July 4, 2008

Intellectual Property and Information Technology Due Diligence in Merger and Acquisition Transactions

Martin B. Robins, DePaul University College of Law
INTELLECTUAL PROPERTY AND INFORMATION
TECHNOLOGY DUE DILIGENCE IN MERGERS AND ACQUISITIONS

Martin B. Robins*

* The author may be reached at mrobins@mr-laws.com. The author wishes to acknowledge the most helpful assistance and comments of Gayle Jackson, Esq.

Few decisions have greater consequences for a business than the decision whether to acquire another business. In today’s world, one of the key determinants of a business’ value is the value of its intellectual property (IP) and information technology (IT).

---

1 “Few things a company can do are taken more seriously than a big acquisition. Because that often means betting the farm ….” Gomes, “HP’s IBM Envy Drives Deal”, Wall Street Journal, May 14, 2008, p.B8. In his recent book, Deals from Hell (John Wiley & Sons 2005), University of Virginia Business School Dean Robert Bruner, describes in detail the potentially dire consequences of an acquisition gone awry, including large losses and sometimes, liquidation, for companies such as Penn Central, Revco Drugstores, Quaker Oats/Snapple, Mattel/Learning Company and others, as well as the positive consequences from a deal done well. An example of how poor integration of IT adversely impacts a transaction is found in Enrich, “Pandit of Citigroup Plots a Turnaround but Not a Breakup”, Wall Street Journal, May 10, 2008, p.C1, referring to the failure to integrate sixteen data centers following the 1998 M&A transactions which created Citicorp.

2 “Now, tangible assets make up less than 20 percent of companies’ market value.” Keith Cardoza, managing director, Ocean Tomo Corp., quoted in Van, “Stock index values firms on basis of their patents”, Chicago Tribune April 15, 2006. Microsoft Corporation in its 2006 Annual Report to Shareholders identifies as material risk factors, “We may not be able to protect our intellectual property rights against
However, with relatively rare exceptions, the due diligence (DD) process by which businesses assess whether an acquisition candidate is worthy of their time and money, does not emphasize such matters. Traditional matters such as minute books, suit papers, credit agreements and accounting work papers are emphasized. Even when IP is addressed, the focus is often on procedural matters such as the timeliness of filings and review of suit papers in pending infringement disputes as opposed to the substance of the IP and the process by which it is developed and used. This article is intended to explain why additional substantive attention is warranted as a result of recent changes in the legal piracy, infringement of our patents by third parties, or declining legal protection for intellectual property” and “Third parties may claim we infringe their intellectual property rights.”

3 The term “due diligence” was introduced in the cases construing Sec. 11(b)(3)(A) of the Securities Act of 1933, Cf. Escott v. BarChris, 283 F.Supp. 643 (S.D. NY 1968), to refer to the standard of care required of one deemed an “underwriter” in a securities offering, but has expanded in common use to refer to the fact finding done by one party to a transaction about the other party and the subject matter.

4 “Many companies approach due diligence by dotting the I’s and crossing the t’s [but] [i]nstead I would focus all of my time making sure the strategic value is there.” O’Sullivan, “Time to Buy”, CFO Magazine, June 2008, p.79, quoting David Williams from the Financial Advisory Services practice of Deloitte and Touche. For most companies today, IP and IT are key and perhaps the key, drivers of strategic value.

and technological environments and the diverted focus of many practitioners, and how it can best be provided in actual transactions.

The objective is to provide a conceptual framework to supplement and guide the myriad of mechanical steps which are required in this process, as well as a conceptual framework to guide the development of new steps which will be needed to accommodate the inevitable changes which will occur in the legal and technological environments. Hopefully, this discussion will be helpful not only to the practicing bar, but also to the bench and commentators striving to develop standards of conduct and liability to govern the disputes which will inevitably arise to an increasing extent from IP and IT issues in M&A transactions.

GENERAL CONSIDERATIONS:

Of initial interest is what constitutes IP. The term is universally understood to refer to patents, copyrights, trademarks and trade secrets, all of which may be directly owned as a result of purchase or development or licensed from a third party. With the exception of trade secrets, almost all of the relevant law is federal.

Why conduct due diligence? How do these factors impact IP and IT?

6 An excellent description of the major elements of each type of IP is found in Liang, “Going in-house with intellectual property”, Business Law Today, March/April 1997, p.37. Each type inherently involves an element of exclusivity or monopoly – the right to exclude others from doing something. Such exclusivity is deemed to be in society’s interest by promoting innovation. Sources as varied as the U.S. Constitution, Art. I, Sec. 8, clause 8 and the 2007 U.S. Supreme Court in the KSR case discussed infra, reach this conclusion.
The most basic reason is to determine if it is appropriate to proceed at all with a particular deal. If the process reveals that the other company (the “target”) is not what it was represented to be or is a poor “fit” with the acquirer as a result of business philosophy, cultural or personal incompatibility considerations, the acquirer should simply walk away, if allowed to do so by applicable documentation, such as a letter of intent. Frequently, claimed competitive advantage from the target’s IP turns out to be non-existent or exaggerated, when the underlying IP is closely evaluated. Similarly, a review of IT process, people or physical infrastructure reveals that integration of the companies would be much more difficult or costly than originally contemplated.

Even if the IP/IT review does not dictate “cratering” the deal, they may dictate pricing adjustments in the acquirer’s plan for the deal. If a patent has less time until expiration than originally contemplated or a device or service is likely to prompt legal challenges of some sort, the acquirer must allow for the unfavorable effects when determining what to pay. Less frequently, the process will reveal unanticipated benefits – such as pending registration applications - from the target’s IP portfolio which justify a price even higher than what was contemplated.

Apart from pricing considerations, IP/IT matters may dictate how a deal may or must be structured. Many IP licensing agreements will be breached if the licensee becomes a party to one type of transaction but not to another. Prudent legal and business practice

\[7\] Ziff, The Effect of Corporate Acquisitions on the Target Company’s License Rights, 57 The Business Lawyer 757 (February 2002) The article explains how the distinction between stock sales, asset sales and
dictates close review of license documents before determining the formal structure for a deal.

DD also impacts the mechanics of a deal. All acquisition agreements will spell out in some form the major “property” and contract rights/obligations being acquired such as real estate, inventory (of merchandise for resale, finished goods and raw materials), fixed assets, receivables, employee benefit plans and the like. Customarily, such matters are enumerated in schedules to the definitive agreement – e.g. “Target does not own any real property except as indicated on Schedule 4.1.” Identical treatment should be accorded to IP and IT, both owned and licensed, including pending matters such as registration applications. The due diligence process must be used to help both parties develop and agree upon the information comprising this schedule.8

The information obtained in DD can be quite helpful once the deal is done. It should facilitate and expedite the integration of the two firms by allowing acquiring management

mergers impacting the licensee often determines whether the licensee is in breach of IP licensing agreements which do not expressly enumerate the consequences of acquisitions. Distinctions between exclusive and non-exclusive licenses and patent or copyright licenses on the one hand as opposed to trademark licenses on the other are often relevant. The article frequently refers to a leading case regarding the assignability of patent licenses, PPG Industries, Inc. v. Guardian Industries, Inc., 597 F.2nd 1090 (6th Cir. 1979)

8 As is the case with all definitive agreement schedules, the acquirer must review what is proposed by the target prior to executing the agreement, in order to ensure that its contents are consistent with its observations during the DD process.
to know what it is getting into and how best to use the resources being brought to the party by the target. Good managements will operate on parallel tracks during the acquisition process so that the information they obtain in DD is used for both deal pricing, structuring and documentation as well as integration planning. While all information obtained in DD is likely to be helpful, the IP and IT information is likely to be among the most helpful material which is obtained.

The technical information which is IP typically indicates in detail how a firm runs major elements of its business. For example, a patented process or device that is used by the target means that by definition, it functions in such respect in a different manner than comparable firms. Such information will be invaluable to operating management charged with combining the operations of the two firms. A customer or supplier list protected as a trade secret, provides the same benefits in the pertinent areas and will be invaluable to acquiring management in knowing with whom it will be dealing (and often on what terms). The same can also be said for pending or recently granted applications for patents; such items are likely to indicate the short or medium term agenda for the target and allow the acquirer to “hit the ground running”.

While many traditional elements of DD are fairly straightforward and have not changed a great deal in recent years – e.g. review of contracts, corporate minutes and filings and papers in pending litigation – IP and IT materials are by their very nature quite complicated and normally serve to define the essence of a business’ position in the
marketplace. Changes in the marketplace and legal environment\(^9\) have greatly increased both the complication and opportunity associated with these topics and necessitate a significant time commitment and the involvement of a wide variety of people who are not typically thoughts of as part of a DD “core” team.

Who should participate in the IP/IT DD process?

For the most part, DD is the province of transactional lawyers and accountants, with secondary involvement from subject matter experts (“SME’s”) such as environmental consultants, employee benefits specialists and the like. However, with respect to IP and IT matters, this is not appropriate.

It is necessary to engage SME’s with pertinent technical expertise in the relevant area, be it an electrical engineer to review a patent for items involving transmission of electricity, a physician researcher to review a patent for a drug or a chief information officer to consider a target’s IT environment and its integration with that of the acquirer. Such SME’s should be taking the lead in the substantive review process\(^{10}\) in which the business significance of the various items of IP and the IT infrastructure are absorbed and

\(^9\) E.g. *KSR International Co. v. Teleflex, Inc.* 550 U.S. __, 127 S. Ct. 1727 (2007), which raised the standard for granting or sustaining a patent, and *Metro Goldwyn Mayer Studios Inc. v. Grokster, Ltd.* 545 U.S. 913, 125 S. Ct. 2764 (2005), which explained (and arguably created some of) the elements of a cause of action for secondary copyright infringement with respect to digital media.

\(^{10}\) As opposed to the procedural review process of the filings pertaining to each item of IP when registered and as maintained through required filings with governmental bodies, and infringement claims, where lawyers are likely to play a leading role.
evaluated. For example, an engineer would advise the DD team of whether the subject matter of a patent is likely to work as advertised and whether it is genuinely a breakthrough for commercial purposes or whether it is easy for someone to invent around it.

The types of SME’s who are required will vary greatly depending on the type of IP at issue. Consideration of patents will involve engineers and/or scientists and patent lawyers, while consideration of trademarks will usually be for sales and marketing management, with some input from trademark counsel. Copyright matters will usually require persons with design or literary expertise, although the growing concern with secondary infringements brought about through technological innovations, may cause the involvement of engineers or computer scientists here as well. Trade secret issues will likely remain the province of lawyers, with significant involvement from human resources professionals.

IT matters will require discussion from each side’s IT management with the discussion being framed by lawyers with some familiarity with major issues in this context.

What are we looking for in the DD process?

The IP analysis of the DD team must have a quadruple focus:

- What is the target’s IP worth, now and in the future, in the plant, in the marketplace and in court;

---

11 Grokster, supra
• How well does it insulate the target’s business from legitimate and illegitimate competition; and

• Does the target face a realistic threat of third party claims for infringement of their IP?

• Does the target take proper measures to minimize the likelihood of involvement in disputes concerning alleged infringement of the IP of third parties?

This multifaceted approach reflects the need for both an offensive and defensive analysis of the target’s IP posture. It is little consolation for an acquirer to establish that the target has outstanding technical personnel who have developed a valuable IP portfolio, if such portfolio has not been properly defended from misappropriation (or worse, legitimate appropriation) by competitors. It is of less consolation to discover that a seemingly valuable IP portfolio is the result of misappropriation or infringement of that of others. Even the likelihood of spurious claims of such activity by the target should give pause to the acquirer in view of their potentially drastic consequences.\textsuperscript{12} As is true with all legal claims, one does not want to acquire a lawsuit or the need for same when one does an acquisition. The IP area is particularly susceptible to legal disputes.

In that so much IP is licensed, and so much software used in the IT area is also licensed, DD work must always address not only prevailing legal doctrines in the respective areas – e.g. patent, copyright, trademark and trade secret – but also obligations contained in the

\textsuperscript{12} Injunctions or large settlements/damage awards often result from infringement claims and attorneys’ fee awards are also fairly commonplace. Large legal fees are a certainty.
applicable license documents. In many cases, behavior which is clearly permissible or at worst, arguable under common and statutory law, is the subject of an express contractual provision which either permits or prohibits it. In many cases involving copyrights, the contract at issue is not a traditional one on paper but is a so-called “click wrap” agreement where one clicks a button with their mouse to manifest their agreement. Inquiry must be made as to whether the target customarily agrees in such manner, or even tracks whether anyone does so.

Who is the Licensor? Legal and Operational Implications

For IP which is licensed in to the target, as licensee, it is worth considering the financial stability of the licensor. If the licensor disappears or encounters major problems, this will at the least impact the support provided to the licensee for the IP following the license, which is often referred to as “maintenance”. Until fairly recently, a licensor bankruptcy could also result in a termination of the license by the licensor or its trustee, with devastating consequences for a licensee who needed to continue to use the IP in its business. However, Sec. 365(n) of the Bankruptcy Code now dramatically reduces this risk for all IP except trademarks.\(^\text{13}\) A licensee bankruptcy may also be problematic for the licensor and is not governed by a specific, IP-oriented statute.\(^\text{14}\)

In that M&A transactions as well as macroeconomic turmoil can have a major impact on the viability of licensors and licensees, it is also prudent to address the termination provisions of any major license agreements to which the target is a party to determine if they can be terminated if new players enter the game – i.e. there is a “change of control” of the licensor - or if their circumstances drastically deteriorate.

**Outside the US**

While space considerations dictate that the focus of this article is on US issues, it must be stressed that to an increasing extent, IP matters are the subject of law outside the US. This means that for both an offensive and a defensive analysis, the acquirer of a target with any material non-US operations must get counsel on and consider foreign IP law and practice. Foreign countries are under increasing pressure from their own commercial communities and the international community to bring their IP laws and practice in line with those of the US and are doing so in order to protect their own large companies and avoid World Trade Organization sanctions for winking at infringement of the IP of Western firms.

**SPECIFIC DD TECHNIQUES:**

There are vast differences in the steps to be taken with respect to each of the topics covered in this article, but in all cases, it will be necessary to consider both procedural and substantive matters. That is,

---

14 *E.g., In re Catapult Entertainment, Inc.*, 165 F.3rd 747 (9th Cir. 1999).
• whether the target has “jumped through the right hoops” regarding the notices and filings which are needed with government and private parties to establish and maintain the particular IP rights at issue (including the content of such materials as well as its timeliness) or avoid third party disputes, and

• whether the particular contract and property rights, if properly reserved, are sufficient to provide the acquirer with the anticipated business benefit(s);

• Whether the target is properly respectful of the IP of others.

Patents\textsuperscript{15}

Quite surprisingly given its seemingly arcane nature, this area has become a focal point for many discussions about how best to maintain or enhance the competitiveness of the American economy. Many have argued that the patent system has discouraged innovation and creativity by allowing the granting of many patents for “inventions” which add little to the greater good, but simply serve to enrich their inventors by discouraging legitimate competition which would naturally flow from the existing knowledge base.\textsuperscript{16} The granting of patents for so-called business methods authorized by the Federal Circuit in the \textit{State Street Bank} case in 1998\textsuperscript{17} has been seen by many as particularly problematic.

Apparently in response to these concerns, the U.S. Supreme Court has recently acted to scale back the rights of patent holders and patent applicants, making patents harder to get,

\textsuperscript{15} This analysis is based upon the legislation in effect at this writing. Legislation which would substantially alter the patent environment is pending in Congress, but prospects for its enactment in whole or part are uncertain.


\textsuperscript{17} \textit{State Street Bank v. Signature Financial Group}, 149 F.3\textsuperscript{rd} 1368 (Fed. Cir. 1998)
enforce and maintain in the face of infringement. Most notably the Court in the *KSR v. Teleflex* case\(^\text{18}\), has raised the bar for demonstrating that the subject matter of a patent is not “obvious” to “a person having ordinary skill in the art” within the meaning of the Patent Act\(^\text{19}\). The court approvingly cited the District Court’s view that obviousness is to be judged by reference to the knowledge of someone with a bachelors’ degree in engineering in the relevant field as opposed to merely a reasonable person.\(^\text{20}\) This will clearly make it harder to obtain a patent and, since a defendant in an infringement action, may defend on the basis of the patent’s invalidity, easier to infringe one that is granted.

At this writing, the Federal Circuit is considering whether to flatly overrule its decision in *State Street Bank* and prohibit the granting of business method patents.\(^\text{21}\)

In addition, the Supreme Court has also limited the remedies available to patent-holders by making clear that requests for injunctive relief must be held to the same standard as in

---


\(^{19}\) 35 U.S.C. Sec. 103, in which the basic standard for granting of a patent is an invention which is “new, useful and non-obvious.”

\(^{20}\) “Granting patent protection to advances that would occur in the ordinary course without real innovation retards progress and, may, in the case of patents combining previously known elements, deprive prior inventions of their value or utility.” 550 U.S. at __.

\(^{21}\) The Federal Circuit is considering, en banc, in *In re Bilski*, whether to overturn the holding in *State Street Bank, supra*. *Wall Street Journal* February 20, 2008. U.S. Supreme Court review of the decision in *Bilski* or a comparable case would not be surprising.
any other case, rather than strongly presumed or automatically available for the aggrieved patent-holder.  

All of this means that a target’s patent portfolio and pipeline of patent applications, is likely to be worth less than it would have been several years ago, especially if it is comprised of business method patents to any significant degree. Existing patents are more likely to be invalidated in infringement litigation and applications are less likely to be granted, and those which are will likely offer their holders less effective relief from infringement. Conversely, many pending or threatened actions against a target for patent infringement will now fail and perhaps do so without the need for protracted legal proceedings. Patents and inventions in process must be evaluated in light of these more rigorous standards to determine their genuine viability.

Assuming the validity of a target’s patent portfolio, the acquirer needs to assess its business value by enlisting SME’s with appropriate technical skills and marketplace

22 In *Ebay, Inc. v. Mercexchange, LLC*, 547 U.S. 388; 126 S. Ct. 1837 (2006), the Supreme Court reminds us that a court in a patent case, as in any other case not governed by a contract or statute, must consider whether the plaintiff has suffered an irreparable injury, whether there is adequate relief to be found at law with money damages, the balance of hardships between plaintiff and defendant, does not indicate that the burden of an injunction would be disproportionate, and that the injunction is not contrary to the public interest. 547 U.S. at __.

23 “Patentees have long had the upper hand in patent litigation, but the KSR case has shifted the balance of power back to defendants” according to Prof. Dennis Crouch of the University of Missouri Law School, quoted in Lattman, *Wall Street Journal*, July 31, 2007, “How a Patent Ruling is Changing Court Cases.”
familiarity who can consider how much the patents advance the target or industry’s practical knowledge in terms of allowing the development of a meaningful new product or enhancement to an existing one, or providing for significant efficiencies in the production of an existing one. A major part of this process is review of the “claims” included in each patent application to refer to the specific technical improvements brought about by the patent application, which define the extent of the exclusivity. This process should encompass both granted and pending patent applications.

This is a stage where transactional lawyers can best serve their client by enlisting and coordinating the input of patent attorneys, engineers, scientists, manufacturing management and sales personnel to assess the value of the patent portfolio. The same group can also add real value by engaging their target counterparts in a discussion of the target’s patent compliance approach. The discussion must encompass the patent searches conducted in connection with a proposed new invention or refinement to an existing product where a third party’s patents need to be understood in order to minimize the likelihood of unanticipated involvement in litigation. Of course, if the target believes that it is taking a calculated risk with significant business benefits by infringing the invalid (under *KSR* or prior authority) patent of another, this must be noted. The important thing is to screen out companies who are simply unconcerned about the need to respect the genuine IP of others.

The preceding analysis should be conducted with respect to patents which are directly owned by the target as well as those which are licensed to it. If great reliance is placed on
a licensed patent which turns out to be invalid, adverse business and possibly legal consequences will result. It may be more difficult to obtain access to the required information and people with a licensed patent than with an owned one, but the information is essential where the licensed patent is material to the target’s business.

With all patents which are subject to licenses (in both directions), it is critical to closely review the **infringement indemnification** language which allocate responsibility for dealing with third party infringement claims\(^\text{24}\). Such provisions usually address responsibility for both defense costs – i.e. legal fees – and ultimate settlement or judgment amounts. There are an infinite number of variations of such provisions, dictated by prevailing legal and marketplace circumstances. Key topics where exposure and recourse can drastically differ and which the DD report should address for material items, include:

- Applicability to all patents or merely those existing when the license is signed;
- Applicability to patents issued in all countries or only those issued by specified countries, such as the US;

---

\(^{24}\) Separate indemnification provisions in the definitive acquisition agreement should cover misstatements by the **seller** as to IP and other matters, particularly third party claims arising prior to the closing (and sometime reflect the desired risk allocation for known, disclosed claims). For example, if the target is sued for infringement after the closing but the alleged events occurred prior to the closing, a well drafted agreement would require the seller to take responsibility for such claim. The seller may be able to look to a third party’s indemnity in favor of the target but should be liable in the first instance to the acquirer.
• Requirements for prompt notice of a claim for which an indemnity is sought being a complete defense if not complied with or coming into play only to the extent of actual prejudice for the delayed notice; and

• Right/obligation of the indemnified party to take control of the defense of a claim.

An acquirer should understand the significance of the contingent claims represented by the target’s outstanding indemnification of third parties as well as potential recourse which it may have if it is challenged on account of patents licensed in by the target. If infringement disputes are customary in the space occupied by the patents in question, greater value must be attributed to these “contingent” claims than if such disputes are rare in the specific environment at issue. Of course, the financial strength – i.e. ability to remain in existence and satisfy claims - of any third party who has provided an indemnity to the target is also relevant to the analysis of its value.

Concurrently with the preceding discussion and analysis, counsel should work with its counterpart to address the procedural aspect of the target’s patent portfolio, which may also have major implications for its value and which will have to be translated into a definitive agreement schedule. Matters which need to be disclosed, proved with corroborating documentation such as patent certificates and applications and enumerated in the schedule include:

• Patent (or application) number;

• Patent type (design, process, composition, device or business method);
• Ownership of patent and target practices with respect to requiring formal written assignments of IP rights from employees;\(^{25}\) if these do not exist, the acquirer should be wary of potential claims by employees and contractors on patents of the target, especially where the patents are of fairly recent vintage;

• Major claims in application;

• Status (applied for, granted or subject to a provisional patent)\(^{26}\)

• If application is pending, substantive correspondence from U.S. Patent and Trademark Office (“USPTO”);

• Any legal opinions or other discussions of “prior art”

---

\(^{25}\) While there is legal authority providing for automatic ownership by the employer of IP, particularly copyrights, generated by an employee within the scope of their employment, 17 U.S.C. Sec. 101, the exact parameters of this authority are somewhat murky, with respect to patents (and even copyrights), and it is far simpler and better to rely on express written assignments or appropriately titled patent applications. Additionally, in many cases when a company is started, it relies upon patents obtained by its founder(s), without providing for a formal transfer of ownership. See also, Thompson, “Protecting Your Company’s Assets with Strong and Strategic Invention Disclosure Systems”, ABA Business Law Section e-newsletter, April 2008

\(^{26}\) Under 35 U.S.C. Sec. 112, as explained on the USPTO website at www.uspto.gov/web/offices/pac/provapp.htm, a provisional patent requires little documentation but is only good for one year and serves as something of a “placeholder” for a patentee who is testing the water to see if is prudent to incur the expense associated with a full scale application. If a “traditional” patent is granted, the patentee’s exclusivity relates back to the granting of the provisional patent. During the one year, the applicant can refer to its “patent pending” status.
• Date of application or grant and remaining time left on patent of its original 17 year term; for major patents, this will have great business significance if little time is left, and must be thoroughly discussed with the acquirer’s management;

• Review of related patent applications by the target to ensure that no inconsistent statements have been made to the PTO;\textsuperscript{27}

• Payment of required fees and making of required filings to keep the patent in force.

Appropriate analysis should be conducted with respect to in-process items for which the target contemplates the filing of an application. Such matters should also be included on the definitive agreement disclosure schedule. Such schedule should also enumerate pending developments and applications, for which the target will normally covenant that it will cooperate with the acquirer in connection with patent prosecution.

Pending and threatened infringement claims by and against the target need to be identified, catalogued and evaluated in the same manner as other litigation, but with appropriate substantive input from patent counsel and scientific or engineering personnel.

Licensed patents (going in both directions) call for separate analysis with the emphasis on not only the nature of the patents which are the subject matter, as described above, but also commercial issues such as:

• License duration and extension options;

• Use limitations – e.g. type of product, geographic, number of units, etc.

\textsuperscript{27} Thompson, \textit{supra}
• Royalty amounts and formulae and adjustments;
• Compliance audit or verification mechanism;
• Identity of parties, with emphasis on identification of those who are financially unstable or likely to be untrustworthy in a manner which would spawn litigation or compromise the value of the patent;
• Whether or not exclusive vis a vis both the licensor and the rest of the world or whether the licensor is excepted; and
• Assignment or change of control provisions impacting the proposed transaction.

If the proposed structure conflicts with a material license, then the parties should, depending on the relationship with the other party to the license, either request their consent, or reconsider their structure.

In that many infringement suits arise from failed licensing negotiations (initially or with respect to renewal), the target should include on the disclosure schedule any pending negotiations, with it acting either as licensor or licensee.

---

28 Cf. Cieri, Morgan, at N. __, supra and accompanying text.
29 Ziff, The Effect of Corporate Acquisitions on the Target Company’s License Rights, 57 The Business Lawyer 757 (February 2002) To overgeneralize, non-exclusive patent and copyright licenses which are silent on the matter are usually deemed non-assignable, and thus contravened by asset sales and mergers even without a showing of prejudice, but not contravened per se by stock sales. Trademark license analysis usually involves consideration of actual prejudice to the licensor from the proposed transaction. Express permission or prohibition of M&A transactions contained in licenses are given effect.
Any patent pools – arrangements whereby a group of patent holders allow each member of the group to utilize a specified group of patents developed by such members, with or without payment of a royalty - need to be identified, evaluated and described. A given patent of the target may have less value than anticipated if it is in a pool where other companies can use it as well as the acquirer. Similarly, the target may have rectified a gap in its IP and added to the value of its IP portfolio and company, by becoming a participant in a pool which gives it access to required technology.

In addition to patent pools, any collaborative arrangement whereby the target contracts with other companies with respect to the use of IP, other than a genuinely non-exclusive license involving IP, such as exclusive territorial provisions and joint R&D or grantback agreements to which the target is a party also needs to be specifically identified and evaluated from a trade regulation perspective, in addition to application of traditional trade regulation analysis. Since IP by definition involves a limitation of competition, any collaboration among firms involving the shared access to IP requires significant scrutiny. The U.S. Department of Justice and Federal Trade Commission have promulgated “Guidelines” indicating when they will challenge multi-company arrangements involving IP.\(^\text{30}\) The Guidelines also contain a safe harbor for arrangements involving companies

\(^{30}\) “\textit{Antitrust Guidelines for the Licensing of Intellectual Property,}” Department of Justice, Federal Trade Commission, April 6, 1995. While these Guidelines are important to businesspeople and practitioners when structuring transactions, they are not binding on private plaintiffs, who are free to sue under the antitrust laws if they believe that they have evidence of a violation. These Guidelines also address “tying” arrangements, whereby one wishing to purchase the patented product must also purchase another, non-patented product. In \textit{Illinois Tool Works v. Independent Ink}, 547 U.S. 28, 126 S.Ct. 1281 (2006), the U.S.
with under 20% of the relevant market. If a target is a party to any arrangements within
the scope of the Guidelines, or if the proposed transaction would negate the safe harbor,
consideration should be given to the likelihood and significance of an antitrust challenge.

Where a transaction takes the form of an asset sale or a patent (or group of patents) is
transferred by itself, a filing is required with the PTO.31 This should be addressed both
for the transaction for which DD is being performed and for any other material patents
which were separately acquired by the target, in order to ensure that it has good title to
such patent.

**Trademarks and Servicemarks**

These can appear in a variety of situations. While the most obvious such situation is a
target with branded products, such marks will also appear in franchise agreements to
which the target is a party and may also appear as corporate logos or for “orphaned”
products. Strictly speaking, such marks do not require any governmental filing or
registration, but as a practical matter, they are not likely to have great value without U.S.

---

31 The USPTO no longer (following October 1, 2005) provides a specific form for this purpose, but still

Special consideration, (and verification with the USPTO) should be given to pre-October 2005 assignments
of mission-critical patents. This site indicates that the assignment “should identify the patent by number
and date (the name of the inventor and title of the invention as stated in the patent should also be given)” and
that the assignment should be notarized.
federal registration. Preferably, such registration will be on the “Principal Register” instead of the “Supplemental Register.” The registration certificates will have to be examined as part of the procedural DD.

Before addressing procedural matters, sales and marketing management along with trademark counsel for the acquirer should address the marketplace value of the target’s marks. There is a dichotomy between the legal strength of a mark and its identification with the underlying product or service. The marks which are most defensible in a legal proceeding are those with no apparent connection to the product and which contain fanciful shapes or characters – e.g. “Exxon” or “McDonald’s” Marks which on their face refer to a type of good or service are more likely to be easily and legitimately appropriated by competitors. Ultimately, the issue is whether the acquirer is getting what it expects from the target’s trademark portfolio with respect to both marketplace value – distinguishing the goods from those of competitors - and legal defensibility.

[32] In contrast to the Supplemental Register, the Principal Register provides several procedural benefits for the holder in infringement litigation and renders the mark incontestable in the face of most challenges after five years. Westenberg, What’s in a Name? Establishing and Maintaining Trademark and Service Mark Rights, 42 The Business Lawyer 65 (1986). There is also a fairly new statute providing special protections to “famous” trademarks even without a showing of likelihood of confusion, the 1995 Trademark Dilution Act, 15 U.S.C. 1125© (amended in 2006), but its applicability – i.e. what is “famous”? - and significance can not yet be gauged. This statute should be considered if the target owns or is using any marks which are arguably famous.

[33] Westenberg, supra.
A related topic is whether and how well the target has “policed” its marks against persons who use them on counterfeit products or on competitive products. The owner of a mark has a legal obligation to avoid public confusion by taking action against those who use the mark in a misleading manner. Apart from the legal obligation, it is also good business to avoid “dilution” of one’s mark through its use on someone else’s goods, especially if they are inferior to your own. The basic standard for enjoining the use of a mark is whether it is causing or is likely to cause consumer confusion.

The target’s policing practices need to be evaluated to see if they have put at risk any marks to which the acquirer is assigning significant value. If it appears that the target has largely ignored infringing uses, then the acquirer should attribute little or no value to the mark in question. Policing action can range from simple letters to other users seeking agreement not to use the mark in a manner which causes confusion for the customers of either company to legal action against infringers for damages and preliminary or permanent injunctive relief. Increasingly, legal action against foreign counterfeiters will involve recourse to non-U.S. courts or the World Trade Organization. Even meritorious legal action can cause a backlash against the target in the “court of public opinion”.

---

34 Id at 85. A failure to police will result in the loss of the mark.
35 Id at 68. Marks are registered only for specific products or services. The same consequences can also result if a mark becomes synonymous with an entire category of products. Id. At 83. Where applicable the target’s efforts to avoid this result should be considered – e.g. Xerox running advertisements reminding the public not to use its name as a verb.
Alleged infringers frequently respond with not only traditional legal papers, but also internet-based public relations campaigns seeking to depict the mark’s owner as a bully which is seeking to trample on the “rights” of a tiny company or individual. Whatever the merits of any particular dispute, a company which reflexively responds to alleged infringement with legal filings is likely to offend many potential customers in the marketplace, and may instigate counterclaims, putting at risk its own mark. Such situation may have just as much associated risk as doing nothing to police, and should be noted by the acquirer in their evaluation of the worth of the target’s marks. Of course, the possibilities of using such a campaign to respond to a pending infringement claim brought against a target which is a smaller company should also be considered along with the evaluation of traditional legal defenses.

The target’s use of the mark also needs to be evaluated to better understand its susceptibility to legal attack and whether its marketplace value is being impaired through use in a confusing manner on unrelated or inferior goods. One key indication of the quality of the target’s analysis in this area is whether and to what extent it conducts trademark “searches” with a commercial vendor before pursuing a new mark of its own. Such searches are intended to identify other uses of the proposed mark. If such searches are not done at all or are largely ignored, the underlying marks are probably impaired and the target may be at risk for infringement claims. Copies of recent searches done by the

---

target should be reviewed to get a better idea of competitive activity and the risk associated with the target’s marks.

By the same token, it is useful in the trademark context to have the same type of discussion discussed above with respect to the approach taken by the target with respect to the target’s approach to the patent rights of others. If the target is sensitive to the need to avoid such disputes and does its homework and uses search results appropriately as to avoid potentially problematic activities and ways to mitigate the risk, this should provide comfort to the acquirer. On the other hand, if such matters are “off the radar screen” of target management, the acquirer should anticipate trademark-based legal challenges, disputes or litigation.

Procedurally, the process should encompass the cataloguing of the target’s granted and pending federal registrations with attention paid to the types of products for which the mark is registered and compared to the acquirer’s anticipated use. The target’s practice with respect to payment of required continuation fees and associated calendar entries should also be noted, as should continued use of the mark itself. The same analysis noted above regarding patents for required registration formalities associated with an IP or line of business asset sale is also applicable here. Appropriate use of the ® and ™ symbols should also be addressed.

37 Abandonment is a potential defense to a claim of infringement. That is, if a mark ceases to be used in interstate commerce, it effectively ceases to exist. The same is true of the use of the mark by its owner on inferior goods. Westenberg, supra at 83.
Trademark license documentation in both directions must also be reviewed and compliance and the effect of the proposed acquisition\textsuperscript{38}, assessed. If licensees of the target’s marks are out of compliance regarding their actual use of the mark, as opposed to payment obligations, this may constitute a failure to police which jeopardizes the mark.

As a result of the exception from the scope of Sec. 365(n) of the Bankruptcy Code for trademarks discussed above\textsuperscript{39}, someone with financial expertise should obtain and review the financial statements of a licensor to the target to reduce the likelihood of a licensor bankruptcy disrupting the target’s operations. If the licensor appears to be shaky, either a pricing adjustment or a back-up marketing plan need to be considered.

**Copyrights**

Few areas have seen DD practices impacted by legal and technological change as much as this one. Traditional analysis, which is still necessary, involves review and cataloging of the federal copyright registration forms which are filed for the target’s creative works to see if they are consistent with what has been informally discussed with management and discussing whether anyone on either side is familiar with anyone else who is arguably duplicating such works, whether or not they are the subject of a filing. Such

\textsuperscript{38}“Hershey’s lucrative right to sell KitKat chocolate bars in the U.S. reverts to Nestle SA if ownership of Hershey changes, under a licensing agreement between the companies.” Jargon, Patrick, “More Sweet Deals in the Candy Aisle?”, Wall Street Journal, April 29, 2008, p.B2. This analysis may dictate a different structure or request for licensor consent. \textit{Cf.} Ziff, \textit{supra}.

\textsuperscript{39} Note __ and accompanying test, \textit{supra}.
federal filings are usually quite short. Similar analysis to that discussed above is also appropriate regarding the target’s respect for the creative works of others. Appropriate use of the © symbol should also be addressed.

A related query is whether the target is in compliance with all of its copyright license agreements. Even for non-creative firms, there are likely to be some such agreements for software. Even assuming compliance with statutory obligations, a firm will face liability if it fails to comply with its contractual obligations.\textsuperscript{40}

The new capabilities provided by internet and scanning technology have opened up not only a wide variety of business opportunities involving copyrighted works (including new forms of copyrighted works, such as digital music and video), but also a wide variety of legal exposure. An organization which freely shares (for internal use) by scanning or similar means\textsuperscript{41} the copyrighted reference materials which it pays for and exceeds the usage limits upon which it has agreed, faces copyright infringement suits. An organization which acquiesces to such sharing without proper adjustment of its pricing model by its customers is likely missing out on significant revenue.

In “borderline” cases where material appears to have been shared in good faith, without an attempt to deprive the copyright holder of revenue, a “fair use”\textsuperscript{42} defense may be available to one who is sharing the material. While the literature associated with this

\textsuperscript{40} E.g. Wall Data Inc v. Los Angeles County Sheriff’s Dept., 447 F.3rd. 769 (9th Cir. 2006)
\textsuperscript{41} Including hard drive imaging. \textit{Id.}
\textsuperscript{42} \textit{Id} at __
defense is voluminous and well beyond the scope of this article, the four factors comprising such defense are:

- The purpose and character of the use, especially whether it is for commercial or educational or other non-profit purposes;
- The nature of the work at issue, specifically whether it is "creative";
- The amount of the work at issue which is used by the alleged infringer; and
- The effect of the use on the market for the work.\(^{43}\)

More fundamentally, the rise of digital music and movies has facilitated the creation of many businesses which provide hardware, software and services for such marketplace. It has also prompted Congress to enact the Digital Millennium Copyright Act\(^{44}\) ("DMCA") to provide the beginning of a customized regulatory structure for such marketplace. Many of such offerings are of questionable validity under such statute and "regular" copyright authority. If the target has any operations which involve digital music or movies, the DD process must encompass the implications of the DMCA. Even a company which is itself not even arguably infringing anyone’s copyright but facilitating someone else’s infringement, may face liability for “secondary infringement” of others under the

---

\(^{43}\) 17 U.S.C. Sec. 107

\(^{44}\) In pertinent part, 17 U.S.C. Secs. 512, 1201
Supreme Court’s recent decision in *Universal Studios v. Grokster*\(^{45}\) and the pending case of *Viacom v. YouTube*, discussed *infra*.

For anyone offering a product or service which purports to allow a consumer to avoid the copy protection that many providers of digital content are using, often referred to as “digital rights management”, Section 501 of the DMCA clearly makes them at least civilly liable for such action.\(^{46}\) Any target engaged in such business should be avoided. For companies which produce devices which may be used in this manner, but also have genuine lawful uses, the analysis will be more difficult and reference should be made to relevant legal authorities at the time of inquiry.\(^{47}\)

More challenging is the situation of a target which allows consumers to share electronic files or to post their own content on an internet message board for public access. While

\(^{45}\) 545 U.S. 913 (2005)

\(^{46}\) Section 1201. **circumvention of copyright protection systems**

(a) violations regarding circumvention of technological measures.

(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.

...

(3)(A) As used in this subsection – “to circumvent a technological measure” means to descramble a scrambled work, to decrypt an encrypted work or other wise to avoid, bypass, remove, deactivate or impair a technological measure, without the authority of the copyright owner”

\(^{47}\) *In Sony Corp. of America v. Universal Studios, Inc.*, 464 U.S. 417 (1984), the Supreme Court permitted the production and sale of video recorders which allowed for both legal “time shifting” and prohibited dissemination of copyrighted material, but the language of Section 501 of the DMCA arguably impacts this holding.
there is nothing inherently inappropriate about such services\textsuperscript{48}, there is the potential for misuse, if they are used to disseminate copyrighted content for access by persons who are not paying for it. Many companies provide such forums in order to encourage feedback about their products, in the form of simple textual comments or more elaborate songs or videos describing customers’ experiences with the products.

While there are relatively few companies that provide for consumers to formally share files, those that do have been the subject of numerous legal challenges by the holders of copyrights, many of which have been resolved in favor of the copyright holders. Most notably, in the \textit{Grokster} case, the Supreme Court made clear that any such service must be able to demonstrate that it \textbf{actually} provides substantial non-infringing services in addition to its use by those who are themselves infringing copyrights:

\begin{quote}
We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement is liable for the resulting acts of infringement by third parties.\textsuperscript{49}
\end{quote}

A mere theoretical possibility as to how such service may be used for lawful purposes will not suffice in the face of large scale infringement.\textsuperscript{50}

\\textsuperscript{48} In fact, it has recently been said that “[o]ne of the new rules of doing business online is that you must create a community where visitors to your Web site can add comments and content, not just consume it.” Worthen, \textit{Wall Street Journal Business Technology Blog}, http://blogs.wsj.com/biztech/2008/05/08/, May 8, 2008, commenting on a case where someone posted gyrating images on a site operated by the Epilepsy Foundation, which sickened some visitors to the site and prompted round the clock monitoring.

\textsuperscript{49} 545 U.S. at __

\textsuperscript{50}
A pending case which is likely to amplify the meaning of *Grokster*, the fair use defense and the relevant sections of the DMCA, for companies allowing users to post their own content, some of which will be infringing, is *Viacom v. YouTube*,\(^{51}\) in which the defendant’s business model is encouraging consumers to post their own content for public consumption and selling advertising for viewing on such site. All types of content find their way to the site including perfectly legitimate home videos, and infringing movies, TV shows and music. The owners of the copyrights on the music, TV shows and movies are alleging both direct and secondary infringement by the party operating the site. Even companies which merely invite public comment on their products but allow such comments to include more than simple text\(^{52}\) may face liability or at least legal challenge on such theory, if copyrighted content shows up on its site.

In section 501 of the DMCA, Congress sought to balance the competing interests which come into play in these situations. While the exact meaning of the statute is still not clear, the DD process for any company which allows public posts should at least apply the major elements of this section in order to gauge the likelihood of a significant challenge.

---

\(^{50}\) In that the conduct of the defendants in *Grokster* was so egregious – reflected in (among other things) internal memoranda expressly stating their intention to provoke litigation, 545 U.S. at __, one wonders how much of a legitimate use will have to be shown by defendants who are more discrete.

\(^{51}\) *Civ. Action 07 CV 2103 (SD NY 2007)*

\(^{52}\) Even “pure” text may invite legal claims if it is obscene, defamatory or racist, so the target’s practices regarding screening for these things should be addressed as well as the copyright screening described herein. See N.__, *supra*, for an example of such misuse.
In particular, one allowing public posts, who desires to avail themselves of this provision must:

- Designate an “agent” to receive complaints from copyright holders and advise the Copyright Office of such person’s name and contact information;
- Not receive a direct financial benefit from the infringing activity
- Not modify the content posted by users; and
- “Expeditiously” “take down” as soon as practicable, content which a copyright holder advises is wrongfully posted.\(^53\)

The statute does not expressly provide for any duty of inquiry by the operator of a site as to whether any content which is submitted is infringing anyone else’s rights, but the YouTube case, if it is not settled, is likely to provide some guidance in this regard.

In the meantime, the DD process pertaining to any target which operates a website allowing public posts, should include inquiries as to both the target’s awareness of and compliance with the DMCA. If either appears to be lacking and the target makes no effort to discourage submissions of copyrighted material – e.g. with language on the site – and does not use a common sense approach with postings of seemingly professionally prepared content – e.g. a clip it recognizes from a song, TV show or movie – bewing flagged, there is reason for concern about potential claims following the closing. While there is no formal authority to this effect, it seems logical to anticipate the law developing to require more scrutiny for companies operating sites devoted to sharing of user-

\(^{53}\) DMCA Sec. 512©
generated-content as their business model, than for companies operating sites simply inviting comments on the company’s product.

The acquirer should also be aware of developing technology allowing the digital “fingerprinting” of copyrighted material in order to facilitate its identification and removal from unauthorized display. While this technology is still in its infancy\textsuperscript{54}, anyone soliciting public submissions should be giving thought to the use of such technology at the appropriate time. If the target is not aware of the existence of such technology, this does not bode well for their compliance posture.

Given the radical changes in the environment impacting copyrights which have occurred in the last decade, for any target having relevant operations, it is an essential element of the DD process to ascertain at both a conceptual and a technical level, whether the target has kept up in the appropriate manner.

**Trade Secrets**

Unlike the other types of IP, this area is governed by state law, which makes relevant, and sometimes conclusive, the target company’s internal practices involving sensitive information. In at least 40 states, the governing law is each state’s version of the Uniform Trade Secrets Act and the cases construing it. Thus, questions concerning whether particular material will be protected need to be addressed with reference to the enacted

statute and cases in the jurisdiction(s)\textsuperscript{55} in question. Also unlike other IP, there is nothing filed with any governmental body.

The Uniform Act defines “trade secrets” as

“information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data or list of actual or potential customers or suppliers, that (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.”\textsuperscript{56}

It allows their owner to enjoin their use by another or recover damages for such use. Examples of materials which can qualify for trade secret protection if properly handled include:

- Customer and prospect lists;
- Supplier lists;
- Employee lists;
- Product formulae; and

\textsuperscript{55} Where the target has operations or employees in more than one state, a choice of law analysis must be conducted to determine which state’s law is applicable. Even for the handful of states which have not enacted some form of the Uniform Act, there is still a body of statutory and case law to be considered.

\textsuperscript{56} Illinois version of Uniform Act, IL Rev. Stat. Sec., 1065/2(d) .
• Production process information or manuals\textsuperscript{57}.

What is fundamental to DD analysis and practice in this area, is consideration of whether the target has taken appropriate steps under the law to maintain the secrecy of its sensitive business information which is not otherwise protected by a patent, trademark or copyright. Traditional analysis focuses on physical steps taken to maintain secrecy, such as keeping putative trade secrets in locked file rooms and cabinets and restricting access to such areas to employees and other persons with a “need to know”.\textsuperscript{58} While this is still the correct starting point, in today’s world of cheap, portable electronic storage and communication, it is hardly sufficient.

Electronic access through flash drives, scanners, camera phones, e-mail and the like can be of far greater significance than physical access to paper files. It is essential to understand how the target secures its sensitive materials from misappropriation through such devices. The acquirer must ask: what material is kept in readily accessible computers, what policies exist regarding use of such devices, what “virtual partitions” exist to keep persons with a legitimate reason for access to one electronic file from getting into another for no good reason, and what intrusion detection devices are deployed to deal with problems at an early stage?

\textsuperscript{57} Cf. Minnesota Mining and Manufacturing Company v. Pribyl, 259 F.3\textsuperscript{rd} 587 (7\textsuperscript{th} Cir. 2001). This case stresses that even a compilation of public materials can qualify if it is properly handled.

\textsuperscript{58} Cf., Klitzke Trade Secrets: Important Quasi-Property Rights, 41 The Business Lawyer 555 (February 1986)
For extremely sensitive material which is often used in connection with identity theft and other fraud, such as that containing personally identifiable information of employees or customers or employees of customers – social security numbers, credit card numbers, drivers license information, etc. – is it at all times kept and transmitted in scrambled (encrypted) form? To what extent does the target deal with the public? Who is issued electronic devices which can be misused in this manner? Both formal written policies and their application in practice are relevant. Equally relevant is the target’s actual history. If it has experienced several instances of alleged misappropriation which have led to competitive harm or litigation with former employees, consultants and the like, there is probably something wrong with its practices or policies.

The firm’s dealings with its employees are also critical to this analysis in several respects. First, it is essential that there be in place with all employees having anything to do with IP use or development or other sensitive material, including creation of or access to the types of information indicated above in this section, written non-disclosure agreements, acknowledging that they are working with company property and, during and after their employment, that they will use it only in furtherance of the company’s interest. Such agreements and employment applications should also contain an express representation that the individual is not bringing to their new position and will not utilize in the

59 In “Credit-Card Security Falters”, Perieira, Wall Street Journal, April 29, 2008, the point is made that in a major security breach involving the Hannaford Bros. grocery chain, customer personal data was encrypted at all stages except its initial intake at the point of sale but that it was stolen at such point, with significant financial losses for Hannaford.
performance of their duties, any trade secrets or other IP of anyone else, irrespective of its form.\textsuperscript{60}

Organizations are likely to become entangled in litigation brought by an employee’s former employer against such employee, alleging misappropriation of the former employer’s trade secrets by the new employer in addition to the employee. Such cases typically include allegations that the new employer somehow “induced” the individual to breach their obligations to the previous employer and must be enjoined from benefiting from such breach. It is essential that the new employer be able to demonstrate its good faith in hiring and such a representation is one way to do so. If the target’s practices do not include such actions, the acquirer should plan on prompt change during the integration process. For these purposes, human resources management should be part of the DD team.

It is also useful to assess the target’s practices regarding use of non-disclosure agreements when confidential material is shared with anyone, such as customers, prospects, suppliers. An absence of attention to the need for confidentiality and discretion in such situations is likely to be problematic.

\textbf{INFORMATION TECHNOLOGY}

\textsuperscript{60} That is, paper, electronic or memorized. A recent Ohio Supreme Court case, \textit{Al Minor & Associates, Inc. v. Martin}, (2008-Ohio-292 February 6, 2008) indicates that in some, but not all, states trade secrets can be misappropriated solely through memorization.
It is not intuitively apparent why this topic is addressed along with IP. However, there are two reasons why this is the case. First, in practice, it is often the case, for better or worse, that the same people on the DD team are asked to address both. Secondly, a great deal of the software used for this purpose is procured through copyright or patent licensing agreements of the sort which are discussed above, so that the compliance analysis is equally relevant.

Whatever the conceptual rationale or DD team assignments, this is a critical area of the DD process. A misstep here either with respect to evaluation of system compatibility between target and acquirer for integration purposes or evaluation of target company competence and capability can doom an acquisition with adverse legal and operational consequences in areas such as sales (if there are problems filling orders, tracking inventory or securing customer data in order to prevent fraud and identity theft), manufacturing, billing and financial reporting. Of course, such consequences are likely to be accompanied by major litigation and potential governmental sanctions, not to mention adverse publicity. In addition, a security breach which impacts the integrity of material will also be operationally disruptive. For example, a deletion or corruption of a

---

61 E.g. Waste Management, Inc. v. SAP AG (2008-17510 Harris County TX District Court) a pending case addressing the huge problems encountered by a major corporation from a problematic software implementation, and leading to a demand for damages in excess of $100 million.

62 Such litigation often involves not only class action suits, but also 20 year consent decrees with the Federal Trade Commission, requiring extensive and burdensome third party monitoring. E.g. In the Matter of The TJX Companies, Inc., (FTC File No. 072-3055 March 27, 2008). This data breach has cost TJX in the vicinity of $250 million and litigation is still pending.
customer list, inventory schedule or pending accounts receivable or payable information will wreak havoc even if no third party is impacted.

**Information Security**

As a result of growing concern with individual privacy, this topic has emerged as a strategic priority for lawmakers, commentators, regulators and enlightened corporate managements. Therefore, information security should be the first part of this phase of the DD review. As usual, informal discussion should be had with target management to understand and evaluate its commitment to the topic and ability to follow through on such commitment. At such time, a request should be made for any third party reports or certifications of its practices, with the objective being a so-called “SAS 70” report from a recognized provider such as a major accounting firm. Such report has come to prominence in response to the Sarbanes-Oxley Act of 2002 and is often used as a key part of the financial audit and report on internal controls. If such a report exists (with a recent date and without material qualification) this should go along way toward assuring

---


64 As described at SAS70.com: “A service auditor’s examination performed in accordance with SAS No. 70 is widely recognized … [as] an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes…. [T]he requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.” SAS 70 reports come in two flavors, type I and type II, with the type II report involving additional work by the reviewer.
the acquirer that it is not walking into a hornets’ nest. If it does not and the target is of any significant size or has as its clientele companies which are, especially public companies, there is reason for concern as to what claims or unhappy customers or employees may emerge post-closing, and at the least, the acquirer should plan on promptly spending time and money to bolster the target’s practices and infrastructure.

With or without a SAS 70 report, the DD process should also extend to the specific devices and processes which the target uses to maintain security, with special emphasis placed on security of customer or employee PII\textsuperscript{65}. While any company or individual can be victimized by a hacking incident, the problem is most acute with companies dealing with the general public on a large scale or which have large volumes of employee data. This inquiry should start with evaluation of physical security of facilities and areas where sensitive material is kept\textsuperscript{66} and individual access rules, but extend to more technical matters such as:

- Use of commercial grade, mainstream hardware firewalls and their settings;

\textsuperscript{65} An excellent definition and description of this term (its synonym, “personal information”) is contained in the FTC’s Order involving TJX discussed at Note __, supra and accompanying text.

\textsuperscript{66} Including movement of physical media such as tape cartridges. Several security breaches have involved media literally falling off trucks. \textit{Enterprise Strategy Group White Paper: Tape Loss and Data Theft, Myth and Reality} (January 2006) discussing such issues during 2005 at Bank of America, Citicorp and Marriott Vacation Club.
• Encryption of data in storage and transmission, especially when it resides on laptop computers or involves PII or the target is governed by special obligations associated with health care or financial services such as the Gramm-Leach-Bliley Act 67;
• Purging of data when no longer needed 68;
• Use of mainstream anti-virus software;
• Special handling for wireless transmissions of PII or other sensitive material;
• Requirement for alpha-numeric passwords of at least 6-8 characters and varying cases, for network access, with expirations of no more than 90 days;
• Disaster recovery vehicle with off-site facilities 69;
• Rules and procedures for prompt incident reporting 70;

68 The FTC’s Disposal Rule, 16 CFR Sec. 682.1 et seq (2005), requires “proper disposal of consumer information”. The report of the Canadian Privacy Commissioner on the TJX incident discussed at N. __, infra and accompanying text, takes the company to task for “retaining too much information for too long.”
69 New York Stock Exchange Rule 146, which is applicable at a minimum to NYSE member firms, and possibly to all listed companies.
70 Most states have statutes requiring prompt reporting to the public of any breaches. California’s statute, Civ. Code 1798.80--.84, is the most prominent and probably most significant of these, since it impacts all companies with California operations. A summary of all 38 of these laws is contained at www.csoonline.com/article/221322.
• Rules and procedures for meaningful checking of backgrounds of employees having access to sensitive material, in order to screen out persons with a history of identity theft, virus dissemination or similar disreputable or fraudulent activity;
• Use of commercial grade intrusion detection products; and
• Rules for disabling of employee/contractor system access upon termination.

Special attention must be paid to target websites which allow transactions by the public (e-commerce) and are therefore collecting sensitive information. It is critical that targets operating such sites not only have good security in fact, but also live up to any public statements which they have made concerning their security.\(^7\) Contracts with third parties involving the hosting of such sites need to be reviewed in the same manner as described, with an emphasis on initial and ongoing provision of a SAS 70 report for the relevant hosting facility.

Material deviations from mainstream practices must be discussed with respect to not only integration, but also pricing and whether or not to proceed at all, if the exposure appears to be too great or major claims are already pending or appear probable or the target’s culture places little emphasis on the topic.

\(^7\) In the Matter of DSW, Inc. (File No. 052 3096 2006); In the Matter of BJ’s Wholesale Club FTC (File No. 042 3160 2005)
Where major functions, such as the entire IT function, are outsourced by the target to offshore providers, it is necessary to focus not only on the contents of the relevant contract, but also on the actual steps being taken to comply. Practical difficulties with enforcement of contracts against non-U.S. entities make it essential to understand what is actually being done – how likely is a lawsuit? – as opposed to merely ensuring that there is a contract providing for appropriate action.

A public company acquiring a private one needs to be especially cognizant of this issue as the author has observed that many capable private company managements are (justifiably) not familiar with the special requirements which public companies must satisfy with respect to security under Sarbanes-Oxley and otherwise. Consequently, many well run private companies are nowhere near ready for integration with public companies and will require substantial investment in infrastructure and people and significant retraining to allow the company to function properly in the public arena. It should also be noted that European consumer privacy standards are uniformly more stringent than those of the U.S., so that any M&A transaction which will cause a U.S. company to have a significant European consumer presence will require additional scrutiny of EU standards.

This is an area where it is difficult to distinguish best practices and law. With technology – both protective and malicious – changing so rapidly, it is impossible for any legislative or administrative body to spell out in any meaningful way what technical measures are required. Thus, there is no body of “law” in the traditional sense to use when testing target methods and practices.
However, it is clear from cases such as TJX, that after the fact consideration of responsibility for a problem looks to what technology was available to prevent it when it arose. The nature of a useful DD review will change from time to time to reflect changes in technology and will also focus on whether the target understands the flexible and ever-growing nature of its obligations.

Other IT Issues

A topic which is frequently related to security but involves different considerations is system performance, particularly with respect to web-based applications and public websites used as part of the sales or marketing process. The focus should be on whether the target has the required hardware and software infrastructure to handle its business with reasonable dispatch on a standalone basis as well as when integrated with the acquirer. Web-based products will often slow to a crawl – i.e. take forever to open or move from screen to screen when information is input or the user requests - or “crash”.

72 The Canadian Privacy Commissioner noted that while TJX did encrypt customer PII after its collection, prior to its wireless transmission, it did so using an older standard known as Wired Equivalent Protocol (“WEP”) rather than the more recent standard of Wi-Fi Protected Access, and that the newer approach was not nearly as susceptible to hacking as was WEP. Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner of Alberta, September 25, 2007, http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp, “Report of an Investigation into the Security, Collection and Retention of Personal Information. The Information and Privacy Commissioner for Alberta stated when such report was released, “When the technology exists to protect data, we expect companies to move quickly to adapt that technology.”
completely, if excessive demand is placed upon them and no backup mechanism is available. The acquirer’s IT management must take a close look at the technical nature of the target’s capability – e.g. web server, application server software (is it intended for high demand environments?), storage, information bandwidth in and out, load balancing capability - and practices to see if they are suitable for the intended post-closing use(s). A publicly accessible system which crashes amidst a major promotion will undermine the target’s market position for a long time. Contracts with and infrastructure of third party “hosting” providers for such sites should be reviewed by both lawyers and IT management.

A more procedural, but equally essential, part of the DD review is to assess the target’s general IT approach and capabilities to see if they are in accordance with then-accepted industry practices and are compatible with the acquirer’s approach without a great deal of retrofitting.

Most fundamental, is the question of whether the basic hardware and software relied upon by each organization is reasonably current and will allow the organizations’ computers to talk to each other. If one company relies upon state of the art IBM mainframe or minicomputer (AS400) hardware and the other upon Sun or even older IBM hardware, problems may result. Similarly, if one relies upon a centralized processing model with most data and applications residing on one or a few servers while the other uses a more distributed model or relies heavily upon “software as a service”
with major applications accessed at a third party vendor’s website, integration may be problematic.

Whatever hardware is in use, attention should also be paid to both software operating systems and application programs. If one organization uses IBM “big iron” or AS-400’s with the customary MVS operating system while the other uses UNIX as its main operating system, this may be an issue. Even at the desktop level, the same considerations apply between Apple and Microsoft Windows applications. Within the Windows world, the process must address which versions of operating systems and applications such as Office are in use. If one firm has upgraded to Windows Vista while the other is still using Windows 98 or 2000, work may not flow smoothly or at all from one “side” to the other.

The same analysis is needed for versions of Office and all material applications, including proprietary ones, to ensure that people who will be expected to work together will have the same (or compatible) tools. If one firm intends to install software on the computers of the other, it must ensure that it is technically possible to do so. Philosophies regarding system updates and upgrades need to be compared. Some companies will stick with the tried and true, even if it is ten years old, while others insist upon being early adopters. Version numbers must be compared and differences evaluated.

Additionally, if it is desired to have data flow from the system of one company into the computers of the other without “re-keying” – for example with sales or inventory data
going into a financial accounting system – it must be determined whether the two systems allow for this or whether an “interface” program must and can be developed.

The acquirer’s IT management must be intimately involved in the DD process and “get their hands dirty” at this level of detail in order to determine if a good fit exists on this front. More importantly, any advice to the contrary, must be heeded by the ultimate decision-maker(s).

The acquirer’s lawyers should rejoin the process when it addresses the target’s software license compliance approach and status. All licenses must be catalogued and characterized by type. That is, whether they allow the use of the software at one site, multiple sites, without limit within one firm or multiple firms under common control, by named users, by a specified number of users or on one or more specified computers or are otherwise limited. Once this is done, inquiry must be made as to known compliance/non-compliance and third party vendor challenges as well as mechanisms in place to facilitate compliance. Organizations which rely upon “cute” technical practices to avoid or circumvent contractual limitations on use can expect to encounter costly resistance, which may involve heavy damages, attorneys’ fee awards and even enjoined use.

73 Which are becoming a key element of vendor business models. “Software vendors unveil a new program designed to maximize revenues – their revenues, not their customers….A good portion of the extra income is coming from aggressive policing of current licensing agreements. “ Edwards, Thumbscrew 2.0, CFO Magazine, February 2005.

74 Wall Data, supra. This case involved a vendor’s successful effort to recover damages and attorneys fees for the efforts of the Los Angeles County Sheriff’s Department which licensed a product subject to a limit
A software compliance issue is not usually enough to justify reconsideration of a deal but may have pricing implications if there appears to be a good deal of exposure to vendor claims, and may raise questions about the overall competence and integrity of the target’s organization. On the positive side, this review may also identify duplicative licenses for software or related “maintenance” services, which allow cancellation and cost savings.

This inquiry must also extend to whether the license agreements contain language under which the transaction itself may constitute a breach or require an additional payment, even if the target is otherwise in compliance. At the least, the target will have to provide the vendor with written notice of the transaction.

An unrelated, seemingly mundane but important consideration is the terms of any leases for IT hardware. Such leases are non-cancellable for their stated terms, which limits any potential short term savings to be realized from integration of two firms’ IT functions. Such leases often contain onerous terms governing equipment return or purchase or lease extension, which can also require significant management and make illusory some of the anticipated savings from integration. The DD process should also involve a review and cataloging of the target’s hardware leases to ensure that the acquirer understands the nature of the financial commitments and any problematic terms governing required notice of about 3500 users but installed it on about 6000 computers, with a mechanism to prevent its concurrent use by more than 3500 users. The Ninth Circuit was not impressed with the Department’s creativity as it held in favor of the vendor and also awarded attorneys’ fees to the plaintiff.
of termination at the end of the stated term, requirements to purchase all items covered by a lease even if only a portion of them are desired, minimum or arbitrarily determined end-of-term purchase price or required condition at return.

CONCLUSION

While the M&A process always involves significant business risk and its outcome is susceptible to macroeconomic factors which are not subject to mitigation even by the best practices, good DD will go along way toward shifting the odds in favor of success for those deals which do go forward. Good DD today requires a sophisticated approach to IP and IT matters. It is hoped that this article can make a modest contribution toward increased sophistication of executives and practitioners in this area.