receive
copies. Mere interaction with a user through a computer network, with no transfer
of a copy, is not conveying.”

Under US law, distribution requires actual transfer of a copy, in whatever
form. Therefore, under US law, SAAS use—which involves accessing software
without transfer of a local copy to the user—does not trigger copyleft require-
ments under GPL.

The Edge Cases

Leaving aside the two relatively clear business cases of a distributed product
(which clearly constitutes distribution) and pure SAAS deployment (which does not), we turn to some of the edge cases that also are common business activities
but do not fall so neatly on one side of the distribution coin or the other.

• Employees. While companies often worry about this case, it is not a diffi-
cult one. Clients often ask whether “internal distribution” within a corpo-
ratio triggers copyleft requirements. However, under law, there is no such
thing as internal distribution because corporations and their employees
are considered a single legal person. Therefore, one employee’s providing a
copy of software to another employee of the same company in the course
of performing their duties as employees is clearly not distribution; while

11 The term is often attributed to Richard Stallman, but that may not be accurate. See the April
3, 2007, interview with Mr. Stallman in Groklaw, in which he says the term is misleading:


13 It is worth considering that even in SAAS implementations, some components may be distrib-
uted. Today, most SAAS is accomplished only via a browser, so client software is no longer a
common requirement to use SAAS. However, there are always exceptions, mostly notably Java-
Script or mobile applications. Keep in mind that these are usually clearly distributed and would
be subject to copyleft requirements.
it may be a transfer of a copy, it is not a transfer to another person. Free software advocates sometimes refer to this as providing *private copies*.

- **Independent contractors—individuals.** Companies often engage individuals as independent contractors rather than as employees. Emerging growth companies, in particular, do this to avoid the regulatory overhead costs (such as employment taxes) associated with hiring employees. The function of a contractor in such cases is nearly identical to that of an employee; however, because a contractor is not an employee, providing a copy of software to a contractor could be considered distribution. This is one of the thornier areas of GPL 2 interpretation, and it is discussed in more detail below.

- **Independent contractors—consulting firms.** Companies often hire small consulting firms to develop, test, or support software. These consultant entities often consist of a few persons working in a team, but their functional relationship to the company is similar to that of an individual consultant or an employee. Individuals in small consulting firms are not, legally speaking, employees of the company, and therefore, providing a copy to them is probably distribution. However, there may be arguments that the copies are not intended for public availability and that, thus, transferring them is not publication and therefore not distribution. This argument has risks, but it is probably supportable under law, particularly if buttressed by a written consulting agreement that recites the parties’ intentions. This business case is very similar, in a legal sense, to the engagement of an individual contractor.

- **Independent contractors—outsourcing.** Larger companies often outsource entire business areas such as software development or software support. Outsourcers are clearly separate companies, rather than employees, so providing a copy to them is clearly providing a copy to a person other than the company. However, some outsourcing companies provide “leased” staff to work on servers and equipment owned or controlled by their customers. In this case, IT companies may reasonably make arguments that copies made available to those persons have not been transferred outside the companies’ control. This argument may be less successful, however, for outsourcers who are outside the United States—as most are. The international divide may make it unclear which body of law will determine what is distribution under GPL.

- **Cloud providers.** With the rise of cloud-based computing services such as Amazon Web Services, companies worry about whether uploading soft-
ware to a cloud service is distribution. Although the question is subject to some debate, the answer is probably not. Although technically this involves the transfer of a copy to the cloud service provider, the virtual space in which the copy resides is under the control of the company user; cloud services agreements generally do not provide the cloud service provider with any control over the information stored in a cloud account. Any transfer of a copy, then, is not “general” under copyright law.

- **Subsidiaries and affiliates.** Companies often create affiliate structures to conduct business for various strategic reasons such as tax planning, needing to do business in other countries through local entities, or engaging in a particular line of business. For example, a company may use a copy of the Linux kernel, which it has modified for its own purposes, to run an online service. It may provide this modified kernel to a subsidiary or affiliate in Europe or China to offer a local service. For tax, regulatory, or other reasons, it may be important to locate the servers for the business in Europe or China in those territories. If the recipient entity is a wholly owned subsidiary of the company, the company has a good argument that, due to unity of ownership, the copy is a “private copy” that has only been given to the company itself and that, therefore, no distribution has taken place. This argument is also reasonably strong for a majority-owned affiliate because the parent effectively exercises control over the affiliate. But if the recipient is a minority-owned affiliate, the company faces a more serious concern over whether distribution has taken place. This scenario is quite common, particularly where companies have little choice but to create minority-owned operating entities in territories, like India or China, that impose significant restrictions on foreign ownership of businesses operating within their borders.

- **Mergers and acquisitions.** US law can be quirky and counterintuitive on the subject of assignments by operation of law in connection with mergers and acquisitions. An assignment of a contract (or a license) occurs when one party to the contract transfers its rights to another. Therefore, for instance, if a corporation enters into an agreement with another party, it may be able to transfer that agreement to another corporation—depending on what the agreement has to say about it. Contracts are generally considered

---

14 In addition, because the copyleft requirements of GPL only allow binary recipients to seek source code copies, where the recipient is a majority-owned affiliate, the issue may be moot; the recipient would simply never make the request.
assignable under US law, but intellectual property licenses are subject to different rules. Generally, nonexclusive copyright and patent licenses are not assignable. Therefore, if a corporation takes a nonexclusive license to a patent, it cannot transfer the license to another corporation unless the license agreement expressly allows transfer. To make matters even more complicated, there are courts that have held that an acquisition—even a transaction such as a reverse triangular merger in which the target entity survives—can be an assignment by operation of law. Even if the licensee is the same corporation before and after the acquisition, the license may not be exercisable after the transaction. This rule of law may also have implications for the definition of distribution. If a change of control is an assignment by operation of law, one might logically conclude that it also constitutes providing a copy to another entity and thus a distribution triggering copyleft obligations. Keep in mind, also, that the effectuation of some forms of M&A transactions, such as asset sales, are clearly assignments and also likely to constitute distribution under GPL 2.

- **Productization.** Although this business case is not complex from a legal standpoint, it is such a frequent trap for companies managing open source compliance that it is worth mentioning in any discussion of distribution issues. Companies that offer SAAS solutions tend to rely on the fact that they are not distributing their products to ensure their GPL compliance. They do this by merely avoiding licenses like Affero GPL that have requirements even in the absence of distribution. However, this can be a dangerous strategy. For a business development manager who is not focused on legal and technical niceties, it is easy to cause transactions to trip over the distribution line. A company with a SAAS offering may, for instance, approach a customer operating in a highly regulated market (such as health care or financial services) that will insist that the SAAS offering be operated via a private instance on the customer’s premises or on servers under the customer’s control. This demand usually arises from security or regulatory auditing concerns. From the business point of view, a private instance of a SAAS product is a technical detail. But of course, providing a copy to the customer will likely constitute distribution. If the company’s

---

15 Other than special kinds of contracts, where assignment would change the basic nature of the contract, like contracts for personal services or requirements contracts. See Restatement (Second) Contracts, Section 317.

16 For patent, see *PPG Indus. Inv. v. Guardian Indus. Corp.*, 597 F.2d 1090 (6th Cir. 1979). For copyright, although the law is conflicting see, e.g., *SQL Solutions, Inc. v. Oracle Corp.*, 1991 U.S. Dist. LEXIS 21097 (N.D. Cal. 1991). This is an unpublished decision and arguably contrary to the California Supreme Court’s view in *Trubowich v. Riverbank Canning Co.*, 182 P.2d 182 (Cal. 1947).
open source compliance strategy hinges on refraining from distribution within the context of a SAAS model, the company may find that it cannot deliver a compliant product in any reasonable amount of time—usually because it has intermixed GPL- and non-GPL-compatible code or has not properly kept track of open source elements in the product.

With these edge cases in mind, we now turn to extrinsic evidence of the meaning of GPL 2 and best practices in managing distribution issues.

**The FSF View**

The GPL 2 FAQ, promulgated by the Free Software Foundation (FSF), offers the FSF’s insight into what it considers a distribution that would trigger copyleft requirements. For example, one of the FAQs is as follows:

> Is making and using multiple copies within one organization or company “distribution”?

No, in that case the organization is just making the copies for itself. As a consequence, a company or other organization can develop a modified version and install that version through its own facilities, without giving the staff permission to release that modified version to outsiders.

However, when the organization transfers copies to other organizations or individuals, that is distribution. In particular, providing copies to contractors for use off-site is distribution [emphasis added].

The FAQ also discusses a transfer between an organization and a majority-owned subsidiary:

> Does moving a copy to a majority-owned, and controlled, subsidiary constitute distribution?

Whether moving a copy to or from this subsidiary constitutes “distribution” is a matter to be decided in each case under the copyright law of the appropriate jurisdiction. The GPL does not and cannot override local laws. US copyright law is not entirely clear on the point, but appears not to consider this distribution [emphasis added].

---

17 [www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#InternalDistribution](http://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#InternalDistribution). This same FAQ appears in the GPLv3 FAQ as well ([www.gnu.org/licenses/gpl-faq.html#InternalDistribution](http://www.gnu.org/licenses/gpl-faq.html#InternalDistribution)).
If, in some country, this is considered distribution, and the subsidiary must receive the right to redistribute the program, that will not make a practical difference. The subsidiary is controlled by the parent company; rights or no rights, it won’t redistribute the program unless the parent company decides to do so.\(^{18}\)

In this FAQ, the FSF acknowledges that, at least in the United States, a transfer to or from a majority-owned and majority-controlled subsidiary may not constitute distribution. Further, the FSF gives weight to one organization’s effective control over another to determine whether the two entities are effectively one entity for the purposes of the analysis.

There is also discussion in the GPL 2 FAQ about providing modifications of GPL code under a nondisclosure agreement:

Does the GPL allow me to develop a modified version under a nondisclosure agreement?

Yes. For instance, you can accept a contract to develop changes and agree not to release your changes until the client says OK. This is permitted because in this case no GPL-covered code is being distributed under an NDA.

You can also release your changes to the client under the GPL, but agree not to release them to anyone else unless the client says OK. In this case, too, no GPL-covered code is being distributed under an NDA, or under any additional restrictions.

The GPL would give the client the right to redistribute your version. In this scenario, the client will probably choose not to exercise that right, but does have the right.\(^{19}\)

Many companies find the distribution question confusing because they find this FAQ confusing. In this FAQ, the FSF considers two different scenarios: (1) the contractor releases the modified code to the public generally at the direction of the client, and (2) the contractor releases the modified code to the client under the GPL, and the contractor promises not to release the modified code to anyone else. Unfortunately, this FAQ section does not specify whether “a modi-

\(^{18}\) [www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#DistributeSubsidiary](http://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#DistributeSubsidiary).

This same FAQ appears in the GPLv3 FAQ as well ([www.gnu.org/licenses/gpl-faq.html#DistributeSubsidiary](http://www.gnu.org/licenses/gpl-faq.html#DistributeSubsidiary)).

\(^{19}\) [www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#DevelopChangesUnderNDA](http://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.html#DevelopChangesUnderNDA).

This same FAQ appears in the GPLv3 FAQ as well ([www.gnu.org/licenses/gpl-faq.html#DevelopChangesUnderNDA](http://www.gnu.org/licenses/gpl-faq.html#DevelopChangesUnderNDA)).
fied version” refers to a modification of the contractor’s own GPL code, to GPL code that may have been already modified by the client, or to a modification of third-party code. Clearly, these three situations could be analyzed differently. If the FAQ refers to GPL code owned by either the client or the contractor, it is a trivial question; obviously, the owner of GPL code can choose to deliver that code under GPL terms or not as it sees fit, because an author (as licensor) is not bound by the copyleft obligations of GPL—only the licensee is. If the FAQ refers to modifications to third-party code, it implies that even if the delivery of the original code constitutes a distribution, that distribution does not trigger the copyleft obligations of GPL.

Other information promulgated by the FSF suggests that this FAQ element is not intended to address third-party code. But that is, by far, the most common situation: a company wants to use some GPL code but needs modifications, so it finds an expert in the code willing to modify it on a contract basis. In fact, this scenario is so common that it is touted as one of the advantages of open source software. But the company may not plan to ever distribute the software. Therefore, if providing the code to the consultant is distribution that triggers copyleft requirements, the company will likely be unwilling to engage the consultant.

The FSF’s view is problematic for a couple of reasons. First, a practical problem: companies that hire consultants simply don’t distinguish between the business cases of in-house and contractor development. They do not expect to encounter a completely different GPL compliance landscape based on the distinction. Because FSF’s view contravenes business expectations, it is a trap for the unwary. Second, a legal problem: the provision of code for development purposes is more akin to “communicat[ing] the contents of a manuscript to a definitely selected group and for a limited purpose, and without the right of diffusion, reproduction, distribution or sale” (i.e., not publication under copyright law) than it is to common notions of redistribution or publication. Therefore, there is a strong argument that such a transfer is not distribution under the law.

The International View

It is important to keep in mind that the distribution question as it is analyzed here is largely unique to US law. Because GPL 2 does not have a choice-of-law provision and is a conditional copyright license, it governs only what is protected via local copyright law. A full discussion of the tenets of international copyright law bearing upon this issue is beyond the scope of this chapter, but it seems likely that the question would have different answers outside the United States. The Berne Convention for the Protection of Literary and Artistic Works, as amplified by the WIPO Copyright Treaty, provides for a right to “make avail-
able” a literary work. This may be broader than the US notion of distribution, and most importantly, it could include SAAS offerings. Therefore, the triggers for copyleft obligations based on activity outside the United States may have a lower threshold than those based on activity in the United States.

**Best Practices for Contract Drafting and Deal Structuring**

As lawyers in private practice await clarity in the common law on distribution issues, they may wish to consider implementing certain drafting and structuring practices to clarify their clients’ intent or to minimize the uncertainty of the results should the courts later announce decisions on distribution questions. Such practices cannot address all distribution issues should there be a contrary court pronouncement, but they might help discourage claims, provide evidence of intent, or reduce confusion when those not directly involved in the deal are later asked to assess distribution issues.

**Development Agreements**

To avoid confusion about whether development activities constitute distribution, consider adding language such as the following to your development agreements:

- “Contractor shall conduct development services only on systems and equipment under the control of Customer.” This language limits work to customer-controlled servers. This will address whether a distribution has occurred, the theory being that even though the contractor is a separate person, no copy of the software has been transferred.
- “Contractor acknowledges that it is performing the development services solely for the benefit of Customer, and solely as directed by Customer, and shall not make any copy of the Software available to any other person or entity.” This language states that copies are intended to be private, thus addressing the situation that the FSF FAQ says constitutes distribution.
These approaches are attractive because they comport with customary confidentiality provisions and “work made for hire” provisions in development agreements, which often recite customer control of the development activities to support treatment of the work as “work made for hire” under *CCNV v. Reid.*

**Mergers and Acquisitions**

- Avoid delivery of GPL software. Particularly in asset purchase deals, determine whether there is a reasonable way to refrain from delivery of open source packages in favor of having the buyer download them directly from the original source or a third-party source. This approach is useful mostly in situations in which drivers or other significant original code belonging to the seller is being delivered. It is not useful when the seller is delivering integrated modifications. In that case, the seller would deliver only its additions, and the buyer would receive third-party open source code separately. Clearly, if third-party open source code is extensively modified, this strategy may not be feasible because it would be so difficult to separate the seller’s code from the third party’s code. However, companies that are very conservative on this issue may deliver only diffs, or patches, in an attempt to avoid delivery of any third-party GPL code. Keep in mind that distribution is usually an issue for the seller, not the buyer. Therefore, asset purchases that consist of all the assets of the seller entity may render the concern moot, but a seller’s divestiture of partial assets, business lines, or product lines may cause the seller to have concerns about GPL distribution. A seller wishing to sell its own code may find buyers unwilling to pay for that code if the code must be delivered under GPL.

**SAAS Agreements**

- Avoid drafting that confuses SAAS with distribution. There is some controversy among technology lawyers as to whether SAAS agreements are licenses or merely service agreements. Sometimes, as an artifact of their

---

20 *Community for Creative Non-Violence v. Reid*, 490 U.S. 730 (1989), held that the factors for determining whether a work of authorship is a work made for hire (owned by the company) or not (owned not by the company but by the author) are, among others, the level of skill required to create the work, the source of the tools used in creating the work, where the work was created, the duration of the relationship between customer and author, the extent of the contractor’s discretion over when and how long to work, and whether the work is part of the regular business of the customer or consultant. Therefore, many consulting agreements recite where work will be performed, as well as other facts that might bear on whether distribution has occurred.
business antecedents in distributed software, SAAS agreements are drafted so much like distributed software licenses that it is difficult to tell the two apart. Although the distribution question would likely turn primarily on the supplier’s actions, not merely on document drafting, it is best not to hurt your position by using a SAAS agreement that reads like it covers a distributed product.

**Intercompany Agreements**

- Recite intent not to distribute. In software agreements between corporate affiliates, parent entities may wish to clarify that no distribution is intended, much in the same way as recommended above for consulting or development agreements. This may seem obvious, but in fact, intercompany technology licenses are often not drafted by technology lawyers. Instead, they are drafted by tax lawyers or corporate lawyers who are documenting intercompany arrangements for the purpose of managing imputed tax issues, rather than precisely considering intellectual property issues. It is crucial to review these agreements with a view to open source as well as intellectual property issues.

**An Enduring Puzzle**

It is unlikely that the federal courts in the United States will answer these distribution questions anytime soon. The open source enforcement actions that have been brought to date have not resolved these questions. Given that other heady issues (such as the scope of derivative works under GPL 2 and the interaction of patent law and open source licensing) are still unclear in open source law, they may not be ripe for dispute. Also, most authors who release code under GPL 2 are simply not focused on issues like intercompany agreements and mergers or acquisitions. This is because they are primarily technologists rather than corporate strategists. If GPL authors generally do not intend to enforce their rights in these edge cases, there may not be a constituency that is interested in bringing a lawsuit that will make law in this area. It therefore seems likely these questions will persist as long as GPL 2 remains a widely used license, and based on the prevalence of the Linux kernel alone, this will be a long time. Companies assessing open source compliance should be sure they have identified the types of distribution that are most likely to be questioned so they can use open source software with confidence and plan their transactions in a way that comports with their open source compliance strategy.
Today, it is considered a best practice for a company to have a written open source policy. In some areas of law (such as employment law), the fact of having a written policy has a direct bearing on liability, but for open source, the policy is entirely functional. Copyright infringement is largely a *strict liability* regime—meaning that intent is not an element of infringement.\(^1\) Therefore, a company will not be able to avoid liability for the infringing acts of its employees merely because it has a written policy. A written policy that everyone disregards is worthless and, in fact, can be counterproductive because it sends a signal that the company will look the other way when violations occur.

Written policies need not be long or complicated. But having them in writing is useful, particularly when a company has multiple development teams who may be in different countries and may speak different languages. Having a written policy gives these teams the time and opportunity to read and understand the policy, ask questions, and refer to the policy when necessary.

However, there is no one-size-fits-all policy. Here are some things to consider if you are contemplating an open source policy for your business.

**Start Small**

Your company may not need all the topics in the model policy at the outset; the policy is drafted to allow you to remove the “extras” easily. The most important elements of the policy are the compliance elements, which make up most of the policy. Topics like contributions, code releases, and transactional terms can be added when the company is ready for them; before that time, these elements are usually handled ad hoc.

---

\(^1\) Willful infringement can lead to a higher statutory damages award, but that is a relatively minor enhancement compared to what occurs in other areas of law.
Business Processes

The corollary to the policy is the process that attends it. The policy only describes certain checks and processes; the business then has to implement them. For example, if using GPL code in a product requires the approval of an engineering manager or the legal department, the company may want to implement an automated way to generate that request. Also, every company needs to consider how it will capture and store the information about the open source software it is using. Using spreadsheets is a fairly bad way to do this, and any method is only useful if it is easy to update and if updating it is incorporated into the development and release cycle. A company should also consider when in the development cycle the open source “seal of approval” needs to be applied. The closer to release it happens, the more likely that any remediation or substitution of code to comply with open source licenses will delay release or simply be abandoned in favor of meeting the release date.

Staffing

The title of the person designated to approve requests to use open source software in the business will differ from company to company. Some companies want to conserve the resources of their legal department and delegate some decisions to engineering management; some take the opposite approach and delegate the question to legal; some have a committee to deal with open source matters (usually composed of representatives from legal, engineering, and management areas); some hire a specialist paralegal or lawyer to handle open source matters. Most open source compliance matters can be handled by someone with minimal, but solid, engineering and legal training. As the volume of approvals at a company goes up, decisions need to be pushed down to an operational level so senior management is not tasked with making routine or recurring decisions. Recurring requests to use the same open source software are frequent because code that works well in one company product may very well work well in all of them.

License-Based Review

The model policy focuses on review of software based on the license that covers it, and this is the way most companies review their potential use of open source software. However, there are good reasons to take a more nuanced approach. Some companies review and approve the use of open source software package by package; this is most common when the company has heightened security concerns or exacting product qualification requirements from their customers.
Some companies create a “sandbox” from which all open source software used in the company must be drawn, and they forbid downloading directly from the Internet. Some companies review open source software for patent infringement or other legal matters (such as export restrictions) as well. Accordingly, the model policy takes a lightweight approach to review, based only on the license.

**Use Cases**

A policy for an SAAS company may not fit a consumer electronics company, and vice versa. They are at opposite ends of the spectrum of open source risk. Depending on the company’s appetite for risk, it may require much less review of open source risks than do other companies. However, SAAS companies should keep in mind that basing an open source compliance policy on the absence of distribution can lead to terrible results. Most SAAS companies eventually distribute their products—whether to customers who want a private instance of the software to manage regulatory or security issues, to corporate partners or affiliates, or to successors in interest. So don’t start what you can’t finish—interleaving GPL code with proprietary code in the same program, particularly at a granular level, will likely lead to problems someday. Also, companies that assume they are immune to open source risk will be tempted to ignore record keeping. Taken together, these practices can mean the software can never be distributed. Then, when the company decides that distribution is its next business initiative, no one will want to deliver the news that it can’t be done without a massive reengineering and audit effort.
While most audits are conducted at the time of an investment, corporate sale, or other such transaction, other audits are conducted in connection with customer sales or simply as a process of establishing responsible internal business controls that manage intellectual property hygiene. Today, many customers who are buying licenses for software insist on a full disclosure of open source components. In fact, if the product is to be distributed to the customer, the vendor has an obligation to provide this information to the customer—in the form of the license notices required by the applicable open source licenses.

Open source compliance can be easy to forget and can suddenly become a major concern. It is best to be ready for this challenge before you need to make guarantees that your company is compliant.

**The Challenges of Open Source Compliance**

Open source compliance is not especially difficult—particularly compared to compliance requirements for proprietary licenses, which might require constant tracking of the software’s users, servers, or use cases. In fact, on a conceptual level, open source compliance is easy in most cases. Only a small number of use cases raise the potentially complex legal issues discussed in Chapter 6: What Is Distribution? and Chapter 8: The GPL 2 Border Dispute. But open source compliance does involve some information management challenges, and when people say open source compliance is difficult, they are usually referring to this issue.

The information management challenge arises because open source software tends to circumvent normal business processes. In contrast, if you must license software from a proprietary vendor, then you must first pay a license fee. Most businesses have internal controls that capture the payment of fees: if you must write a check to a licensor, you must sign a license agreement, and the license agreement must undergo legal review, which causes a lawyer or contract negotiator to consider whether the uses contemplated by the company will be compliant and
whether the fees to be paid are reasonable in light of the licensing terms. However, open source is always free of charge and can usually be downloaded freely from the Internet without signing any agreement or paying any fee. This means that for most organizations, there are no internal controls that capture the initial use of the software and, therefore, there is no advance consideration of whether the company can comply with the licenses. Open source compliance is left as a “cleanup” matter for a later time.

As a consequence, many companies wake up one day to discover that they do not know what open source software they are using or whether they are compliant with open source licenses. When this happens, companies may initiate an audit. Alternatively, companies are often forced to initiate an audit when a potential buyer or customer demands it.

**Snapshots, Surveys, and Title Searches**

There are two kinds of audits—the snapshot and the ongoing business review. If you have been asked to undertake an audit to support a transaction like an investment or acquisition, you are probably taking a snapshot. The snapshot identifies the open source software in your code base at a particular moment in time; for an acquisition, that would be the moment of closing the transaction. However, companies that are more sophisticated about open source compliance want to make sure that they are always compliant—not just when someone else demands it. Therefore, they conduct diligence on an ongoing basis as code is added or changed in the code base of their products.

An open source audit is like any other audit, in the sense that one is looking for problems but one can never be sure that all problems have been found. The art of auditing involves engaging in efforts that are financially and technically practical to eliminate the most significant problems. The proper level of effort depends on how risky you think a mistake will be, and that in turn depends on the use case for the software you are auditing and your assessment of the existing internal controls used to manage open source licensing compliance.

There is no one right way to conduct an audit. Lawyers are often asked to make a decision about whether to hire a code-scanning consultant to examine the code. It is never wrong to do this. However, hiring a consultant is like buying insurance: it may be useful, but it may be too expensive. It’s possible to spend all the money you like on managing risk, but it only makes sense to spend money on activities that actually reduce risk.

Economically speaking, the equation is this:

\[
AC < R \times L,
\]
where AC = Audit Cost, R = Risk of a problem, and L = Loss that would occur if the problem occurred.

Thus, a problem with a small likely loss is not worth spending a great deal of money to find. Risk and loss depend on use case and your assessment of the company’s internal controls. If a company has no internal controls on open source software use, R will be higher. If the software is distributed in a consumer electronics product, both R and L will be higher than they would be for an SAAS product.

It is not difficult to tell whether a company has internal controls for open source compliance processes in place—all you have to do is ask. For instance, if you ask for a list of open source code that is in a product, and if the company doesn’t have such a list (or doesn’t understand the question), then the company likely has no compliance process in place. In such a case, hiring a code scanner is a great idea. However, if the company provides a list of open source code and licenses that looks reasonably professional, you may decide that hiring a code scanner is unlikely to yield additional information that is material to risk.

There are two overarching approaches to automated auditing: forensic matching and string searching. Companies like Black Duck Software, Palamida, nexB, and OpenLogic perform services known as forensic matching. In other words, they examine the source code for a particular code base and match it against known open source code. They identify the known open source code by its tools. The other approach is to run a string-matching program, which programmers often call a GREP. This kind of program compares strings (which in programming language means text characters) in the source code against regular expressions—meaning target strings, sometimes with wild cards—to find indicia of licensing terms such as copyright notices and licensing statements. Using GREPS is a bit like typing a query into a search engine. So for instance, if you searched the code base for “copyright,” “Copr.,” or “license,” you would find copyright notices, licensing notices, and probably a lot of extraneous items as well. Programs like FOSSology, an open source utility for compliance, use this basic approach.

Alternatively, you may be asked to conduct an audit based on the external records kept by the company. Most often, self-disclosures are in the form of spreadsheets or text lists, and they list software and licenses. The difference between these two approaches is like the difference between a land survey and a title search. Forensic matching is like a survey—it looks at what is actually there and tries to map it onto known information. String matching or self-reporting is like a title search—it looks at what people have recorded about the licensing of the code and assumes that the information is reliable.

---

1 GREP, the name of an old UNIX routine that does string searching, stands for “globally search a regular expression and print.”
In truth, neither of these approaches is foolproof, nor is either without its challenges. Forensic matching is less prone to false negatives—it can find open source for which the copyright and licensing notices have been removed from the software being audited. This removal of licensing notices is considered poor programming practice, but it happens. However, forensic matching is prone to false positives in that it finds potential problems that are not actual problems. On the other hand, a GREP approach will not identify code for which licensing information has been removed or not properly preserved. Therefore, the GREP approach is very useful at identifying entire packages, files, or libraries of open source code, but it may not be successful in identifying fragments or snippets of code.

In an auditing effort, false negatives are more dangerous than false positives. Therefore, proper auditing techniques should tend toward zero false negatives and minimal false positives. To understand better how this works, consider the following seeming paradox: Most people who test positive for a serious disease probably don’t have it. Does this mean the test is wrong? No, it means the test is properly designed to avoid false negatives. If the test is positive, more accurate tests will be done, and these tests are intended to weed out the false positives. The first level of testing is performed on a much larger population than subsequent tests, so it produces many more false positives than the true positives found in later testing. Any kind of audit of testing works in this way.

But as a result, reports that are generated by auditing efforts can be maddeningly difficult to review. They tend to include a lot of false positives, or “noise.” Every code base will have small fragments of code that may be taken from elsewhere, but not all such fragments constitute infringement. For very common code lines, it may be difficult to tell the original source. Also, the copyright law will not protect what it calls de minimis use of copyrighted material.

The upshot of all this is that audit reports give you information, not answers.

**Setting the Rules**

Once you perform such an audit, you must determine whether the information you have found meets the criteria that you have set for compliance. For many companies, these criteria are embodied in an open source software policy. (For more on open source policies, see Chapter 11: Open Source Policies.) Different companies have different levels of tolerance for risk, and different use cases have different risk profiles. However, one thing is certain: you cannot tell whether an audit has passed your criteria if you don’t have criteria to apply.

Today, most companies conducting audits consider permissive licenses to be of little concern. Of course, distributing code that includes open source software licensed under permissive licenses requires the delivery of a notice, so some basic
compliance is always necessary. However, delivering notices is almost always possible, even if administratively burdensome. Mostly, in audits a company is looking for copyleft software—particularly copyleft software under licenses like GPL and LGPL—because it is concerned that the audited software may have been engineered in a way that causes compliance to be impossible, even if all of the information is known and the license notices are applied. For example, if a proprietary application uses a GPL library, it may be impossible to comply simultaneously with both licenses.

The Perils of Self-Disclosures

Self-disclosures are often skeletal, inaccurate, and misleading. They generally contain correct information about the open source code that is included—at least at a package level. A list of open source components can usually be generated by the build instructions for the software. This package-level information is reasonably reliable because the compiler must be given this information in order to build the product. But this information does not include any license information. In a typical open source self-disclosure, license information is prepared manually. However, it is often very inaccurate due to any or all of the following issues:

- Lack of license information
- No versions for licenses
- Conflicting license information
- Lists software that is not open source

Here is a hypothetical self-disclosure:

Linux...GPL
Jboss...LGPL
GCC...GPL
XYZ...GPL/MIT
Java ...GPL
Adobe...public domain

The problems with this self-disclosure are that there are no license version numbers, one of the items is clearly inaccurate (Adobe is not a specific piece of software and is likely neither open source nor public domain), one item references a dual license without explanation (which usually, but not always, means the licensor has a choice), one item (GCC) is a development tool that is unlikely to be in a product, and Java is generally under GPL+ exception. Correcting self-disclosures
is a long-standing pastime in auditing. Those who do audits for a living see all manner of weird self-disclosure. One of my personal favorites was “GNU BSD.” Therefore, if you are conducting an audit based on a self-disclosure, you should not rely on the licensing information you have been given, unless you trust that the source of the information knows how to locate and vet the information.

This means that those conducting audits spend a lot of time researching licensing terms, starting from a list of packages. Researching licensing terms can be tricky. For instance, if you have been told that code base includes a piece of software called FOOBAR, your first step would be to search for FOOBAR in a search engine. If you’re lucky, you will find a FOOBAR project page that indicates the license terms. At this stage, several things can go wrong: there may be more than one project called FOOBAR, there may be no project called FOOBAR, or the licensing information for FOOBAR may not be clearly indicated on the project web page. Moreover, if you take the trouble to download the FOOBAR source code, you may find that the licensing notices in the project are not the ones that are indicated on the project web page.

Therefore, researching licensing terms is more of an art than a science. Projects that are competently run will clearly indicate licensing terms on the web page, and the licensing terms will match the license notices that are actually in the code when you download it. Projects that are not competently run may have no license terms or inconsistent license terms. The cloud development platform GITHUB is especially known for projects with no licensing terms. Unfortunately, if no licensing terms are applied, the default is that no rights are granted to use the software. In such cases, there is no way to be compliant.

If you are presented with conflicting licensing terms, such as one license identified on the web page for a project and another in the source code COPYING file, you should make a reasoned judgment as to which set of terms is right. If a project seems not to have taken proper care with upstream rights, you may need to try to determine where the code came from to determine which licenses must apply. Generally, the license that is actually in the source code will be the more reliable indicator. But there is no magic to this inquiry. Assuming the licensor has made his own due diligence mistakes, you can rely on any license that the author has applied to the software. Placing a license notice on the software is usually enough to indicate that the author has intended to apply those licensing terms.
Versioning

Occasionally, the license terms that are provided to you in an audit process may be inaccurate because the project has changed its license terms. In other words, the license in the software notices for the code you are auditing may be correct, but it may not match the license terms in the currently available version of the software. One way to avoid this problem is to ask for version numbers in the disclosure to be audited. License changes almost always coincide with the release of a major update, so it is usually possible to check the licensing from publicly available sources if you have the software version number. It is most common for a project to change to more permissive licensing terms rather than less permissive licensing terms, so this phenomenon does not usually cause audit problems. In fact, if the license that applies to the version of the software in the audited code base is too restrictive, it is possible that moving to a later release will solve the problem.

Solving Problems

If you identify a problem in an audit, you should always think about a solution. (This comment is mostly for the benefit of lawyers. Engineers always think about solutions; lawyers sometimes seem to think their job is to find problems and stop there.) Almost every audit problem has either an engineering solution or a licensing solution, or both. Always consider all of these possibilities:

- **Remove.** In any code base, quite a bit of code goes unused. There are various explanations, but the most common is that the code was used in testing but not in the final product. The actual binary of a software product need not contain all the code in the source code repository from which the product is built. Therefore, if you find a licensing problem, your first questions should be “Is this code really in the product? If so, can we remove it?”

- **Replace.** Open source packages are often created as alternatives to popular proprietary software, or vice versa. Therefore, if the open source terms are a problem, you may be able to find a proprietary alternative that you can substitute for the open source package with minimal engineering effort. Often, proprietary substitutes are not expensive—after all, there is a substitute good that is free of charge.

- **Reengineer.** This is the option everyone wants to avoid because it is expensive and time-consuming. Of course, it is rarely necessary unless the issue involves GPL or LGPL, because these are the licenses whose conditions rely on the means of integration of software.

- **Relicense.** If the open source software is provided under license terms that you cannot comply with for the use case you are auditing, you may ask the
author if he or she is willing to grant an alternative license. Clearly, this approach will not work with most major projects, such as the Linux kernel or Apache web server, which have set licensing terms based on the project’s philosophy. Relicensing works best for individual authors. Keep in mind that if a project has more than one author and you seek an alternative license, you may have to locate and make an agreement with all the authors.

**Audits and Mergers & Acquisitions**

Anyone who has ever been involved in a mergers and acquisitions (M&A) transaction knows that open source audits can be frustrating to accomplish within the confines of such a transaction. Despite the fact that it is more popular than ever to conduct code scans for M&A deals, most due diligence in M&A is still based on self-disclosure. Unfortunately, these disclosures tend to come late in the deal process and be extremely inaccurate, so they tend to create issues too late to do much about them. If you are running a startup business, you can effectively streamline investment transactions and corporate sales by engaging in at least basic open source compliance and keeping records of the open source software you are using. Preauditing your own products can save you a lot of time and trouble and make your company look more professional in the due diligence process. (For more on this, see Chapter 17: Mergers & Acquisitions and Other Transactions.)