

INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY DUE DILIGENCE IN MERGERS AND ACQUISITIONS: A MORE SUBSTANTIVE APPROACH NEEDED

Martin B. Robins[†]

I. INTRODUCTION: REASONS FOR A NEW APPROACH

Few decisions have greater consequences for a business than the decision of whether to acquire another business.¹ In today's world, one of the key determinants of a business's value is the value of its intellectual property ("IP") and information technology ("IT").²

However, it appears that with relatively few exceptions, the due diligence ("DD") processes,³ by which businesses assess the benefits of acquiring a

[†] Mr. Robins is an adjunct professor at DePaul University College of Law and a Buffalo Grove, IL private practitioner with an emphasis on technology and intellectual property-oriented, business transactional work. He holds a B.S. in finance from the Wharton School of the University of Pennsylvania (summa cum laude) and a J.D. from Harvard Law School (cum laude). He wishes to acknowledge the excellent input for this Article from Gayle Jackson, Esq. Comments on this Article are most welcome and may be directed to mrobins@mr-laws.com.

1. Lee Gomes, *H-P's IBM Envy Drives Deal*, WALL ST. J., May 14, 2008, at B8 ("Few things a company can do are taken more seriously than a big acquisition. Because that often means betting the farm . . ."); see, e.g., ROBERT F. BRUNER, *DEALS FROM HELL: M&A LESSONS THAT RISE ABOVE THE ASHES* 95-340 (2005) (describing in detail the potentially dire consequences of acquisitions gone awry, including large losses and, sometimes, liquidation for companies, such as Penn Central, Revco Drugstores, Quaker Oats, Snapple, Mattel, The Learning Company, and others, as well as the positive consequences from a deal done well); David Enrich, *CEOs Grapple with Subprime Beast: Pandit of Citigroup Plots a Turnaround but Not a Breakup*, WALL ST. J., May 10, 2008, at B1 (referring to the failure to integrate sixteen data centers following 1998 acquisitions by Citigroup). Many troubled financial institutions find themselves in an acquisition predicament, in part, as a result of acquisitions of other institutions. See, e.g., Dan Fitzpatrick et al., *With Wachovia Sale Looking Likely, a Makeover for Charlotte, U.S. Banking*, WALL ST. J., Sept. 29, 2008, at C1 ("Wachovia [Bank's] fall began with its \$25 billion purchase of mortgage lender Golden West Financial corp. in 2006.").

2. Jon Van, *Stock Index Values Firms on Basis of Their Patents: Chicago's Ocean Tomo Ranks 300 Companies*, CHI. TRIB., Nov. 15, 2006, § 3, at 1 ("Now, tangible assets make up less than 20 percent of companies' market value."). For example, Microsoft Corporation in its 2006 Annual Report to Shareholders, identifies as material risk factors to its business model, problems protecting "intellectual property rights against piracy, infringement of . . . patents by third parties, or declining legal protection for intellectual property" and infringement claims brought by third parties. MICROSOFT CORPORATION, MICROSOFT CORP. ANNUAL REPORT 2006 15 (2006), available at http://www.microsoft.com/msft/reports/ar06/downloads/MS_2006_AR.doc; see also Enrich, *supra* note 1, at B1 (referring to an example of how poor integration of sixteen data centers adversely impacted Citigroup).

3. *Escott v. BarChris Constr. Corp.*, 283 F. Supp. 643, 682-83 (S.D.N.Y. 1968) (introducing the term "due diligence" and construing section 11(b)(3)(A) of the Securities Act of 1933 as referring to the standard of

potential target, do not emphasize such matters. Rather, businesses emphasize traditional matters such as minute books, suit papers, credit agreements, and accounting work papers.⁴ Although the customary confidentiality of the DD process means that there is no way to perform meaningful empirical analysis to test this conclusion, both the author's observations and the limited pertinent commentary corroborate this assertion. "Many companies approach due diligence by dotting the *i*'s and crossing the *t*'s," but companies should instead "focus all of [their] time making sure the strategic value is there."⁵

Frequently, when IP and IT are addressed, the focus is 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.⁶ This Article is intended to explain why additional substantive attention is warranted when reviewing a company's IP and IT processes, as a result of recent changes in the legal and technological environments and the diverted focus of many practitioners. Additionally, this Article will discuss how to best provide this additional attention to actual transactions. The objective is to provide a conceptual framework to supplement and guide the myriad of steps that are required in this process, as well as guide the development of new steps that will be needed to accommodate the inevitable changes that will occur in the areas of law and technology. This framework involves the *critical* consideration of the genuine economic and operational value and risks associated with a target's IP and IT related practices.

More traditional document-based DD was appropriate for many years when IP and IT were rarely key drivers of business value. However, in today's

care required of one deemed an "underwriter" in a securities offering).

4. For an example of the traditional approach being applied, as well as the potential impact of merger and acquisition transactions on IP licenses, see Elaine D. Ziff, *The Effect of Corporate Acquisitions on the Target Company's License Rights*, 57 BUS. LAW. 767, 786-87 (2002) (surveying several courts' approaches to determining assignability of patent and copyright licenses). While Ziff provides outstanding guidance to the bar as to the structural considerations impacting license compliance, with emphasis on the need to consider the form of the corporate transaction when crafting a license compliance strategy, the article does not discuss the equally significant need for a substantive analysis of the subject matter of those patents. *See generally id.*

5. Kate O'Sullivan, *Time to Buy*, CFO, June 2008, at 79 (quoting David Williams of the Financial Advisory Services practice of Deloitte and Touche).

6. *See* Geoffrey Groshong & Samantha Pak, *Patent Portfolios in Bankruptcy Cases: Protecting and Maximizing Their Value*, BUS. L. TODAY, July-Aug. 2008, at 51 ("[P]atent counsel must remain highly vigilant and know the patent rules to ensure that deadlines are not missed."). This article, which discusses analogous circumstances of a trustee or debtor in possession of an IP holding company in bankruptcy, is intended to provide guidance for those assuming control of bankrupt entities. *Id.* The article contains some discussion of the need to use relevant professionals to assess the substance of patents as they impact operations, but focuses on procedural aspects of due diligence, with headings such as "List All Patents and Applications," "File a Power of Attorney," "Be Aware of Deadlines," and "Ensure Maintenance Fees are Paid." *Id.* at 52. The latter topics are certainly essential, especially for one with a fiduciary obligation to preserve or maximize a company's value, but must not overshadow the need to fully understand the strategic value of the patents in today's environment. Notably, the article does not even cite or mention *KSR Int'l Co. v. Teleflex Inc.*, which must be properly applied to understand the current value of a given patent. *See generally id.* at 51-55. An anecdotal illustration of this approach is found in NAT'L BUS. INST., INTELLECTUAL PROPERTY IN BUSINESS TRANSACTIONS: BEST PRACTICES IN LICENSING AND ACQUIRING IP RIGHTS (2008) (brochure on file with author). Of the five specific topics listed in the "Considerations during Mergers and Acquisitions" segment of the program, three are: Hart-Scott-Rodino Notification Rules, Drafting Non-disclosure Agreements, and Accounting for IP: Statement of Financial Accounting Standards 141 and 142. *Id.*

world, where hard assets normally play a subordinate role in business success and valuation, and where judicial decisions (and sometimes even the bringing of suit)⁷ and legislation have such a drastic impact on economic outcomes, a different approach is warranted. Very recent legal and technological developments include:

- The much more stringent standard for sustaining patents against obviousness challenges brought about by the U.S. Supreme Court's decision in *KSR International Co. v. Teleflex Inc.*;⁸
- The increased business potential and legal exposure associated with Web-based blogging and interactive marketing possibly leading to claims of secondary infringement of copyrights and trademarks;⁹
- The creation of major legitimate and illegitimate businesses around digital music and movies;¹⁰ and
- The increasing significance of identity theft and related legislation.¹¹

These developments compel a detailed, rigorous analysis of the target's IP and IT in an effort to assess their ultimate value (or detraction from value). Hopefully, this discussion will be helpful not only to the practicing bar pursuing best practices but also to the bench and commentators striving to develop standards of conduct and liability to govern the disputes that will inevitably arise to an increasing extent from IP and IT issues in merger and acquisition ("M&A") transactions.

II. 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, development, or license from a third party.¹² With the notable exception of trade secrets, almost all of

7. See Kevin J. Delaney, *Google Push to Sell Ads on YouTube Hits Snags*, WALL ST. J., July 9, 2008, at A1 ("Copyright litigation has complicated the YouTube ad push.").

8. 127 S. Ct. 1727 (2007); see Linda Greenhouse, *High Court Puts Limits on Patents*, N.Y. TIMES, May 1, 2007, at C1 (noting that the court's decision in *KSR* "raise[s] the bar for obtaining patents on new products that combine elements of pre-existing innovations.").

9. See discussion *infra* Part III.C.2 (noting that with the rise in digital media offerings has come an increased risk of secondary infringement exposure); see, e.g., *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 940 (2005) (noting that *Grokster* sought profit from secondary infringement, which was significantly different from prior similar case).

10. See generally *Grokster*, 545 U.S. at 939–40 (holding that a "peer-to-peer" file sharing network that derived revenue from the illegal sharing of copyrighted music had an "unlawful objective").

11. See discussion *infra* Part IV.A.

12. See J. May Liang, *Going In-House with Intellectual Property*, BUS. L. TODAY, Mar.-Apr. 1997, at 36 (describing the major element of each type of IP). Each type inherently involves an element of exclusivity or monopoly (the right to exclude others from doing something). *Id.* at 36–41. Such exclusivity is deemed to be in society's interest by promoting innovation. See, e.g., U.S. CONST. art. I, § 8, cl. 8 ("[A]ll duties, imposts and excises shall be uniform throughout the United States . . . [t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."); *KSR Int'l*, 127 S. Ct. at 1746 (noting that giving exclusive rights to ordinary innovation would stifle progress).

the relevant law is federal.¹³

A. Why Conduct Due Diligence? How Do These Factors Impact IP and IT?

The most basic reason to conduct DD is to determine if it is appropriate to proceed 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, technological, cultural, or personal incompatibility, the deal may not make sense and should be reconsidered. In many such cases, unless contractually obligated not to, the acquirer should simply walk away. Frequently, a target’s claimed competitive advantage from IP turns out to be nonexistent or exaggerated upon closer evaluation. Similarly, a review of IT process, people, or physical infrastructure may reveal that integration of the companies would be much more difficult or costly than originally contemplated.¹⁴

Even if the IP/IT review does not dictate “cratering” the deal, it may dictate pricing adjustments in the acquirer’s plan for the deal. For example, 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.¹⁵ 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 is to be structured. Many IP licensing agreements will be breached if the licensee becomes a party to one type of transaction but not to another.¹⁶ Prudent legal and business practice dictates close review of license documents before determining the formal structure for a deal.¹⁷

DD also impacts the mechanics of a deal. All acquisition agreements will spell out in some form the major “property” and rights or 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—for example, “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

13. See Lanham Act, 15 U.S.C. §§ 1051–1141 (2000) (federal trademark law); Copyright Act of 1976, 17 U.S.C. §§ 101–1332 (2000) (federal copyright law); Patent Act, 35 U.S.C. §§ 101–376 (2000) (federal patent law); California Uniform Trade Secrets Act, CAL. CIV. CODE §§ 3426–3426.11 (West 1997) (exemplifying state trade secret law).

14. See Enrich, *supra* note 1, at B1 (referring to the failure to integrate sixteen data centers following the 1998 acquisitions by Citicorp).

15. See 35 U.S.C. §§ 154–156 (defining the term of a patent).

16. See Ziff, *supra* note 4, at 785 (explaining how the distinction between stock sales, asset sales, and mergers impacting the licensee often determines whether the licensee is in breach of IP licensing agreements that do not expressly enumerate the consequences of acquisitions).

17. See *id.* at 767 (suggesting that license provisions be reviewed for determinations on transferability and any specific prohibitions).

registration applications. The DD process must be used to help both parties develop and agree upon the information comprising this IP/IT schedule.¹⁸

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 the acquirer's management to know what it is getting into and how best to use the resources added by the target. Good management organizations will operate on parallel tracks during the acquisition process so that the information they obtain in DD is used for 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 obtained.

The technical information related to IP typically details how a firm runs major elements of its business. For example, a patented process or device that is used by the target means that it functions in some respect differently than comparable firms. Such information will be invaluable to management charged with combining the operations of the two firms by providing insight as to nuances of the target's operations as they will differ from both prevailing practice and the acquirer's own practices. A customer or supplier list, protected as a trade secret, provides the same benefits in the pertinent areas and will be extremely important to acquiring management in knowing with whom it will be dealing (and often on what terms).¹⁹ 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 procedural elements of DD are fairly straightforward and have not changed a great deal in recent years—such as review of contracts, corporate minutes and filings, and papers in pending litigation—IP and IT materials are by their very nature quite complicated and often serve to define the essence of a business's position in the marketplace. Changes in the marketplace and legal environment²⁰ have greatly increased both the complexity and opportunity associated with IP and IT. These changes necessitate a significant time commitment coupled with the involvement of a variety of people not typically thought of as part of a DD "core" team, which in the author's experience and observation has relied heavily on lawyers, accountants, and environmental consultants.

B. Who Should Participate in the IP and IT Due Diligence Process?

For the most part, DD is the province of transactional lawyers and

18. 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.

19. See Illinois Trade Secrets Act, 765 ILL. COMP. STAT. 1065/2(d) (2006) (including a "list of actual or potential customers or suppliers" within the definition of a trade secret).

20. See, e.g., *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727 (2007) (raising the standard for granting or sustaining a patent); *M.G.M. Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (explaining and arguably creating some of the elements of a cause of action for secondary copyright infringement with respect to digital media).

accountants, with secondary involvement from subject matter experts (“SMEs”), 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 SMEs 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 systems integration consultant to consider a target’s IT environment and its integration with that of the acquirer. Such SMEs should take the lead in the substantive review process²¹ in which the business significance of the various items of IP and the IT infrastructure are absorbed and evaluated. For example, an engineer would advise the DD team of whether the subject matter of a patent is likely to work as advertised, whether it is genuinely a breakthrough for commercial purposes, or whether it would be easy for someone to develop the same capability without infringing on the claims of the patent.

For IP matters, the required types of SMEs will vary greatly depending on the type of IP at issue. Consideration of patents will involve engineers and/or scientists and patent lawyers,²² while consideration of trademarks will usually be for sales and marketing management, with some input from trademark counsel.²³ Copyright matters will usually require persons with design or literary expertise, although the growing concerns regarding secondary infringements²⁴ brought about through technological innovations may cause the involvement of engineers or computer scientists, as well.²⁵ Trade secret issues will likely remain the province of lawyers, with significant involvement from human resources professionals.

IT matters will require discussion between each party’s IT managers, framed by lawyers with some familiarity of the major issues in this context.

C. What Are We Looking For in the Due Diligence Process?

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

21. 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.

22. HOWARD B. ROCKMAN, *INTELLECTUAL PROPERTY LAW FOR ENGINEERS AND SCIENTISTS* 98 (2004); *see also* *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 387 (1996) (“As it cannot be expected . . . that judges will always possess the requisite knowledge of the meaning of the terms of art or science . . . it often becomes necessary that they should avail themselves of the light furnished by experts . . .”).

23. David A. Westenberg, *What’s in a Name? Establishing and Maintaining Trademark and Service Mark Rights*, 42 *BUS. LAW.* 65, 65 (1986) (“A trademark is a word, symbol, design or device, or any combination thereof, used by a manufacturer or merchant to identify the source of its goods, and to distinguish them from goods manufactured or sold by others.”). It is necessary for those responsible for selling the product(s) at issue to make an assessment of whether their marks are conducive to doing so in the relevant, post-acquisition circumstances. *Id.* at 66–67.

24. *See Grokster*, 545 U.S. at 914 (“[T]he argument for imposing indirect liability is powerful.”).

25. *See, e.g.*, Complaint at 7–9, *RealNetworks, Inc. v. DVD Copy Control Ass’n* (N.D. Cal. 2008) (No. C-08-4548) (alleging that RealNetworks’s program, which allows the copying of DVDs to computer hard drives, violates the Digital Millennium Copyright Act). The outcome of this case may serve to illuminate the meaning of section 501 of this statute. RealNetworks’s explanation may be diluted as a result of its argument that its license with an affiliate of plaintiffs supersedes any statutory prohibitions. *Id.*

- What is the target's IP worth, now and in the future, in the plant, in the marketplace, and in court;
- How well does it insulate the target's business from legitimate competition as well as infringement;
- Does the target face a realistic threat of third-party claims for infringement of IP; and
- Does the target take proper measures to minimize the likelihood of involvement in disputes concerning alleged infringement of third-party IP?

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 by competitors. It is even worse to discover that a seemingly valuable IP portfolio is the result of misappropriation or infringement of another party's IP. 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.²⁶ As is true with all legal claims, one does not want to acquire a lawsuit or the need for one in an M&A transaction. The IP area is particularly susceptible to legal disputes as a result of many of the recently promulgated authorities, which substantially change the legal environment by expanding or limiting various legal theories of interest to practitioners in the area.²⁷

Since 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—such as patent, copyright, trademark and trade secret—but also obligations contained in the applicable license documents. In many cases, behavior that is clearly permissible or, at worst, arguable under common and statutory law, is the subject of an express contractual provision that either permits or prohibits it.²⁸ In many copyright cases the contract at issue is not a traditional one on paper but is a so-called “click wrap” or “browse wrap” agreement where users click a button with their

26. Injunctions or large settlements/damage awards often result from infringement claims and attorney's fee awards are also fairly commonplace. Large legal fees are certain. The well-known lawsuit involving the patents associated with the Blackberry device—which nearly caused the shutdown of Blackberry service and was settled for over \$600 million, despite serious questions about the validity of the patents—is an example of the impact of such claims. Adam Jaffe & Josh Lerner, *Innovation and Its Discontents*, WALL ST. J., Mar. 21, 2006, at A14.

27. See, e.g., 17 U.S.C. §§ 501, 1201 (2000) (heightening penalties for copyright infringement on the Internet and criminalizing production and dissemination of technology intended to circumvent measures that control access to copyrighted work added as part of the Digital Millennium Copyright Act); *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727, 1740 (2007) (finding that an improvement that is discoverable by a “person of ordinary skill” likely bars patentability); *Grokster*, 545 U.S. at 919 (holding that one who distributes a product used to violate copyright and promotes its use to violate copyright is liable for the resulting infringement by end users).

28. See DONALD M. CAMERON & ROWENA BORENSTEIN, KEY ASPECTS OF IP LICENSE AGREEMENTS 13–15 (2003), available at <http://www.jurisdiction.com/lic101.pdf> (providing examples of types of limitations).

mouse to manifest their consent.²⁹ Inquiry must be made as to whether the target customarily agrees to or tracks the acceptance of licenses covering all relevant products, including those covered by a “traditional” license document and those covered by “click wrap” agreements. Such inquiry should also encompass the use of so-called “open source” software for which the relevant materials are made freely available on the Internet, but are subject to use limitations in a “General Public License” document.³⁰ Noncompliance with the latter can constitute both copyright infringement and breach of contract.³¹

D. Who Are the Parties? Legal and Operational Implications

For IP licensed to the target, it is worth considering the financial stability of the licensor. If the licensor disappears or encounters major financial problems, this will at the least impact the support provided to the licensee for the IP following the execution of the license, which is often referred to as “maintenance,” and is of great significance for software and sometimes (in some form) for patents.³² Until fairly recently, a licensor’s bankruptcy could also result in a termination of the license by the licensor or its trustee, resulting in devastating consequences for a licensee who needed to continue to use the IP in its business.³³ However, section 365(n) of the Bankruptcy Code now dramatically reduces this risk for all IP except trademarks.³⁴ A licensee bankruptcy may also be problematic for the licensor—especially if the bankrupt licensee had an exclusive license—and is not governed by a specific IP-oriented statute.³⁵ At a minimum, as is the case with any contract where a party files for bankruptcy while owing money, there will be an interruption in the payment of royalties and there may be impediments to relicensing the IP to someone else.³⁶

Since M&A transactions and macroeconomic turmoil can have a major impact on the viability of licensors and licensees,³⁷ it is also prudent to address the termination provisions of any major license agreements to which the target

29. See Christina L. Kunz et al., *Browse Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279, 279–80 (2003) (describing “click wrap” and “browse wrap” agreements).

30. E.g., Free Software Foundation, GNU General Public License, <http://www.fsf.org/licenses/licenses/gpl.html> (last visited Nov. 18, 2008).

31. *Jacobsen v. Katzer*, 535 F.3d 1373, 1382–83 (Fed. Cir. 2008).

32. See Richard M. Cieri & Michelle M. Morgan, *Licensing Intellectual Property and Technology from the Financially-Troubled or Startup Company: Prebankruptcy Strategies to Minimize the Risk in a Licensee’s Intellectual Property and Technology Investment*, 55 BUS. LAW. 1649, 1691 (2000) (describing ways to secure performance of obligations under license and maintenance agreements).

33. *Id.* at 1661–63.

34. The Intellectual Property Bankruptcy Protection Act of 1988 expressly precludes “rejection” of an IP license by a bankrupt licensor at the election of the licensee during its stated term. Intellectual Property Bankruptcy Protection Act of 1988, 11 U.S.C. § 365(n) (2000); see also Cieri & Morgan, *supra* note 32, at 1661 (discussing the entire topic of the applicability of section 365 of the Bankruptcy Code).

35. See, e.g., *In re Catapult Entm’t, Inc.*, 165 F.3d 747, 748 (9th Cir. 1999) (describing how a licensor may prevent a licensee from reassigning a nonexclusive patent during post-bankruptcy reorganization plans).

36. RANDY MICHELSON, *Bankruptcy Issues in Negotiating eCommerce Transactions*, in SEVENTH ANNUAL INTERNET LAW INSTITUTE 763, 780 (2003).

37. See Ziff, *supra* note 4, at 787–88 (describing an example of changes in contract rights due to a change of ownership).

is a party to determine what circumstances allow for termination. For example, if there is a “change of control” of the licensor, or if the licensor’s circumstances drastically deteriorate, or merely for the licensor’s own convenience.

E. Outside the United States

While space considerations dictate that this Article focus on U.S. issues, it must be stressed that to an increasing extent, IP matters are subject to law outside the United States.³⁸ This means that for both an offensive and a defensive analysis, the acquirer of a target with any material non-U.S. operations must 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 United States.³⁹ They are doing so in order to protect their own large companies and avoid World Trade Organization sanctions for tacitly allowing infringement of IP rights of Western firms.⁴⁰

F. Proper Use of Due Diligence Findings

The results of the license compliance and patent strength assessments need to be properly used and managed. A pending lawsuit between software giants Oracle and SAP illustrates what happens when this is not the case.⁴¹ When SAP pursued the acquisition of a company called TomorrowNow (“TN”), its DD review was broad enough to discover that TN was misusing Oracle software but proceeded with the transaction anyway.⁴² “Oracle claims that . . . members of SAP’s executive team knew that [TN] misused Oracle’s intellectual property before making the acquisition.”⁴³ Oracle brought suit against SAP in Federal District Court⁴⁴ and included a discussion of the SAP DD team reports in its second amended complaint.⁴⁵

While the outcome of this suit cannot be known at this writing, its existence is certainly a source of expense and embarrassment for SAP.⁴⁶ One

38. See PATRICK J. WHALEN & PEARL HSIEH, PROTECTING INTELLECTUAL PROPERTY IN OUTSOURCING DEALS 3 (2005) (“Through Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), the obligation to protect trade secrets has gone global.”). Despite the limitation of the quoted language to trade secrets, the title of the World Trade Organization Agreement speaks for itself with respect to the internationalization of this area. *Id.*

39. *Id.* at 7.

40. *Id.*

41. Complaint at 28–40, Oracle Corp. v. SAP AG, 566 F. Supp. 2d 1010 (N.D. Cal. 2007) (No. 07-7658) (including counts for, *inter alia*, copyright infringement, breach of contract, and violations of the Computer Fraud and Abuse Act).

42. Second Amended Complaint at 2–3, Oracle Corp. v. SAP AG, 566 F. Supp. 2d 1010 (N.D. Cal. 2008) (No. 07-7658).

43. Ben Worthen, *Oracle Steps up Fight with SAP in Filing*, WALL ST. J., July 29, 2008, at B4.

44. *Id.* at B4.

45. Second Amended Complaint at 19–27, Oracle Corp. v. SAP AG, 566 F. Supp. 2d 1010 (N.D. Cal. 2008) (No. 07-CV-01658).

46. See, e.g., Worthen, *supra* note 43, at B4 (explaining that SAP acquired TN to better compete with Oracle but now has to close it after the discovery of some questionable operating practices); Jacqueline Emigh,

would hope that SAP properly allowed for such considerations when determining the net value of the transaction. In such situations, many companies would be well served by walking away from the deal, rather than grabbing the proverbial hornet's nest.

In any case, the fact that outside of the discovery process Oracle obtained reports from SAP's DD team and quoted them in its complaint indicates that sufficient precautions were not taken to safeguard such materials.⁴⁷ When a DD process does turn up adverse material, it must be properly secured to avoid unintentional disclosure,⁴⁸ and steps must be taken to preserve whatever attorney-client privilege would otherwise apply to protect it from discovery or admissibility in court.⁴⁹ At a minimum, this means minimizing the circulation of the material within the acquirer's organization.⁵⁰

III. SPECIFIC DUE DILIGENCE 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,

- Whether the target has "jumped through the right hoops" regarding the notices and filings that 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;
- Whether the particular contract and property rights, if properly reserved, are sufficient to provide the acquirer with the anticipated business benefit(s); and

SAP Could Sell off Its Embattled Division Amid Oracle Suit, BETANEWS, Nov. 20, 2007, http://www.betanews.com/article/SAP_could_sell_off_its_embattled_division_amid_Oracle_suit/1195597861 (describing how SAP admitted that its customer support division TN "improperly and perhaps illegally downloaded materials from Oracle's Web site by masquerading as one of its customers," and that selling off TN was the best option).

47. See *Oracle Corp.*, 566 F. Supp. 2d at 1013 (allowing production of grand jury documents).

48. Cf. Molly McDonough, *Flying Under the Radar: After Percolating Quietly, These Legal Issues May Grab Headlines in 2005*, 91 A.B.A. J. 35, 36 (2005) (noting many instances of "inadvertent waiver" have been caused by distribution of information to "unintended recipients," which has contributed to an erosion of the attorney-client privilege).

49. Of course, any efforts to safeguard such materials must comply with obligations under the Federal Rules of Civil Procedure and comparable state law to avoid spoliation of evidence that appears to be germane to pending or anticipated litigation. See, e.g., *Zubulake v. UBS Warburg L.L.C.*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (ordering the defendant to supply e-mails stored on backup tapes when no privilege was claimed); *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, No. CA 03-5045 AI, 2005 WL 674885, at *9 n.17 (Fla. Cir. Ct. Mar. 23, 2005) (finding a defendant violated numerous discovery orders when it claimed over two hundred documents were privileged, and considering the claims of privilege unfounded).

50. While practices diverge among the states, in federal court, the privilege can be preserved best by limiting dissemination of arguably privileged material to those within a corporation who have a bona fide interest in its subject matter. *Upjohn Co. v. United States*, 449 U.S. 383, 400 (1981). A commentator summarizes the guiding principle as: "[U]nless you want to risk a waiver, don't send a memorandum dealing with legal matters to anyone who isn't working on or involved with the problem." Michael A. Lampert, *In House Counsel and the Attorney Client Privilege*, FINDLAW, 2000, <http://library.findlaw.com/2000/Oct/1/128767.html>.

- Whether the target is properly respectful of the IP rights of others.

A. Patents

1. Implications of Recent Case Law

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.⁵¹ Many have argued that the patent system has discouraged innovation and creativity by granting many patents for “inventions” that add little to the greater good, but simply serve to enrich their inventors by discouraging legitimate competition that would naturally flow from the existing knowledge base.⁵² Issuing patents for so-called business methods was authorized by the Federal Circuit in *State Street Bank v. Signature Financial Group* in 1998,⁵³ and has been seen by many as particularly problematic.⁵⁴

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, enforce, and maintain in the face of infringement. Most notably the Court in *KSR International Co. v. Teleflex Inc.*,⁵⁵ 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.⁵⁶ The Court approvingly cited the district court’s view that obviousness is to be judged from the perspective of someone with a bachelor’s degree in engineering in the relevant field, as opposed to merely a reasonable person.⁵⁷ This will clearly make it harder to obtain a patent and easier to escape liability for infringement, since a defendant in an infringement action may defend on the basis of the patent’s invalidity.

As this Article went to press, in a closely followed case involving a

51. Such discussions appear in many places, not least of which is the U.S. Supreme Court’s opinion in *KSR Int’l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1746 (2007) (“And as progress beginning from higher levels of achievement is expected in the normal course, the results of ordinary innovation are not the subject of exclusive rights under the patent laws. Were it otherwise, patents might stifle, rather than promote the progress of useful arts.”); see also *eBay Inc. v. Mercexchange, L.L.C.*, 547 U.S. 388, 393 (2006) (discussing the new economic function of a patent holder); Jaffe & Lerner, *supra* note 26, at A14 (claiming that the current system induces abuse rather than innovation and suggesting potential reform).

52. Jaffe & Lerner, *supra* note 26, at A14.

53. See *State St. Bank & Trust v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1376–77 (Fed. Cir. 1998) (holding that there was no statutory subject matter bar to a business method patent).

54. Jaffe and Lerner advise that “financial patents are being litigated at more than 10 times the rate of awards more generally.” Jaffe & Lerner, *supra* note 26, at A14. As an apparent precursor to its decision in *Bilski*, the Federal Circuit reacted to the *KSR* decision by ruling in *Comiskey* that a mental process needs some sort of technological connection to be patentable. *In re Comiskey*, 499 F.3d 1365, 1374–79 (Fed. Cir. 2007).

55. 127 S. Ct. at 1742.

56. 35 U.S.C. § 103(a) (2000) (requiring that such items be nonobvious); see also *id.* § 101 (noting that the basic standard for granting of a patent is “any new and useful process, machine, manufacture, or composition of matter . . .”).

57. *KSR Int’l*, 127 S. Ct. at 1738. The Court also noted that “[g]ranteeing patent protection to advances that would occur in the ordinary course without real innovation retards progress and may, for patents combining previously known elements, deprive prior inventions of their value or utility.” *Id.* at 1732.

commodity trading strategy, in which thirty-nine amicus briefs were filed, the Federal Circuit, acting *en banc*, substantially limited the patentability of business methods without a direct physical application. In *Bilski*,⁵⁸ the court indicated that it would be insufficient for a method application to be based only on the existence of the “useful, concrete and tangible result,” which was approved by the same court in the *State Street Bank* case. The *Bilski* opinion made clear that it was not promulgating a per se rule barring the issuance of business method patents, but relied upon the U.S. Supreme Court’s decision in *Gottschalk v. Benson* to reiterate that any patent based on a process or method would have to have some genuine, meaningful connection to a machine or transform a particular article into a different state or thing.⁵⁹

In addition, the Supreme Court has limited the remedies available to patent-holders by making clear that even where infringement is established, requests for injunctive relief must be held to the same standard as in any other case, rather than strongly presumed or automatically available for the aggrieved patent-holder.⁶⁰

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 to any significant degree of business method patents. Existing patents are more likely to be invalidated in infringement litigation⁶¹ and applications are less likely to be granted. Those patents that are granted and upheld will sometimes offer their holders less effective relief from infringement.⁶² 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.

2. Assessment of Business Value

Assuming the validity of a target’s patent portfolio, the acquirer needs to assess its business value. This means enlisting SMEs with appropriate

58. *In re Bilski*, No. 2007-1130, 19–21 (Fed. Cir. Oct. 30, 2008), available at <http://www.cafc.uscourts.gov/opinions/07-1130.pdf>

59. *Id.* at 10 (citing *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)).

60. In *eBay Inc. v. Mercexchange, L.L.C.*, the Supreme Court reiterated that before granting equitable relief in a patent case, the court must consider (as in any other case not governed by a contract or statute) 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, whether the burden of an injunction would be disproportionate, and whether the injunction is contrary to the public interest. *eBay Inc. v. Mercexchange, L.L.C.*, 547 U.S. 388, 391 (2006).

61. According to Professor Dennis Crouch of the University of Missouri Law School, “[p]atentees have long had the upper hand in patent litigation but the KSR case has shifted that balance of power back to defendants.” Peter Lattman, *How a Patent Ruling Is Changing Court Cases*, WALL ST. J., July 31, 2007, at B1. In *Reinventing Patent Law*, Donald R. Ware of the Foley Hoag law firm aptly summarized the trend: “[T]he Supreme Court, Congress and the patent office are moving in a direction that is unfavorable toward patentees. That is a big change.” Steve Seidenberg, *Reinventing Patent Law*, A.B.A. J., Feb. 2008, at 59.

62. See generally Seidenberg, *supra* note 61, at 60–61 (discussing cases that make it difficult for patent holders to obtain certain types of relief).

technical skills and marketplace familiarity who can determine how much the patents advance the target or industry's ability to introduce commercially successful products to the market. A major part of this process is review of the "claims" included in each patent application. "Claims" refer to the specific technical improvements brought about by the patent application and define the extent of the exclusivity.⁶³ This process should encompass both granted and pending patent applications.

At this stage, 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 and patent defense approaches. The discussion must encompass patent searches conducted in anticipation of a proposed new invention or refinement to an existing product where a third party's patents need to be evaluated in order to minimize the likelihood of infringement. Of course, if the target believes that it is taking a calculated risk with significant business benefits by infringing the arguably invalid patent of another, any potential infringement must be noted and quantified to the extent possible. It is important to note that this may give effect to the possibility of additional damages resulting from the willful infringement. The important thing is to screen out companies who are simply unconcerned about the need to respect the genuine IP of others.

3. *Additional Burdens of Licensing*

The preceding analysis should be conducted with respect to patents that are directly owned by the target, as well as those that are licensed to it. If great reliance is placed on a licensed patent that turns out to be invalid, adverse business and possibly legal consequences will result.⁶⁴ It may be more difficult to obtain access to the required information and people if a target has licensed a patent rather than if it owns one, but this information is essential where the licensed patent is material to the target's business.

With all patents subject to licenses (as both licensee and licensor), it is critical to closely review the *infringement indemnification* language that allocates responsibility for dealing with third-party infringement claims.⁶⁵

63. See 35 U.S.C. § 112 (2000) (outlining the requirements for patent claims).

64. See Jaffe & Lerner, *supra* note 26, at A14 (noting that a business was forced to pay a settlement of over \$600 million to prevent Blackberry handhels from going dark, due to a potential injunction resulting from patent infringement litigation).

65. 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). See generally James J. Widland, *Selling the Family Business*, BUS. L. TODAY, May-June 2005, at 43, 47 (discussing misstatements within indemnity provisions for preparing purchase agreements for selling businesses). 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. Transaction pricing will impact, if not dictate, the indemnification structure.

Such provisions usually address responsibility for both defense costs—for example, 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 licensor’s entire patent portfolio 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 United States;
- Requirements for prompt notice of a claim for which an indemnity is sought as a complete defense if not complied with, or only coming into play to the extent of actual prejudice from the delayed notice; and
- Right or obligation of the indemnified party to take control of the defense of a claim.⁶⁶

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 it may have if it is challenged on account of patents licensed 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., the 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.

4. Procedural Due Diligence

While this Article argues strongly for increased emphasis on substantive analysis of patents, it must be emphasized that this does not reduce the importance of procedural review. Concurrently with the substantive analysis, counsel should work with its counterpart to address the procedural aspects of the target’s patent portfolio. This procedural analysis may have major implications on the target’s value and will have to be translated into a definitive agreement schedule. Matters that need to be disclosed in the schedule along with corroborating documentation such as patent certificates and applications include:

- Patent (or application) numbers;
- Patent types (design, process, composition, device, or business method);
- Ownership of patents including written assignments of ownership

66. See generally James P. Hanrath, *Before You Agree... Consider Alternatives to Patent Indemnity* (2001), <http://www.muchshelist.com/471.htm> (discussing “due diligence checklists” for patent transactions).

from employees⁶⁷ (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 applications;
- Status (applied for, granted or subject to a provisional patent);⁶⁸ and
- Filings and fee payments to keep the patent in force.⁶⁹

Counsel should also conduct appropriate analysis of products being developed for which the target contemplates filing a patent application. These matters should also be included on the definitive agreement disclosure schedule. Such a schedule should also enumerate pending applications for which the target will normally sign a 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 (where target is either licensor or licensee) call for separate procedural analysis with the emphasis on not only the nature of the patents involved, as described above, but also commercial issues such as:

- License duration and extension options;
- Use limitations—e.g., type of product, number of units, and geographic limitations; royalty amounts, formulae, and adjustments;
- Compliance audit or verification mechanisms;
- Identity of parties, with emphasis on identification of those who are financially unstable or likely to be untrustworthy in a manner that would spawn litigation or compromise the value of the patent;

67. 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. *See* 17 U.S.C. § 101 (2000) (defining a “work made for hire” as one that is “prepared by an employee within the scope of his or her employment.”). 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* Eric J. Moutz & Adrian Eissler, *Four Strategies for Controlling Employee-Created IP*, 36 COLO. LAW. 31, 31 (2007) (explaining that the best way for a company to establish ownership rights to IP is by getting employee-inventors to sign an employee agreement).

68. A provisional patent requires little documentation but is only good for one year, and it serves as something of a “placeholder” for a patentee who is testing the water to see if it is prudent to incur the expense associated with a full scale application. *See* 35 U.S.C. § 112 (2000) (specifying the required elements in a claim); *see also* U.S. Patent & Trademark Office, Provisional Application for Patent, www.uspto.gov/web/offices/pac/provapp.htm (last visited Nov. 18, 2008) (explaining the process for filing a provisional application for patent). If a “traditional” patent is granted, the patentee’s exclusivity relates back to the granting of the provisional patent. *Id.* During the one year, the applicant can refer to its “patent pending” status. *Id.*

69. *See* U.S. Patent & Trademark Office, Fees – FY 2009 Fee Schedule, <http://www.uspto.gov/web/offices/ac/qs/ope/fee2008october02.htm#maintain> (last visited Nov. 18, 2008) (outlining patent maintenance fees including fees for late payment).

- Whether or not the license is exclusive vis-à-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.⁷⁰

If the proposed deal or resulting corporate 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 the structure of the deal.⁷¹

Additionally, because many infringement suits arise from failed licensing negotiations (initially or with respect to renewal),⁷² the target should include, on the disclosure schedule, any pending license negotiations and its status as either licensor or licensee.

5. Patent Pools, Trade Regulation, and Other Considerations

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 its members, with or without payment of a royalty—need to be identified, evaluated, and documented.⁷³ 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. 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 that 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 nonexclusive license involving IP), such as exclusive territorial provisions and joint research and development or grantback agreements to which the target is a party, also needs to be specifically identified and evaluated from a trade regulation perspective.⁷⁴ Because IP, by definition, involves a limitation of competition, any collaboration among firms involving the shared access to IP requires significant scrutiny.⁷⁵ The U.S. Department of

70. See Ziff, *supra* note 4, at 785 (describing the Sixth Circuit's handling of the issue of assignability in patent licenses). To overgeneralize, nonexclusive patent and copyright licenses that are silent on the matter are usually deemed nonassignable, and thus contravened by asset sales and mergers, even without a showing of prejudice, but not contravened per se by stock sales. *Id.* Trademark license analysis usually involves consideration of actual prejudice to the licensor from the proposed transaction. *Id.* Express permission or prohibition of M&A transactions contained in licenses are given effect. *Id.*

71. While *Grokster* arose in connection with a copyright issue, its teachings are equally applicable to all types of IP and are included in this section because the patent DD process is likely to generate more findings than the process for other IP. *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 915 (2005) (referencing patent law concepts in defining a theory of contributory copyright infringement).

72. See, e.g., *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1729 (2007) (arising because of breakdown of licensing negotiations).

73. 54 AM. JUR. 2D *Monopolies, Restraints of Trade, and Unfair Trade Practices* § 137 (2008).

74. U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, *ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY* 24–32 (1995), available at <http://www.usdoj.gov/atr/public/guidelines/0558.pdf> (requiring the licensee to provide the licensor with a license to any derivative works produced by the licensee from the licensed IP).

75. See *id.* at 2–4 (applying standard antitrust analysis to IP).

Justice and Federal Trade Commission have promulgated “Guidelines” indicating when they will challenge multi-company arrangements involving IP.⁷⁶ The Guidelines also contain a safe harbor for arrangements involving companies with under 20% of the relevant market.⁷⁷ 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.⁷⁸

Where a transaction takes the form of an asset sale or transfer of a patent (or group of patents), a filing is required with the U.S. Patent and Trademark Office (“PTO”).⁷⁹ This should be addressed, both for the transaction for which DD is being performed and for any of the target’s previous transactions in which patents were acquired, in order to ensure that it has good title to such patents.

B. Trademarks and Servicemarks

Trademarks and servicemarks can appear in a variety of situations. While the most obvious such situation is a target with branded products, such marks will also appear as a consequence of franchise agreements to which the target is a party, or as corporate logos. 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. federal registration.⁸⁰ Preferably, such registration will be on the “Principal Register” instead of the “Supplemental Register.”⁸¹ The registration certificates will have to be examined as part of the procedural DD.

76. *Id.* 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. *Ill. Tool Works v. Indep. Ink*, 547 U.S. 28, 45 (2006). These Guidelines also address “tying” arrangements, whereby one wishing to purchase the patented product must also purchase another, nonpatented product. *Id.* In *Illinois Tool Works*, the U.S. Supreme Court directed that such arrangements be evaluated on a case-by-case, rule of reason basis, instead of their prior rule of per se illegality. *Id.* at 36.

77. U.S. DEP’T OF JUSTICE & FED. TRADE COMM’N, *supra* note 74, at 22.

78. *Id.* at 24–25.

79. As of October 1, 2005, the PTO no longer provides a specific form for this purpose but still requires assignments to be recorded in its records. U.S. Patent & Trademark Office, Assignments and Licenses, www.uspto.gov/web/offices/pac/doc/general/assign.htm (last visited Nov. 18, 2008). Pre-October 2005 assignments of mission-critical patents should be verified with the PTO. 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 the assignment should be notarized. *Id.*

80. Westenberg, *supra* note 23, at 69.

81. 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. *Id.* at 70. There is also a fairly new statute providing special protections to “famous” trademarks even without a showing of likelihood of confusion. Trademark Dilution Revision Act of 2006, Pub. L. No. 109-312, § 2, 120 Stat. 1730 (to be codified as amended at 15 U.S.C. § 1125(e)). 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 that are arguably famous.

1. Substantive Considerations

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.⁸² The marks that are most defensible in a legal proceeding are those with no apparent connection to the product and which contain fanciful shapes or characters—such as “Exxon” or “McDonald’s.”⁸³ Marks that on their face refer to a type of good or service are more likely to be easily and legitimately appropriated by competitors.⁸⁴ 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.

A topic related is whether, and how well, the target has “policed” its marks against persons who use them on counterfeit products or on competitive products.⁸⁵ The owner of a mark has a legal incentive to avoid public confusion by taking action against those who use the mark in a misleading manner; inadequate policing of a mark can lead to a loss of trademark rights.⁸⁶ 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:

Trademarks receive legal protection primarily to prevent buyers from being fooled about the source of goods or services. If a company that owns a trademark fails to control who uses the mark to the extent that the mark no longer indicates a single source of goods or services, the rationale underlying legal protection collapses.⁸⁷

The basic standard for enjoining the use of a mark is whether it is causing or is likely to cause consumer confusion.⁸⁸

The target's policing practices need to be evaluated to determine if they adequately protect marks to which the acquirer has assigned significant value. If it appears that the target has largely ignored infringing uses, then the

82. Westenberg, *supra* note 23, at 66.

83. *Id.*

84. *Id.*

85. *Id.* at 85; see also Deborah Wilcox, *Resist Cease and Desist: A Lighter Approach May Work Better with Trademarks*, BUS. L. TODAY, May-June 2006, at 27 (“Taking action to enforce trademark rights against infringers might be a major cost of doing business, but it is required under the law to maintain the integrity of the trademark.”).

86. Westenberg, *supra* note 23, at 85. A failure to police may result in the loss of the mark. *Id.*; see e.g., *Murphy Door Bed v. Interior Sleep Sys.*, 874 F.2d 95, 101–02 (2d Cir. 1989) (finding “Murphy Bed” to be a generic term and thus no longer a valid trademark in spite of *Murphy Door Bed's* unsuccessful attempts at policing the mark).

87. Wilcox, *supra* note 85, at 27.

88. Westenberg, *supra* note 23, 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—for example, Xerox running advertisements reminding the public not to use its name as a verb. See *id.* at 85 (noting that a trademark owner in such danger may wish to engage in advertising to request that the public use its mark properly).

acquirer should attribute little or no value to the mark in question.⁸⁹ Policing actions can range from simple letters, to agreements not to use the mark in a manner that causes confusion for the customers of either company, to legal action against infringers for damages and injunctive relief.⁹⁰ Increasingly, legal action against foreign counterfeiters will involve recourse to non-U.S. courts or the World Trade Organization.⁹¹

Even meritorious legal action can cause a backlash against the target in the “court of public opinion.”⁹² 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 trying to trample on the “rights” of a tiny company or individual.⁹³ Whatever the merits of any particular dispute, a company that reflexively responds to alleged infringement with legal demands or filings is likely to offend many potential customers in the marketplace, and may instigate counterclaims, putting its own mark at risk.⁹⁴ Such a situation may have just as much associated risk as doing nothing to police, and should be noted by the acquirer in its evaluation of the target’s marks’ value.⁹⁵ Of course, the possibilities of using such a campaign to respond to a pending infringement claim brought against a target that is a smaller company should also be considered along with the evaluation of traditional legal defenses.

2. Practice Assessment

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 by others in a confusing manner on unrelated or inferior goods.⁹⁶ 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

89. *See id.* (describing how a trademark owner may lose rights in the mark by the failure to police the trademarks).

90. *See, e.g.,* Wilcox, *supra* note 85, at 27 (noting the use of cease and desist letters when seeking to enforce trademarks).

91. *See generally* COMMENTS ON THE PRELIMINARY DRAFT CONVENTION ON JURISDICTION AND FOREIGN JUDGMENTS IN CIVIL AND COMMERCIAL MATTERS (2001), available at <http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/haguecomments.pdf> (providing copies of public comments received between October 2000 and January 2001 of a draft convention on online trade and commerce).

92. Wilcox, *supra* note 85, at 29.

93. *Id.*; Gwendolyn Bounds, *A Growing Dispute: Fertilizer Start-up Uses Web as Defense*, WALL ST. J., May 22, 2007, at B1 (discussing a Web-based public relations campaign waged by Terra Cycle, Inc. against Scotts Fertilizer’s trademark infringement claim).

94. OMS Investments, Inc. v. TerraCycle, Inc., No. 07-1064 (JAP), 2007 WL 2362597 (D. N.J. Aug. 15, 2007) (discussing how TerraCycle, an alleged infringer, responded to an infringement suit by another well known fertilizer company, with both a large Internet-based public relations campaign against the plaintiff and its own legal claims for false advertising and trademark invalidity).

95. Wilcox, *supra* note 85, at 28–29 (describing potential consequences of sending a cease and desist letter to a party using a company’s trademark without authorization).

96. *Cf. In re E. I. DuPont DeNemours & Co.*, 476 F.2d 1357, 1357, 1364–65 (1973) (holding that using trademark “Rally” for an automobile cleaner does not conflict with using “Rally” for an all-purpose detergent).

commercial vendor before pursuing a new mark of its own.⁹⁷ 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 may well be impaired and the target may be at risk for third-party infringement claims.⁹⁸ 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 apply the same type of analysis discussed above to the target's respect for the patent rights of others.⁹⁹ The acquirer should be comforted by the target's desire to avoid trademark disputes and its use of trademark search results to avoid potentially problematic activities and generally to mitigate risk of litigation. 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.

3. Procedural Considerations

Procedurally, the process should encompass cataloguing the target's granted and pending federal registrations with attention focused on the types of products for which the mark is registered and compared to the acquirer's anticipated use. The target's practice of paying continuation fees and associated calendar entries should also be noted, as should continued use of the mark itself.¹⁰⁰ The same analysis noted above for registration formalities of patents associated with an IP or line of business asset sale is also applicable here.¹⁰¹ Appropriate use of the ® and ™ symbols should also be addressed.¹⁰²

Trademark license documentation in both directions must also be reviewed, and the effect of the proposed acquisition assessed.¹⁰³ If licensees of the target's marks are noncompliant in their actual use of the mark, as opposed to payment obligations, this may constitute a failure to police that jeopardizes the mark.¹⁰⁴

97. Thomson and Thomson, probably the most prominent trademark search firm, advises on its Web site that its "In-Use Investigation Services" program "provide[s] the in-depth intelligence you need to assess potential infringement, to mitigate risk and to plan an effective protection strategy." Thomson Compumark, In-Use Investigation Services, <http://compumark.thomson.com/do/cache/off/pid/100> (last visited Nov. 18, 2008).

98. See, e.g., *Am. Ass'n for Advancement of Sci. v. Hearst Corp.*, 498 F. Supp. 244, 251–52 (D.C. Dist. 1980) (noting that no trademark search was performed prior to adoption of the infringing mark).

99. See *supra* Part III.A.3 (discussing key elements affecting exposure and recourse when patent infringement occurs).

100. 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. See Westenberg, *supra* note 23, at 83.

101. See *supra* Part III.A.4 (discussing procedural DD analysis for patents).

102. Westenberg, *supra* note 23, at 83–84.

103. "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." Julie Jargon & Aaron O. Patrick, *More Sweet Deals in the Candy Aisle?*, WALL ST. J., Apr. 29, 2008, at B1. Cf. Ziff, *supra* note 4, at 770 (suggesting that this analysis may dictate a different structure or request for licensor consent).

104. See generally MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 18:48 (4th ed. 2001) (discussing a licensor's duty to control and the perils of "naked licensing," which is equated to trademark abandonment).

As a result of the IP license exception for any trademark material to the target in section 365(n) of the Bankruptcy Code discussed above,¹⁰⁵ someone with financial expertise should obtain and review the financial statements of the target's licensor to help evaluate the likelihood and effect of a licensor bankruptcy on the target's operations.¹⁰⁶ If the licensor appears to be shaky, either a pricing adjustment or a back-up marketing plan may need to be considered.

C. Copyrights

For a long time a backwater issue with significance mainly in the literary and artistic fields, copyrights have gained greater commercial significance as a result of both the introduction of digital media and the rapidly increasing significance of Internet-based marketing.

1. Procedural Due Diligence

Few areas of legal and technological change have impacted DD practices as much as those associated with copyrights.¹⁰⁷ Traditional copyright analysis involves review and cataloging of the federal copyright registration forms filed by the target to determine if they are consistent with what has been disclosed by management. Additionally, there should be discussions as to whether either party is familiar with third-party duplication of such works (whether or not they are the subject of a filing).¹⁰⁸ Federal copyright filings are usually quite short.¹⁰⁹ 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.¹¹⁰

A related query is whether the target is in compliance with all of their copyright license agreements. Even for noncreative firms, there are likely to be some copyright license agreements for software. Even if a firm complies with its statutory obligations, it will still face liability if it fails to comply with its contractual, licensed obligations.¹¹¹

105. See *supra*, Part II.D (explaining that the bankruptcy code expressly precludes "rejection" of an IP license by a bankrupt licensor but excludes trademarks from the definition of IP).

106. See 11 U.S.C. § 365(n) (2) (stating that in exchange for the licensor's retention of its license rights, the licensor waives certain contract rights).

107. See, e.g., *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (applying a contributory copyright infringement theory to a file-sharing service); Complaint at 10, *Viacom Int'l Inc. v. YouTube, Inc.*, 2007 WL 774611 (S.D.N.Y. Mar. 13, 2007) (No. 1:07CV02103) (asserting YouTube profited from infringing files posted by its users).

108. 17 U.S.C. § 205 (2000).

109. See U.S. Copyright Office, Form CO — Application for Copyright Registration, available at <http://www.copyright.gov/forms/formco2d.pdf> (last visited Nov. 18, 2008) (consisting of a relatively simple eight-page form to apply for copyright protection).

110. 17 U.S.C. § 401.

111. E.g., *Wall Data Inc. v. Los Angeles County Sheriff's Dep't.*, 447 F.3d. 769, 781 (9th Cir. 2006) (holding that using copyrighted software beyond bargained for uses affects the market for the product).

2. “New Age” Substantive Concerns: The Need to Apply New Case and Statutory Law

a. Internal Use

The new capabilities provided by Internet and scanning technologies 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 that freely shares copyrighted reference materials (for internal use) by scanning or similar means¹¹² may face copyright infringement suits, even though it pays for the materials, because it exceeds the agreed upon usage limits.¹¹³ Likewise a copyright owner that acquiesces to such sharing without proper adjustment of its pricing is likely to miss out on significant revenue that it might have received had it insisted upon the purchase of multiple copies of the material.

In “borderline” cases, where material appears to have been shared in good faith and without an attempt to deprive the copyright holder of revenue, a “fair use” defense may be possible, even though good faith is not sufficient in itself for such a defense.¹¹⁴ While the literature associated with the fair use defense is voluminous and well beyond the scope of this Article, the four factors comprising such a defense are: 1) the purpose and character of the use, including whether such use is of a commercial nature or for nonprofit educational purposes; 2) the nature of the copyrighted work; 3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and 4) the effect of the use on the potential market for or value of the copyrighted work.¹¹⁵

b. Secondary Infringement Exposure Under the Digital Millennium Copyright Act

The rise of digital music and movies has facilitated the creation of many businesses that provide hardware, software, and services for such market. It has also prompted Congress to enact the Digital Millennium Copyright Act¹¹⁶ (“DMCA”) to provide a customized regulatory structure for this market. Many digital media offerings may pose a risk under these provisions, as well as “regular” copyright authority. If the target has operations involving digital music or movies, including the distribution of software that facilitates the copying of such material,¹¹⁷ the DD process must encompass the implications

112. This includes hard drive imaging. *Id.* at 779.

113. *See id.* 781–82 (holding that widespread use of hard drive imaging in excess of one’s licenses detrimentally impacts the market).

114. *See* 17 U.S.C. § 107 (enumerating the fair use criteria); *see also Wall Data Inc.*, 447 F.3d. at 778 (explaining the use of the fair use defense).

115. 17 U.S.C. § 107.

116. *Id.* §§ 501, 512 (setting limitations on liability for copyright infringement relating to online material).

117. *See Wall Data Inc.*, 447 F.3d at 786 (upholding judgment for developer against customer copyright infringer); *RealNetworks, Inc. v. DVD Copy Control Ass’n, Inc.*, No. 08-4548 (N.D. Cal. Sept. 30, 2008)

of recent (and pending) case law involving the DMCA. Even a company that is arguably not directly infringing a copyright but rather is facilitating someone else's infringement may face liability for "secondary infringement" of others under the Supreme Court's recent decision in *MGM Inc. v. Grokster, Ltd.*¹¹⁸

For anyone offering a product or service that purports to allow a consumer to avoid the copy protection, often referred to as "digital rights management," the DMCA makes them at least civilly liable for such action.¹¹⁹ Any target engaged in such business should be avoided, absent a colorable license claim or other recognized defense.¹²⁰ For companies producing devices that may be used in this manner, but that 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.¹²¹

More challenging is the situation of a target that allows consumers to share electronic files or to post their own content on an Internet message board for public access. While there is nothing inherently inappropriate about such services,¹²² there is the potential for misuse if they are used to disseminate

(describing the legal dispute relating to RealNetworks's software "RealDVD" that, when placed into a computer's DVD drive, looks up information about the DVD from Internet databases and stores an image of the copy-protected DVD to a computer hard drive); Complaint at 1, Universal City Studios Prod, L.L.P. v. Real Networks, Inc. (C.D. Cal. Sept. 30, 2008) (No. 2008 Civ 06412) (alleging that RealDVD "circumvents the technology measures that help enforce the prohibition" on copying a DVD).

118. 545 U.S. 913, 914–15 (2005). For more recent cases, pending and decided, see, e.g., Complaint at 10, Viacom Int'l Inc. v. YouTube, Inc., 2007 WL 775611 (S.D.N.Y. Mar. 13, 2007) (No. 1:07CV02103) (alleging that defendants directly profit from plaintiffs' copyrighted audiovisual works uploaded by users onto defendants' Web site); Complaint at 12, Universal City Studios Prod, L.L.P. v. Real Networks, Inc. (C.D. Cal. Sept. 30, 2008) (No. 2008 Civ 06412) ("Real offers to the public, provides, and/or otherwise traffics in a software product – RealDVD – that . . . is designed or produced for the purpose of circumventing CSS or the protection afforded by CSS . . .").

119. 17 U.S.C. § 1201.

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) As used in this subsection – (A) 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."

Id.

120. While the pending RealNetworks case should provide some guidance as to the meaning and application of this section, the fact that it was brought at all, especially given the license of Real to certain relevant technology, should give pause to anyone intending to distribute such a software product. RealNetworks, Inc. v. Streambox, Inc., No. C-08-5448, 2000 WL 127311, at *13 (W.D. Wash. 2000).

121. In *Sony Corp. of America v. Universal Studios, Inc.*, the Supreme Court permitted the production and sale of video recorders that allowed for both legal "time shifting" and prohibited dissemination of copyrighted material, but the language of section 512 of the DMCA arguably impacts this holding. *Sony Corp. v. Universal Studios, Inc.*, 464 U.S. 417, 456 (1984). The Supreme Court in *MGM Studios Inc. v. Grokster, Ltd.*, also shed light on the considerations associated with technology that can be used for legitimate and illegitimate purposes: "mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability," but "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps to foster infringement, is liable for the resulting acts of infringement by third parties." *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936–37 (2005).

122. 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." Posting of Ben Worthen to Wall Street Journal Business Technology Blog, <http://blogs.wsj.com/biztech/2008/05/08/> (May 8, 2008 13:54 EST) (commenting on a case where someone posted gyrating images

access to copyrighted content to persons who are not paying for it.¹²³ 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.¹²⁴

While there are relatively few companies that allow consumers to formally share files, those that do have been the subject of numerous legal challenges by copyright holders, many of which have been resolved in favor of the copyright holders.¹²⁵ Most notably, in the *Grokster* case, the Supreme Court made clear that any such service must demonstrate that it *actually* provides substantial noninfringing services in addition to its use for copyright infringement: "[W]e 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."¹²⁶ A mere theoretical possibility of lawful use will not suffice in the face of large-scale infringement and evidence of wrongful intent.¹²⁷

The pending case of *Viacom International Inc. v. YouTube, Inc.* 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 on the Internet, some of which will be infringing.¹²⁸ In this case, Viacom contends that YouTube's business model encourages users to post their own content for public consumption while selling advertising on their site.¹²⁹ All types of content find their way to the site from perfectly legitimate home videos to infringing movies, television shows, and music.¹³⁰ Viacom, a copyright owner alleges both direct and secondary infringement by YouTube, the Web site's operator.¹³¹

Even companies that merely invite public comment on their products, but allow such comments to include more than simple text, may face liability or at

on a site operated by the Epilepsy Foundation, which sickened some visitors to the site and prompted round the clock monitoring).

123. See, e.g., *Viacom Int'l. Inc. v. Youtube, Inc.*, No. 07 Civ. 2103 (LLS), 2008 WL 2627388, at *1 (S.D.N.Y. July, 2, 2008) (stating plaintiff alleged a copyright violation due to defendant's operation of a video-sharing Web site).

124. For example, as part of a contest, DibsFilmFest.com encouraged aspiring filmmakers during August 2008 to submit their own commercials for the Dibs ice cream novelty product, with winners available on YouTube. YouTube, Dibs1022's Channel, <http://www.youtube.com/user/dibs1022> (last visited Nov. 18, 2008).

125. See, e.g., *A & M Records, Inc. v. Napster, Inc.* 239 F.3d 1004, 1013-14 (9th Cir. 2001) (finding Napster infringed upon the plaintiff's copyrights).

126. *Grokster*, 545 U.S. at 919.

127. 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—one wonders how much of a legitimate use will have to be shown by defendants who are more discrete. *Id.* at 925.

128. See *Viacom Int'l Inc. v. Youtube, Inc.*, 87 U.S.P.Q.2d 1170, 1178-79 (S.D.N.Y. 2008) (indicating that the holding in *Grokster* that distributing a device with clear intent to infringe copyrights will hold the company liable for the actions of third parties will be very important to YouTube's defense, as well as the protections found in the DMCA).

129. *Id.* at 1172, 1177.

130. *Id.* at 1172.

131. *Id.*

least allegations of liability, if copyrighted content shows up on their site.¹³²

In section 512 of the DMCA, Congress sought to balance the competing interests that come into play when a user's posting of copyrighted content is unknowingly facilitated by a service provider.¹³³ While the exact meaning of the statute is still not clear, the DD process for any company that allows public posts should at least apply the major elements of this section in order to gauge the likelihood of a significant challenge.¹³⁴ In particular, a party that allows public posts and desires to avail themselves of this "safe harbor" 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
- "Expediently" take down, as soon as practicable, content that a copyright holder advises is wrongfully posted.¹³⁵

The statute does not expressly create a duty of inquiry by the Web site operator into whether the content is infringing, if no objection is received from a copyright holder.¹³⁶ The *Viacom* case, if it is not settled, may provide some guidance as to whether such a duty exists.¹³⁷

In the meantime, the DD process pertaining to any target that operates a Web site allowing public posts should include inquiries as to both the target's awareness of and compliance with the DMCA. This should include an inquiry into whether the target obtains any potential direct financial benefit from the dissemination of copyrighted material. If there is a lack of DMCA compliance, the target makes no effort to discourage submissions of copyrighted material, and the target does not use a common sense approach to flag postings of seemingly professionally prepared content—for example, a recognizable clip from a song, television show, or movie—there is reason for concern about potential claims following the closing. While there is no formal

132. 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 Posting of Ben Worthen, *supra* note 122 (providing an example of a post of comments on the Epilepsy Foundation's Web site containing flashing pictures that caused epileptic reactions for some viewers).

133. For example, section 512 illustrates this balancing by requiring site operators to designate an agent for receipt of complaints from copyright holders, but prescribes the contents of such complaints. 17 U.S.C. § 512(c)(2) (2000). To the same effect is the exculpatory language for operators who do not directly profit from infringing material and take it down when presented with appropriate notice. *Id.* § 512(c)(3).

134. *Id.* § 512(c)(1); Gerard N. Magliocca, *From Ashes to Fire: Trademark and Copyright in Transition*, 82 N.C. L. REV. 1009, 1052 (2004).

135. 17 U.S.C. § 512(c).

136. See *id.* § 512(c) (neglecting to specify a duty of inquiry, and instead declaring that a service provider shall not be held liable for infringement of copyright about which the service provider did not have actual knowledge).

137. See *Viacom Int'l Inc. v. Youtube, Inc.*, 87 U.S.P.Q.2d 1170, 1177 (S.D.N.Y. 2008) (noting, in the context of a discovery dispute, the central issue in the case: whether YouTube infringed Viacom's copyrights by allowing individuals indiscriminately upload videos copyrighted by Viacom onto their Web site for anyone to view).

authority to this effect, it seems logical to anticipate the law developing more stringent scrutiny of companies operating sites devoted to sharing user-generated-content as their business model, than for companies operating sites that simply invite comments on the company's product.

The acquirer should also be aware of developing technology that allows digital "fingerprinting" or "watermarking" of copyrighted material in order to facilitate its identification and restrict unauthorized display. While this technology is still in its infancy,¹³⁸ 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, it does not bode well for their compliance posture.

Given the last decade's radical changes in the legal and technological environments surrounding copyrights and those currently pending in court and in laboratories, for any target having relevant operations an essential element of the DD process is to ascertain, at both a conceptual and a technical level, whether the target has met its obligations under the law.

D. Trade Secrets

1. Legal Source and Summary

Unlike the other types of IP, this area is governed by state law, which makes the target company's internal practices involving sensitive information relevant and sometimes conclusive.¹³⁹ In at least forty states, the governing law is each state's version of the Uniform Trade Secrets Act and the cases construing it.¹⁴⁰ Thus, questions of whether particular material will be protected need to be addressed with reference to the law of the jurisdiction(s) in question.¹⁴¹ Also, unlike other IP, there is nothing filed with any governmental body.¹⁴²

Illinois, for example, defines "trade secrets" as:

information, including but not limited to, technical or nontechnical 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

138. Kevin J. Delaney, Brooks Barnes & Matthew Kamitschnig, *Policing WebVideo with "Fingerprints,"* WALL ST. J., Apr. 23, 2007, at B1 (noting that some companies were testing fingerprint technology on YouTube in April of 2007).

139. See, e.g., 765 ILL. COMP. STAT. 1065/2 (2006) (defining a trade secret as being the "subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.").

140. *Al Minor & Assoc., Inc. v. Martin*, 881 N.E. 2d 850, 853-54 (Ohio 2008).

141. 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. See WILLIAM M. RICHMAN & WILLIAM L. REYNOLDS, UNDERSTANDING CONFLICT OF LAWS 147 (2d. ed. 1993) (noting that courts handling disputes implicating different states must choose which state's law to apply). Even for the handful of states that have not enacted some form of the Uniform Act, there is still a body of statutory and case law to be considered.

142. 765 ILL. COMP. STAT. 1065/2 (defining "trade secret" but not requiring registration); THE TRADE SECRET HANDBOOK: PROTECTING YOUR FRANCHISE SYSTEM'S COMPETITIVE ADVANTAGE 12 (Michael J. Lockerby ed., 2000) (contrasting patent law and trade secret law, including details about the registration system of patent law).

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.¹⁴³

The Illinois statute also allows the owner to enjoin use by another, or recover damages for such use.¹⁴⁴ Examples of materials that can qualify for trade secret protection, if properly handled, include:

- Customer and prospect lists;
- Supplier lists;
- Employee lists;
- Product formulae; and
- Production process information or manuals.¹⁴⁵

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 not otherwise protected by a patent, trademark, or copyright.¹⁴⁶ Traditional analysis focuses on physical steps taken to maintain secrecy such as keeping putative trade secrets in locked file rooms and cabinets while restricting access to such areas to employees and other persons with a “need to know.”¹⁴⁷ While this is still the correct starting point, in today’s world of cheap, portable, electronic storage and communication, it is hardly sufficient.

2. *Impact of New Technology*

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?¹⁴⁸

143. 765 ILL. COMP. STAT. 1065/2.

144. *Id.* § 1065/3-4.

145. *Cf.* *Minn. Mining and Mfg. Co. v. Pribyl*, 259 F.3d 587, 596 (7th Cir. 2001) (stressing that even a compilation of public materials can qualify if it is properly handled).

146. 765 ILL. COMP. STAT. 1065/2.

147. *See generally* Roman A. Klitzke, *Trade Secrets: Important Quasi-Property Rights*, 41 BUS. LAW. 555 (1986) (discussing the need of the trade secret holder to take affirmative, yet reasonable, steps in maintaining the confidentiality of the trade secret, whether through physical means of restricting access to the secret or limiting disclosure of the contents of the secret). While this article pre-dates the vast technological changes that have occurred in recent years, the legal principles are still applicable but must be extended to encompass both physical and electronic security considerations.

148. Some stress the need for formal policy regarding the use of new media and proper exit interview inquiries and admonitions about downloading, use of sensitive materials, and formal imaging of the hard drives of departing employees with access to the most sensitive materials, in order to trace the activities of

Extremely sensitive material that may be used in identity theft or other fraud must be kept and transmitted in encrypted form *at all times*.¹⁴⁹ An example of this would be material containing personally identifiable information (“PII”) of employees, customers, or employees of customers—for example, social security numbers, credit card numbers, or drivers license information. The DD team must also ask questions such as: To what extent does the target deal with the public, and who is issued electronic devices that can be misused in this manner?

Both formal written policies in dealing with these materials and their application in practice are relevant.¹⁵⁰ Equally relevant is the target’s history in these matters. If the target has experienced several instances of alleged misappropriation that have led to competitive harm or litigation with former employees, consultants, and the like, there is probably something wrong with its practices or policies.

3. Target Human Resources Procedures

The firm’s dealings with its employees are also critical to this analysis in several respects. First, it is essential that employees having anything to do with sensitive material, including the use or development of IP, execute written nondisclosure agreements. These agreements should acknowledge 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 contracts should also contain an express representation that the employee is not bringing to their new position, and will not utilize in the performance of their duties, any trade secrets or materials that if utilized would infringe upon the IP rights of anyone else.¹⁵¹

Organizations can become vulnerable to claims brought by an employee’s former employer. These claims may allege 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.¹⁵² It is essential that

such employees if necessary in litigation. Bradford K. Newman, *Protecting Trade Secrets: Dealing with the Brave New World of Employee Mobility*, 17 BUS. L. TODAY 22, 25 (Nov.-Dec. 2007).

149. Joseph Pereira, *Credit-Card Security Falters*, WALL ST. J., April 29, 2008, at A9 (describing a major security breach where encrypted customer personal data was stolen, with significant financial losses for a grocery chain).

150. A recent case illustrating the practical consequences of “loose” practice is *Al Minor & Associates, Inc. v. Martin*, in which an individual had access to the plaintiff’s customer list, did not sign an employment contract or noncompete agreement (and possibly did not sign a confidentiality agreement), left the company and went into competition based solely on his recollection of the customer list. *Al Minor & Assoc., Inc. v. Martin*, 881 N.E.2d 850, 851 (Ohio 2008). While the Ohio Supreme Court ultimately sided with the employer, the fact that the case got that far indicates the advisability of making explicit what is expected of employees. *Id.* at 855.

151. This would encompass all forms of materials—paper, electronic, or memorized. See *id.* (indicating that in many (but not all) states, trade secrets can be misappropriated solely through memorization).

152. See, e.g., *Atl. Mut. Ins. Co. v. Badger Med. Supply Co.*, 528 N.W. 2d 486, 488 (Wisc. Ct. App. 1995) (discussing plaintiff’s allegation that the new employer persuaded employee to leave plaintiff’s

the new employer be able to demonstrate its good faith in hiring; obtaining these representations as part of the employment application or contract is one way to do so.¹⁵³ If the target's practices do not include these measures, 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 nondisclosure agreements when confidential material is shared with anyone, such as customers, prospects, or suppliers.¹⁵⁴ Ignoring the need for confidentiality and discretion in such relationships is likely to be just as problematic as in the employee-employer relationship.

IV. INFORMATION TECHNOLOGY

It is not intuitively apparent why this topic is addressed in the same breath as IP, however, there are two reasons for doing so. First, in practice, it is often the case that some people on the DD team are asked to address both. Second, a great deal of the software used for IT operations is licensed pursuant to agreements of the sort 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.¹⁵⁵ Of course, such consequences are likely to be accompanied by major litigation and potential governmental sanctions, not to mention adverse publicity.¹⁵⁶ In addition, a security breach that impacts the integrity of material will also be operationally disruptive. For example, a deletion or corruption of a customer list, inventory schedule, pending accounts receivable, or payable information will disrupt

company and induced the employee to divulge customer contacts).

153. Many litigated cases in this arena involve and even turn on the availability of equitable remedies, such as injunctions, with respect to which the parties' good faith or absence thereof is of great significance. Victoria A. Cundiff, *Preventing the Inevitable: How Thinking About What Might Happen Can Help Ensure that It Won't*, 947 P.L.I./PAT. 759, 776–79 (2008).

154. See John S. Dzieńkowski & Robert J. Peroni, *Multidisciplinary Practice and the American Legal Profession: A Market Approach to Regulating the Delivery of Legal Services in the Twenty-First Century*, 69 FORDHAM L. REV. 83, 191 (2000) (discussing how the "Big Five" accounting firms recognize the need to protect IP and have begun requiring prospective clients to sign nondisclosure agreements). See generally *Mangren Research & Dev. Corp. v. Nat'l. Chem. Co.*, 87 F.3d 937, 943 (7th Cir. 1996) (holding that efforts to protect confidentiality can create a trade secret).

155. E.g., Plaintiff's Original Petition, *Waste Mgmt., Inc. v. SAP AG*, No. 2008-17510 (Tex. Dist. Ct., 2008) (demanding damages in excess of \$100 million for problems encountered by a major corporation stemming from a failed SAP implementation).

156. E.g., *In re TJX Co.*, No. 072-3055 (F.T.C. Mar. 27, 2008), available at <http://www.ftc.gov/os/caselist/0723055/index.htm> (ordering TJX to implement or establish an information security system designed to protect the security information collected about customers and a twenty-year consent decree with the Federal Trade Commission, requiring extensive and burdensome third-party monitoring).

operations, even if no third party is impacted and no litigation ensues.¹⁵⁷

A. Information Security

1. Importance

As a result of growing social and legal concerns over individual privacy, this topic has emerged as a strategic priority for lawmakers, commentators, regulators, and enlightened corporate managements.¹⁵⁸ Information security should therefore be the first part of this phase of the DD review. As usual, there should be an informal discussion with target management to understand and evaluate its commitment to the topic and its 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. The objective of this inquiry should be a so-called “SAS 70” report from a recognized provider such as a major accounting firm.¹⁵⁹ Such reports have come to prominence in response to the Sarbanes-Oxley Act of 2002, and are often used as a key part of the financial audit and internal controls report.¹⁶⁰ If a recent SAS 70 report exists (without material qualification), it should go a long way toward assuring the acquirer that it is not walking into a hornet’s nest. If no such report exists there is reason for concern, especially if the target is of any significant size or has large or public clients. The absence of an SAS 70 report increases the likelihood of customer or employee claims, or the emergence of unhappy customers or employees post-closing. Without a recent SAS 70 report, the acquirer should, at the very least, plan on promptly spending time and money to bolster the target’s practices and infrastructure.

2. Process Review

With or without an SAS 70 report, the DD process should also extend to the specific devices and processes that the target uses to maintain security. Special emphasis should be placed on the security of customer or employee

157. See *Waste Mgmt.*, Plaintiff’s Original Petition at 15–18.

158. E.g., Julie E. Cohen, *Privacy, Visibility, Transparency and Exposure*, 75 U. CHI. L. REV. 181 (2008) (concluding that transparency and exposure both visual and informational, especially in our Internet era, have harmed privacy laws); Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203 (2008) (discussing the tension between the desire for security in protecting against credit card identity fraud and the desire for privacy, such as anonymity in transactions).

159. About SAS 70, <http://sas70.com/about.htm> (last visited Nov. 18, 2008).

160. 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.” *Id.* SAS 70 reports come in two flavors, type I and type II, with the type II report involving additional work by the reviewer. *Id.* The underlying standard used for evaluation of security practices is promulgated by the International Standards Organization in standard 17799, codified and restated in standard no. 27001. See generally ALAN CALDER & STEVE WATKINS, INFORMATION SECURITY RISK MANAGEMENT FOR ISO 27001/17799 (2007) (describing the standards used for evaluation).

personal information, as well as PII.¹⁶¹ While any company or individual can be victimized by a hacking incident, the problem is most acute with companies with large-scale dealings with the general public or companies that maintain large volumes of employee data.¹⁶² This inquiry should start with evaluation of physical security of facilities, areas where sensitive material is kept (including movement of physical media such as tape cartridges),¹⁶³ and individual access rules, but should also extend to more technical matters such as:

- Use of commercial grade, mainstream hardware firewalls, and their settings;
- Encryption of stored or transmitted data, especially when it resides on laptop computers or involves PII. This is especially true where the target is governed by special obligations associated with health care or financial services;¹⁶⁴
- Purging of data when no longer needed;¹⁶⁵
- Use of mainstream antivirus software;
- Special handling for wireless transmissions of PII or other sensitive material;
- Requirement for alpha-numeric passwords of at least six to eight characters and varying cases, for network access, with expirations of no more than ninety days;
- Disaster recovery vehicle with off-site facilities;¹⁶⁶
- Rules and procedures for prompt incident reporting;¹⁶⁷

161. An excellent definition and description of the term “personal information” that is often used interchangeably with “PII” is contained in the FTC’s Order involving TJX. *In re TJX Co.*, No. 072-3055 (F.T.C. Mar. 27, 2008).

162. See generally Steven Marlin, *Banks Scramble to Contain Damage from CardsSystems Hacking Incident*, INFO. WEEK, June 22, 2005, <http://www.informationweek.com/news/management/showArticle.jhtml?articleID=164901831> (discussing the infiltration of a major credit card network).

163. Several security breaches have involved media literally falling off trucks. JON OLTSIK, ENTER. STRATEGY GROUP, *TAPE LOSS AND DATA THEFT: MYTH AND REALITY* (2006) (discussing such issues during 2005 at Bank of America, Citicorp, and Marriott Vacation Club).

164. See, e.g., Gramm-Leach-Bliley Financial Modernization Act, 15 U.S.C. §§ 6801–6809 (2000) (mandating the protection of nonpublic personal data by financial firms).

165. 16 C.F.R. §§ 682.1–682.5 (2008) (taking the company to task for “retaining too much information for too long.”); OFFICE OF PRIVACY COMM’R OF CAN. & OFFICE OF THE INFO. & PRIVACY COMM’R OF ALBERTA, *REPORT OF AN INVESTIGATION INTO THE SECURITY, COLLECTION & RETENTION OF PERSONAL INFORMATION* (2007) [hereinafter CPC REPORT], available at http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp.

166. New York Stock Exchange Rule 446 is applicable at a minimum to NYSE member firms, and possibly to all listed companies. NY STOCK EXCH. R. 446 (2008) (incorporating by reference National Association of Securities Dealers Rules); NAT’L ASSOC. SEC. DEALERS R. 3510, 3520 (2008) (listing specifications for Business Continuity Plans).

167. See CAL. CIV. CODE §§ 1798.80–1798.84 (West 1998) (illustrating the most prominent and probably the most significant of the many state statutes requiring prompt reporting to the public of any breaches, since it impacts all companies with California operations); Scott Berinato, *CSO Disclosures Series: Data Breach Notification Laws, State By State*, CSO, Feb. 12, 2008, http://www.csoonline.com/article/221322/cso_disclosure_series_data_breach_notification_laws_state_by_state (providing a summary of thirty-eight state reporting laws).

- Rules and procedures for meaningful employee background checking for those with access to sensitive material. This is important to screen out persons with a history of identity theft, virus dissemination or other disreputable or fraudulent activity;
- Use of commercial grade intrusion detection products; and
- Rules for disabling of employee/contractor system access upon termination.¹⁶⁸

Special attention must be paid to target Web sites that facilitate public transactions (e-commerce) and that are likely collecting sensitive information. Targets operating such sites should not only have good security in fact but more critically also live up to any public statements that they have made concerning their security.¹⁶⁹ Third-party Web site hosting agreements should be reviewed with an emphasis on initial and ongoing provision of an SAS 70 report for the third-party host.

Material deviations from mainstream practices must be discussed with respect to not only integration but also pricing and whether to proceed at all. Factors such as the target's exposure to liability, pending or probable major claims against it, or a culture that places too little emphasis on the topic should weigh against deal closure.

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 contracts 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 the substance of the agreement, as well as the likelihood of successful remedy in the event of a breach—as opposed to merely ensuring that there is a provision providing for appropriate remedy.¹⁷⁰

A public company acquiring a private one needs to be especially cognizant of this issue. The author has observed many capable private company managements that are (justifiably) unfamiliar with the enhanced security obligations of public companies under Sarbanes-Oxley.¹⁷¹ Consequently, many well-run private companies are fundamentally unprepared for public company integration, and will require substantial investment in

168. While the rapid pace of change in this field means that there is no codification of such requirements, they are based upon not only the author's interaction with information security professionals in the course of his practice, but also the recommendations of the Canadian Privacy Commission and the excellent Federal Trade Commission handbook for businesses. CPC REPORT, *supra* note 165; FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, <http://www.ftc.gov/infosecurity> (last visited Nov. 18, 2008).

169. *In re DSW Inc.*, Case No. 052-3096 (F.T.C. Mar. 7, 2006), available at <http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf> (finding DSW did not securely store credit card information and requiring it to develop a security program); *In re BJ's Wholesale Club*, 140 F.T.C. 465, 470–71 (2005) (ordering BJ's, a company collecting credit card information, to establish a comprehensive security program).

170. See, e.g., Scott Hewett, *Section 337 and the WTO: Can GATT Panel Precedent Predict the Future?*, 3 U.C. DAVIS J. INT'L L. & POL'Y 57, 73 (1997) (finding that where a court is unable to attach property, an injunction would be ineffective).

171. See Newman, *supra* note 148, at 26 (stating trade secret practice is a fundamental element of Sarbanes-Oxley compliance).

infrastructure, training, and staff to comply with any cited International Organization for Standards (“ISO”) standards, obtain an SAS 70 report, and otherwise function properly in the public arena.¹⁷² It should also be noted that European consumer privacy standards are uniformly more stringent than those of the United States, so that any M&A transaction that will cause a U.S. company to have a significant European consumer presence will require additional scrutiny under European Union standards.¹⁷³

Information security 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 only a limited body of “law” in the traditional sense to use when testing target methods and practices.

However, it is clear from cases such as *In re TJX Companies, Inc.*, that after the fact assessment of liability for a problem looks to what technology was available at the time to prevent it.¹⁷⁴ 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.

B. Other IT Issues, Operational Assessment

A related topic to security, but involving different considerations is system performance. An evaluation of system performance is particularly important with respect to Web-based applications and other public Web sites used as part of the sales or marketing process. The focus of this evaluation should be on whether the target has the required, sufficient hardware and software infrastructure to handle its business with reasonable dispatch, both before and after integration 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” completely in the face of excessive demand and without adequate load-balancing or backup systems.¹⁷⁵

172. See About SAS 70, *supra*, note 159. ISO standards are widely used and cited. See International Organization for Standardization, ISO Standards, http://www.iso.org/iso/iso_catalogue/catalogue_tc.htm (last visited Nov. 18, 2008) (providing a list of covered fields).

173. Council Regulation on the Control of Concentrations Between Undertakings No. 139/2004, 2004 O.J. (L 24) 1 (EC), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:024:0001:0022:EN:PDF>.

174. The Canadian Privacy Commissioner noted that while TJX did encrypt customer PII after its collection prior to its wireless transmission, it did so using as the older 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. CPC REPORT, *supra* note 165. The Information and Privacy Commissioner for Alberta stated when such report was released, “[w]hen the technology exists to protect data, we expect companies to move quickly to adapt that technology.” Robert Westervelt, *TJX Should Have Had Stronger Wi-Fi Encryption, Say Canadian Officials*, SEARCHSECURITY.COM, Sep. 25, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1273889,00.html.

175. Katherine Nguyen, *The Secret's Out*, OC REGISTER, Dec. 4, 2006, http://ocregister.com/ocregister/life/homepage/article_1371295.php (explaining the most famous—or infamous—example being the Victoria’s Secret 1999 Super Bowl commercial, which drove so much traffic to its site that the site “crashed”).

The acquirer's IT management must closely examine the target's technical capabilities in relation to its anticipated demand. Some examples of these technical capabilities are Web servers, database and application server software, storage, network bandwidth, load balancing capability, as well as internal practices. A publicly accessible system that crashes amidst a major promotion will undermine the target's market position for a long time.¹⁷⁶ Both lawyers and IT management should review any agreements, including Service Level Agreements ("SLAs") with third-party service providers that "host" such sites. This review should also include a review the providers' infrastructure.

A more procedural but equally essential part of the DD review is an assessment of the target's general IT approach and capabilities to see if they are in accordance with accepted industry practices and the acquirer's approach without a great deal of retrofitting.¹⁷⁷ If the acquirer can live with any retrofitting hardware or software costs that are necessary, then a plan to upgrade the target's systems should be generated.

Most fundamental, in the author's experience, is the question of whether the basic hardware and software relied upon by each organization is reasonably current, and how difficult it will be to make the organizations' computers to talk to each other. If one company relies on a state of the art IBM mainframe or minicomputer (AS-400) hardware and the other on a Sun or even on older IBM hardware, problems may result. Similarly, if one relies on 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 on "software as a service" with major applications accessed at a third-party vendor's Web site, integration may be difficult and costly.¹⁷⁸

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-400s with the customary MVS operating system while the other uses UNIX as its main operating system, integration may be more costly. 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.

176. *Id.* The fact that the Victoria's Secret 1999 episode was still being discussed online in 2006 is indicative of the lasting effects from such crashes.

177. *Information Technology: Best Practices Can Improve Performance and Produce Results: Testimony Before the Subcomm. on Government Management, Information and Technology, H. Comm. on Government Reform and Oversight*, 104th Cong. 1-18 (1996) (statement of Christopher Hoenig, Director, Information Resources Management Policies and Issues Accounting and Information Management Division), available at <http://www.gao.gov/archive/1996/ai96046t.pdf> (arguing that executives should be aware of a company's IT approach).

178. Vincent Ryan, *A Place in The Cloud*, CFO, Sept. 1, 2008, at 31 (providing an objective assessment of the pros and cons of such models, sometimes referred to as forms of "cloud computing"). The author explains that potential savings in fixed costs must be weighed against potential performance and security limitations. *Id.* If a target relies on this model for its basic IT capacity, the acquirer should approach the situation with a very critical eye.

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 may insist upon being early adopters. Version numbers must be compared and differences evaluated.

Additionally, if the integration of the two companies involves sharing data between companies' systems—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 is required.

The acquirer's IT management must be intimately involved in the DD process and “get their hands dirty” at a level of detail sufficient to determine whether a good fit exists from a technical perspective. 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, an inquiry must be made as to known compliance/noncompliance and third-party vendor challenges as well as mechanisms in place to facilitate compliance.¹⁷⁹ Organizations that rely upon “cute” technical practices to avoid or circumvent contractual use limitations can expect to encounter costly consequences. These consequences may involve damages, attorney's fee awards and even enjoined use.¹⁸⁰ Practices and awareness involving shrink-wrap and open source code should also be assessed.¹⁸¹

A software license compliance problem is not usually enough to justify reconsideration of a deal, but it may have pricing implications if there appears to be a good deal of exposure to liability. It may also 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 may be canceled for cost savings.

The software license inquiry should also extend to whether the license agreements contain language under which the acquisition itself may constitute a breach or trigger additional payment obligations, even if the target is

179. John Edwards, *Thumbscrew 2.0*, CFO, Feb. 1, 2008 (discussing how software vendors have started “aggressive policing of current licensing agreements” as part of a program to maximize revenues).

180. See generally *Wall Data v. Los Angeles County Sheriff's Dep't.*, 447 F.3d 769 (9th Cir. 2006) (involving a vendor's successful effort to recover damages and attorney's fees for the efforts of the Los Angeles County Sheriff's Department, which licensed a product subject to a limit of about 3,500 users but installed it on about 6,000 computers, with a mechanism to prevent its concurrent use by more than 3,500 users).

181. See discussion *supra* Part II.C (discussing the General Public License documents that generally limit the use of open source software).

otherwise in compliance. At the minimum, the target may have to provide the vendor with written notice of the transaction.

Unrelated and seemingly mundane but important considerations are the terms of any leases for IT hardware. If such leases are noncancellable or nontransferrable for their stated terms, this may affect any potential short-term savings that might be realized from integration of two firms' IT functions.¹⁸² Such leases often contain onerous terms governing equipment return, purchase, or lease extension, and can require significant management to make illusory some of the anticipated savings from integration. For these reasons the DD process should also involve a review and cataloging of the target's hardware leases. The acquirer should have a full understanding of the lease terms, including the nature of the financial commitments, required end-of-term termination notices, end-of-term purchase requirements, and any other required conditions for return.

V. CONCLUSION

While the M&A process always involves significant business risk and its outcome is susceptible to macroeconomic factors that 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 that 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.

182. See, e.g., *Wells Fargo Bank Minn. v. BrooksAmerica Mortgage Corp.*, 419 F.3d 107 (2d Cir. 2005) (finding that Bank of America's contract for a sale-leaseback transaction of computer equipment was noncancellable and held them responsible for all rental payment due under the contract); *AT&T Credit Corp. v. Transglobal Telecomm. Alliance, Inc.*, 966 F. Supp. 299 (D.N.J. 1997) (discussing the breach of lease for telephone equipment by lessee Transglobal and finding them liable for damage in the amount of the lessor's return including delinquent rental payments and all rental payments due).