

MARCH 2020

DEVOTED TO
LEADERS IN THE
INTELLECTUAL
PROPERTY AND
ENTERTAINMENT
COMMUNITY

VOLUME 40 NUMBER 3

THE *Licensing*
Journal®

Edited by Gregory J. Battersby and Charles W. Grimes

With All the New Technologies Out There, Does Your IP Due Diligence Need an Upgrade?

Tyler Maddry and Kevin Georgerian

Tyler Maddry is a partner and co-head of the Intellectual Property Practice Group at Hunton Andrews Kurth LLP. Tyler focuses his practice on structuring, drafting and negotiating complex intellectual property and technology contracts. He also has extensive experience in negotiating IP and technology provisions in M&A transactions, conducting IP and IT due diligence investigations, and advising on open source software compliance.

Kevin Georgerian is a partner in the Mergers and Acquisitions Practice Group at Hunton Andrews Kurth LLP. Kevin's frequently advises clients with respect to acquiring and selling companies or businesses with important intellectual property and technology components. Kevin's experience includes numerous "carve-out" transactions involving complex post-closing licensing arrangements designed to allow sharing of core intellectual property and technology components among separated business units.

Intellectual property (IP) aspects of corporate transactions continue to become more interesting as companies increasingly rely on new technologies to run their businesses. In many cases, software, proprietary information, and data represent a significant component of a target company's value. Compared to traditional registered IP such as patents and trademark registrations, it can be more challenging to identify and track the development and ownership of software, data, trade secrets, and other unregistered IP assets. The issues become even more interesting when new technologies such as artificial intelligence and machine learning and the use of open source software are factored in. This article will provide recommendations on how to identify these types of assets and how to handle the resulting legal issues that arise in mergers, acquisitions, joint ventures and other corporate transactions.¹

A. Due Diligence

Some level of IP and technology due diligence is a component in virtually every merger, acquisition, joint venture, or other corporate transaction. From the perspective of a company conducting the investigation, for example, an acquiring company, IP and technology due diligence generally covers three lines of inquiry: (1) identifying and evaluating the IP and technology assets of a target company; (2) analyzing contracts that grant IP and technology licenses or related services to or from a target company; and (3) analyzing whether a target company's operations risk infringing third-party IP rights. Each of these inquiries is being impacted by the prevalence of new technologies.

1. IP and Technology Assets

a. Proprietary Software

One of the more challenging tasks in conducting IP and technology due diligence is to identify the proprietary software and related data assets developed by or for a target company. While third-party commercial software licensed to a target is generally easy to catalog, customized software, technical information, and trade secrets are often not labeled or documented with any consistency. Thus, a simple request by an acquiring company for a list of these material assets held by a target company typically results in little or no response.

So what is the solution? A recommended approach is to find and interview the key person at the target company who has lived through the technology development. He or she may be a senior member of the information technology (IT) or engineering staff with institutional knowledge of the development history of the target company's proprietary software, algorithms, machine learning models, customer-facing services, mobile apps, and proprietary databases. They will also know the other team members who contributed to developing these assets.

Essential questions to ask include: when did the software development begin, what code was used as the starting point, who were the contributors, were third-party contractors retained, are the developers still employees of the target company, and are there agreements in place with developer employees and contractors assigning IP to the target company. With surprising frequency, a target company will not have good answers to many of these questions. This is especially common with early stage companies where the founders and employees are understandably more focused on building a product than seeking legal advice.

In some instances, problems with ownership of the code or use of third-party code can be corrected retroactively. For example, IP assignments can be executed by key employees to assign IP they developed in the past to a target company, or third-party code can be replaced. But other problems, such as the lack of an agreement with a former contractor or employee, may not be easily remedied. The key point is that it is necessary to gather all the facts of the software development in order to identify whether there are any serious problems with a target company's rights in its proprietary software code.

b. Open Source Software

Open source software (OSS) is another matter that can potentially cause significant problems with a target company's IP rights. Some companies understand the rules of using OSS and the need to comply with OSS license terms when developing software products, while others are less well informed. Unaware software engineer employees may download and use source code from various sites like GitHub and SourceForge without paying enough attention to the applicable OSS license obligations. This practice can have serious consequences depending on a few key facts.

The first question to ask is whether the target company has a designated OSS manager and written OSS policies and procedures. The answers to these questions may go a long way towards demonstrating that a target company has OSS compliance under control. If there is no OSS manager and no OSS policies and procedures, then it is probably necessary to look further to see whether and how the target company has used OSS in its business.

The substantive OSS compliance analysis begins with determining which OSS licenses apply. Open source licenses generally fall into two categories, permissive and copyleft. Permissive licenses, such as BSD² and MIT³ generally have only a few obligations that are relatively easy to satisfy. For example, the

MIT license requires the user to reproduce the license in copies of the software, including the copyright notice, permission notice, and disclaimer of liability.⁴ On the other hand, copyleft licenses, such as GPL 2.0⁵ have burdensome obligations such as the obligation to provide source code if the software is distributed in any form.⁶ These types of licenses are sometimes referred to as "viral" because they require distribution of not only the OSS source code, but also any source code (including proprietary code) that is combined with or linked to the OSS code.⁷

Second, if there are copyleft licenses in play, it is critical to know whether the target company is *distributing* any OSS. The term "distribute" is generally interpreted to mean providing a copy of source code or object code to a third party.⁸ In copyleft licenses, distribution generally triggers the obligation to provide copies of the source code.⁹

Third, with copyleft licenses, if OSS has been distributed, it is important to know whether that OSS code has been modified, combined with, or linked to any proprietary source code. If so, the obligation to distribute source code may then apply to the combined work, including any proprietary source code.

The need to dig into the facts of a target company's use of OSS will, of course, depend on the circumstances. If the OSS is governed by permissive licenses and used only internally, the risk will generally be low. However, if a target company is distributing a product that includes OSS governed by a copyleft license, it is then necessary to look carefully at exactly how that OSS has been used, modified, and integrated into the target company's products and services.

The above inquiries are necessary to determine whether a target company may be in the unfortunate situation where its technology is largely embodied in open source software requiring the target company's source code to be distributed, which can significantly diminish its value to an acquiring company.

c. Trade Secrets, Proprietary Information, and Data

There is a natural reluctance for a target company to provide details about its proprietary information and trade secrets. The value of these items to a target company is contingent on their remaining confidential and if not protected in that manner, they are otherwise vulnerable to use by third parties. Often, the response of a target company is "we cannot disclose our trade secrets before the deal closes." Acquiring companies, however, have a legitimate need to know what material proprietary information and trade secrets a target company owns and uses. The appropriate response by an acquiring company is that it is

not asking for the *actual* trade secrets, just a reasonable level of detail identifying the different bodies of *material* trade secrets and proprietary information. An acquiring company will then be in a position, if necessary, to further investigate how they were developed, where they are stored, who owns them, how valuable they are, and who has access to them.

In some situations, it may not be necessary to thoroughly analyze a target company's trade secrets or other proprietary information from a legal perspective, for example, if a target company developed all of its trade secrets internally and has adequately protected them. The integration of new technologies, however, often involves third parties and may introduce complexities arising from third-party ownership of different components of proprietary information and technology that are used together. For example, in the area of machine learning (ML), a target company may use a third-party vendor to provide a trained ML model and may use customer data and other third-party data to train that model, all of which may constitute proprietary information or trade secrets of one of the parties. This type of arrangement can result in distributed ownership of the different proprietary components involved, including the ML model itself, the training data, methods of training the model, and the results generated by the model. While distributed ownership is not necessarily a problem, in situations where these technologies represent significant value, it may be necessary to understand each party's rights, obligations, and transferability with respect to the various components of the proprietary technology and data.

Another situation where it is necessary to analyze the use of proprietary information in more detail arises in carve-out transactions where both an acquiring company and a selling company (*e.g.*, a seller of a business) will need access to the same proprietary information after closing. In this scenario, it is necessary to identify the different components of the proprietary information, where they are stored, the selling company's obligation to provide them, and each party's right to access and use them. If an acquiring company and a selling company are competitive in any way, each party's rights to access and use this information will undoubtedly be scrutinized by the other party.

Finally, given the importance of maintaining and enforcing confidentiality with respect to proprietary information and trade secrets, IP and transaction lawyers should focus on the sale process conducted by a target company. If a target company had engaged in discussions with multiple prospective acquiring companies, and has disclosed some level

of detail regarding its proprietary information and trade secrets with them, an acquiring company and its lawyers should seek to review the confidentiality agreements entered into by the target company and the prospective bidders to make sure that their terms are appropriately protective and that they will transfer with the target company or can otherwise be assigned to the acquiring company.

d. Registered IP

By comparison, the traditional IP due diligence on registered IP assets begins to seem a lot more manageable, at least as far as identifying the assets. For trademarks, the inquiries have not changed considerably and involve searching for trademark applications and registrations worldwide, reviewing use of marks on a target company's website and marketing materials, inquiring into a target's policies and procedures for selecting, clearing, registering, marking and policing its trademarks, identifying opposition and cancellation proceedings, and identifying domain name registrations and social media accounts. Due diligence on copyright registrations involves searching for registrations held by a target company and evaluating what they cover and whether they have been involved in any proceedings or disputes.

The due diligence process for patents also has not changed substantially. It entails searching for patents and patent applications worldwide, verifying ownership by a target company, investigating whether the key inventors are still at the company, determining the number and quality of applications that cover a target's key technologies, and the scope of coverage of a target's issued patents. With respect to patent applications on new technologies such as artificial intelligence and machine learning, it is worth explaining to the business leaders that there is still considerable uncertainty as to whether this type of subject matter is eligible for patent protection.

e. General Considerations

As in any IP and technology due diligence investigation, it is important to start by understanding a target company's business model, including its products, services, customers, and revenue streams. The IP and technology of a target company should always be analyzed in terms of its impact on the business, not in isolation. For example, a target company may offer one service which accounts for the great majority of its revenue and a number of other services which each account for only a small portion. In this situation, it is critical to focus on the IP and technology associated with the service producing the majority of the revenue. The business leaders of an acquiring company

should also be consulted to understand their reasons for acquiring a target company and what they consider to be the key technologies of a target company. This background will guide how to prioritize the IP and technology due diligence inquiries to focus on the most important assets and issues.

2. Agreements

A number of factors in the technology sector elevate the need for well-written IP and technology contracts to be in place in connection with a target company's day-to-day operations. Some of these factors include a highly mobile workforce, reliance on specialized third-party technology vendors, increased integration, use of third-party data sources, and the use of open source software. With the increased reliance on third parties, IT contracts have become an increasingly important asset of a target company's technology infrastructure. In addition to being well drafted, these contracts need to be available after closing, hence transferability is a key inquiry in due diligence.

a. IT Contracts and Transfer Restrictions

IT contracts include software licenses and SaaS licensing and services arrangements. Most operating companies today rely on third-party software and services for significant portions of their day-to-day operations: from Microsoft Office applications, to Enterprise Resource Planning (ERP) systems that integrate management of main business processes and coordinate a company's supply chain, customer relationship management, human resources, financial accounting and virtually all business functions, and sophisticated design and engineering software.

Every category of IP or technology license or contract of a target company merits analysis for transferability in connection with a corporate transaction, however IT contracts deserve special focus because of numerous restrictions often included by licensors that may be impacted by a corporate transaction in addition to well-known assignment and change in control restrictions. For example, IT contracts may contain restrictions regarding: seat counts (*e.g.*, software can only be used on a certain number of computers or servers of the licensee), authorized user counts (*e.g.*, software can only be used by certain employees of the licensee), facility restrictions (*e.g.*, software can only be used in certain facilities of the licensee) and scope of licensee (*e.g.*, a license that is specific to the licensee entity and cannot be used by its affiliates or third-party service providers, including any acquiring company).

In addition, when it comes to licenses involving patents and copyrights, IP and transaction lawyers should be aware that federal law may restrict transferability in connection with corporate transactions in ways that state law traditionally would not. While state corporate and other entity codes typically provide that in the context of a merger, the assets and contracts of a merging entity vest in the survivor "without transfer," federal law in the context of patents and copyrights is more restrictive. In *Cincom Systems, Inc. v. Novelis Corp.*, 2009 WL 3048436 (6th Circ., Sept. 25, 2009), Novelis underwent an internal corporate reorganization pursuant to which no change of control occurred, but one subsidiary (the merged subsidiary) was merged with and into another subsidiary (the surviving subsidiary). Even though the surviving subsidiary continued to use a Cincom Systems license of the merged subsidiary in exactly the same way as the merged subsidiary and despite the fact that state law would have provided that the license was vested in the surviving subsidiary without transfer, the court held that in the context of intellectual property, a license is presumed to be non-assignable and non-transferable in the absence of express provisions to the contrary—even where state law permits the free assignability of a license, absent express authorization. The court held that the merged subsidiary was the only legal entity that could hold the license from Cincom and that if any other legal entity, including the surviving subsidiary, were to hold the license without Cincom's consent, that entity has infringed Cincom's copyright because a transfer has occurred. The *Cincom* holding is not an outlier and IP and corporate lawyers should not assume that a corporate transaction structured to not violate express restrictions in a copyright or patent license will not otherwise constitute an impermissible transfer if challenged under federal law.

b. Employee Agreements

With respect to the ownership of unregistered IP assets such as software, proprietary algorithms, and data, employee agreements are increasingly necessary. There are default legal principles that a target company can point to in order to demonstrate ownership of certain IP developed by its employees, such as the "work made for hire" principle under the Copyright Act.¹⁰ Without a well-drafted employee agreement, a target company, however, is vulnerable to IP ownership challenges by its employees. For example, patent rights are not automatically owned by an employer.¹¹

A best practice is to require new employees to sign an employee agreement on the first day of work. A

target company's employee agreement should contain, among other things, an actual assignment of IP rights, not just an agreement to assign in the future.¹² The employee agreement should cover IP rights that are conceived, developed, created, or reduced to practice during the term of employment, whether in the scope of the employee's employment, or using company resources, or relating to a target company's business. Many companies, particularly early stage companies, do not have an adequate employee agreement. Some even use only a confidentiality agreement with no IP assignment provisions. Since there is no subsequent process for assignment of unregistered IP (*e.g.*, similar to a subsequent assignment document for a specific patent application), the employee agreement is the one document that assigns all of this IP to the employer, including IP developed in the future. Thus, the employee agreement of a target company is an important document to analyze in due diligence, and—of course—it is also necessary to determine whether a target company has retained signed copies from all relevant past and current employees.

For current employees of a target company who have not signed an employee agreement, the situation can be corrected by having them sign an agreement that covers all relevant IP created in the past as well as the future. But with a mobile workforce, there may be situations where contributing employees have already left and are unwilling to cooperate. In either case, it is necessary to understand whether a target company has a clear chain of title to its IP, or whether there are gaps and potential ownership of any IP by its employees.

c. Open Source Software Licenses

Many companies and industries have embraced the use of open source software. It can offer significant benefits including providing software libraries of common functions to expedite development timelines, avoidance of software licensing fees, and enhanced quality that results from a community of interested programmers. Yet, often there is a lag in the level of companies' experience complying with OSS license terms. Not surprisingly, there are many examples where a target company has paid more attention to developing its software than complying with OSS license terms. As described earlier, the first step in analyzing the level of compliance is gathering facts. These facts include, for each OSS module used by a target, the applicable OSS license, whether the OSS is distributed, whether the OSS has been modified, and whether the OSS has been combined with or linked to any proprietary code. If there is extensive use of OSS at a target company, it may be necessary

to request a spreadsheet that includes all of this information. In addition, if a target company has not maintained adequate records of its OSS use, it may be necessary to actually scan its code to identify all OSS modules and corresponding OSS licenses using a service such as BlackDuck or WhiteSource.

The particular OSS licenses that apply to a target company's code base will have a significant impact on its compliance obligations. The manner in which a target company uses OSS will also have a significant impact. Internal use of OSS at a target company generally does not trigger any significant OSS license obligations, even for copyleft licenses. Furthermore, if a target company provides services to third parties using a software as a service (SaaS) business model, most copyleft licenses do not require distribution of source code. The reason is that most copyleft licenses like GPL 2.0 recognize that the SaaS business model does not involve distribution of software. Rather, the software is maintained on a remote server and the user only exchanges data with that server. There is at least one important exception, however. The Affero GPL license recognized this deficiency of GPL 2.0 and was written specifically to require distribution of source code if modified code is used to provide services to third parties in a SaaS model.¹³

If a target company distributes OSS software governed by a copyleft license such as GPL 2.0, the next series of questions is directed at understanding the impact of what other code may be implicated. Taking GPL 2.0 as an example, this license contains obligations that cover modifications to the OSS as well as other code that is combined with or linked to the OSS code. Under GPL 2.0, distribution of modified OSS in any form requires distribution of the modified source code. Distribution of a combined work in any form requires distribution of the source code of the combined work. And even distribution of OSS that is statically or dynamically linked to another work requires distribution of source code for the linked software. Given these burdensome obligations to provide copies of source code of other software, it is easy to see why a thorough analysis of OSS use may be warranted.

Depending on the particular circumstances, there may be ways to remedy a non-compliant OSS situation. For example, some licensors also offer OSS software under a commercial license for a fee without the OSS copyleft obligations and with additional support services. Alternatively, there may be comparable software libraries that can replace the problematic OSS. In any event, because the use of OSS is so common, it is necessary to start the OSS inquiries to see where they lead, and continue the inquiries as far as needed if significant problems are discovered.

d. Software Development Agreements

If a target company has entered into any software development agreements with a vendor, there are a number of terms that need to be analyzed. First and foremost, the agreement should assign ownership of the software deliverables and developed IP to the target company. In addition, if the software deliverables include pre-existing code of the vendor, the agreement needs to include a license to the pre-existing code. The license should be perpetual, irrevocable, and broad enough to enable the target company to use the pre-existing code at least for any use in connection with or related to the deliverables. It should also include the right to grant sublicenses so that the target company can engage third parties whenever necessary to act on its behalf. If a target company needs to further develop the software deliverables or pre-existing code, the agreement should require the vendor to provide source code and any necessary supporting tools and documentation to the target company.

If the software vendor includes OSS in the deliverables, additional scrutiny will be warranted. Presumably, a software vendor using OSS will have an OSS manager and OSS policies and procedures, but it is necessary to inquire and confirm. A software vendor providing OSS to the target company can create as many problems for the target company as the target company can create itself. In fact, a software vendor may create additional problems because the delivery of OSS code to the target company may itself be considered distribution in some circumstances, which triggers burdensome copyleft obligations.

3. Infringement Risk

Usually, the most important inquiry in IP and technology due diligence is uncovering risks that the target company is infringing a third party's IP rights. When working for an acquiring company, the worst case scenario would be having to inform the business leaders after closing that you somehow failed to discover that the target company they just purchased has been involved a contentious IP litigation.

The normal process for evaluating whether a target company has any infringement issues involves analyzing public information as well as confidential information held by a target company. The public information can be obtained by searching public databases such as PACER for federal IP litigation including patent, trademark and copyright infringement and trade secret misappropriation. Public databases such as Westlaw and Lexis can be searched for state lawsuits such as trade secret misappropriation cases under state statutes.

Even if there has been no litigation filed, there are a number of indicators, held in confidence by the target company, that can reveal a risk of infringement or misappropriation of third-party IP. These indicators are uncovered by directly asking a target company, usually in a due diligence questionnaire. One set of questions relates to communications between the target company and any third parties concerning allegations of IP infringement, misappropriation, invalidity, unenforceability, and/or ownership. These inquiries should also request a target company to identify any "offers to license" IP since patent infringement letters are often written this way to avoid creating declaratory judgment jurisdiction.

In addition to this type of communication with third parties, there are other types of internal documents and activities that point to infringement risk. The most noteworthy are formal opinions of non-infringement, invalidity, or unenforceability of third-party IP. If a target company has gone to the trouble and expense of hiring an outside law firm to prepare a formal opinion that a third-party patent is not infringed or is invalid, it generally means that the target company was concerned about infringing the patent. Other types of documents and activities that may indicate infringement risk include invalidity searches and freedom to operate studies.

With software and proprietary information becoming more prevalent, the IP and technology due diligence inquiries need to be broadened in some respects. For instance, many of the ownership and license rights to software and data are defined in IT contracts. In addition, it may be easier to prove a breach of contract claim than a trade secrets misappropriation claim or copyright infringement claim. Consequently, a search for breach of contract litigation may be undertaken to uncover disputes related to the IP and technology being licensed or developed with a third party. Similar inquiries can be prepared for the target company regarding communications with third parties about disputes over IT contracts. For example, software audits by major software vendors are conducted in a confidential manner but can involve many millions of dollars in dispute. Hence the normal inquiries into communications about IP infringement should be broadened to cover breach of IT contracts and similar technology contracts.

Conclusion

Widespread adoption of new technologies has shifted the balance of IP assets and issues that affect most companies from registered IP like patents to

unregistered IP such as software and proprietary information. As software, proprietary information, and other unregistered IP assets provide more value, the IP and technology due diligence inquires in connection with corporate transactions require an update. The new version is a bit more challenging to

implement, but with that challenge comes an opportunity to gain insights into the new technologies being embraced by companies across industries, which is a necessary and interesting element of the new due diligence.

1. The views expressed in this article are those of the authors and do not reflect the views of Hunton Andrews Kurth LLP or its clients.
2. See <https://opensource.org/licenses/BSD-3-Clause>.
3. See <https://opensource.org/licenses/MIT>.
4. *Id.*
5. See <https://opensource.org/licenses/GPL-2.0>.
6. See, e.g., GPL 2.0, Section 3 <https://opensource.org/licenses/GPL-2.0> (“You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: (a) Accompany it with the complete corresponding machine-readable source code...; or (b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code...; or (c) Accompany it with the information you received as to the offer to distribute corresponding source code....”).
7. See, e.g., <https://www.gnu.org/licenses/gpl-faq.html#GPLStaticVsDynamic> (“Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? No. Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, the terms and conditions of the GNU General Public License cover the whole combination.”).
8. See <https://opensource.org/faq#distribution> (“What is “distribution”? What does it mean to “distribute” a program? Is letting people use it on my server the same as distribution? Colloquially, to “distribute” a program means to give someone else a copy of its code — either its source code,

- or its binary (executable) code, or both. Merely allowing people to invoke a program on your server, for example via networked API calls, does not constitute distribution of the program as generally understood.”); *Ximpleware, Inc. v. Versata Software, Inc. et al.*, Order Granting-In-Part Defendants’ Motions to Dismiss, Case No. 5:13-cv-05161-PSG (N.D. Cal. May 16, 2014) (interpreting the term “distribution” under GPL 2.0).
9. See, e.g., GPL 2.0 Sections 2–3.
 10. See 17 U.S.C. §§ 101, 201(b).
 11. See *Board of Trustees of the Leland Stanford Junior University v. Roche Molecular Systems, Inc.*, 131 S. Ct. 2188, 2195 (2011) (“[W]e have recognized that unless there is an agreement to the contrary, an employer does not have rights in an invention ‘which is the original conception of the employee alone.’”).
 12. See *Stanford v. Roche*, 131 S. Ct. 2188 (2011) (Affirming the appeals court decision that distinguished between an agreement to assign and an actual assignment).
 13. See Affero GPL 3.0, Preamble, <https://opensource.org/licenses/AGPL-3.0>, (“...The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public. The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version....”).

Copyright © 2020 CCH Incorporated. All Rights Reserved.
Reprinted from *The Licensing Journal*, March 2020,
Volume 40, Number 3, pages 14–20, with permission from Wolters Kluwer,
New York, NY, 1-800-638-8437, www.WoltersKluwerLR.com



This article presents the views of the authors, which do not necessarily reflect those of Hunton Andrews Kurth LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article. Receipt of this article does not constitute an attorney-client relationship. Prior results do not guarantee a similar outcome. Attorney advertising.
