

Practitioner's Perspective

by Holly K. Towle, J.D.



Holly K. Towle is a partner with Kirpatrick & Lockhart Preston Gates Ellis LLP (K&L Gates), an international law firm, and chair of the firm's E-merging Commerce group. Holly is located in the firm's Seattle office and is the coauthor of *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons). Holly.Towle@KLGates.com, 206-623-7580.

Merger & Acquisition Due Diligence in an E-Information Age

The importance of due diligence ("DD") reviews is no secret. Companies learned hard lessons long ago about acquiring or merging with other companies before finding out relevant details about the target company, such as what leases are non-assignable and what loan defaults can be triggered by a change in control. The only way to discover those details and discern their impact on the target's value is to review selected contracts and documents of the target (such as the lease and loan contracts), and that is just what the DD team does. With the advent of the information age, intellectual property rights and software licenses emerged as significant assets of many businesses. More people were added to the DD team in order to ensure that those more exotic rights would not be lost or changed in the transfer. Even today, DD teams struggle to make intellectual property due diligence sufficiently robust (*e.g.*, adding reviews for open source software and its potential "viral" effect).

DD teams also struggle to cover emerging issues. One of those is what I will call "Non-Intellectual Property/Electronic" due diligence ("E-DD"), and it is the focus of this article. Although intellectual property issues remain important, in E-DD the focus is on information that tends *not* to enjoy intellectual property protection (such as data) and on issues arising from doing business electronically such that computer information is created, collected, held, used, or discarded. Numerous new laws create a need for E-DD because they can influence the target company's value as much or more than the subjects of traditional DD and intellectual property DD.

Simply increasing the scope of a DD review is not the solution. The new laws governing business done electronically (in whole or part) and the information age itself, require: (i) taking another look at some of the fundamental premises of typical merger and acquisition agreements and revising them in small but important ways; and (ii) altering DD procedures to incorporate review of additional issues. Here are a few examples.

1. **Is the wording of the acquisition agreement now unclear?** In most acquisition agreements the target represents that it is qualified to do business in all jurisdictions in which it currently does business and/or in listed jurisdictions. That used to be a fair question that could be answered with reasonable certainty, *i.e.*, the business could decide where it had people, assets, offices, and stores etc. and get pretty close to an accurate answer notwithstanding variations in state or country laws regarding what constitutes "doing business."

With the pervasive use of the Internet where the “corner drug store” can do business globally in over 160 countries and 50 U.S. states with varying laws, such accuracy is more difficult to achieve. A first question is whether the traditional representation even encompasses Internet operations, *e.g.*, would a judge readily interpret acquisition agreement language used pre-Internet to cover Internet operations? A second question is whether, when, and to what extent it is appropriate to require a representation encompassing the Internet? For example, can a target doing business on the Internet reasonably make a representation given the uncertainty of the legal analysis and varying answers that can be supplied to the question of where it is “doing business”?¹ An acquiring party’s demand for a blanket representation may overreach in this context; but targets that have not previously considered the issue will have more troubles ahead than determining how to make an accurate representation. Of course, addressing the question may or may not be important, *e.g.*, the target’s Internet operations might not be material, or it might be difficult to obtain or enforce judgments against the target in other countries, or the target might not have any assets in other countries to seize. Any analysis will change with changes in laws and treaties and E-DD should be scaled appropriately for the circumstances and levels of risk. In any event, however, clarification of the acquisition agreement may be advisable.

2. Is the acquisition agreement wording outdated? Most agreements focus on tangible “property” concepts, yet many items that are important in an information economy are not tangible and some are not even “property.”² This is not a new concept. As intellectual property rights became as or more important than brick and mortar assets, agreements made the shift from focusing on tangible property—“sales,” “leases,” “ownership,” and “title”—to dealing with “licenses” and intangible property rights. But vestiges of too-restrictive language remain in most agreements even as to intellectual property rights, and few fully contemplate E-DD issues.³

For example, when a consumer “opts into” receiving direct marketing e-mails, the resulting customer list may be important in the deal but it is not necessarily a “contract” or “property” and is not an intellectual property “right.” It may simply be a non-contractual permission or consent or waiver of a new right, and the question is whether the acquisition agreement is worded to address such rights and other E-DD concepts? Another illustration concerns use of the word “infringe.” If the agreement has the target warrant that it does not “infringe,” that may work fine with respect to intellectual property rights, *i.e.*, one “infringes” a copyright, a patent and a trademark. But if the target has been sending electronic robots to gather data from third party websites in violation of the terms of use for those sites, that can be a “trespass” under current

law but is it an “infringement”?⁴ Similarly, if a clause requires submission of “material contracts,” will that clause require submission of a non-contractual privacy policy that is material to the transaction? The point is that use of terminology relevant to the target, or relevant in an electronic information age generally, is preferable.

3. What E-DD laws are we talking about? There are too many laws and potential applications to address here, so here are two illustrations:

- Assume an acquirer is valuing the target in part for its customer list at X amount per customer; acquirer intends to use the list to send marketing materials touting the enhanced services available from the merged entity. The target has warranted that the number of customers is accurate, which it is. But *having* customers is not the same, any more, as being permitted to send marketing e-mails to them. In an increasing number of settings, customers may “opt-out” of receiving materials by e-mail and companies possessing lists are obligated (by law or their privacy policies) to track those customers who do so for a number of years to ensure that they do not receive further emails.⁵ If the DD process ignores this issue, the acquiring party may pay for something it is not really getting (and, perhaps, allocate to much value for tax, accounting, and other purposes to the list⁶). Even if an acquirer obtains a representation and warranty that would have been satisfactory in the past, new laws and rules may undermine its value. In fact, one division of the target might not be telling another division about opt-outs; no one at the target may be minding the store with a central list; and systems to track the list for the required number of years may be nonexistent or inadequate. It is not simple or inexpensive to design an adequate tracking system, so it should not be surprising if a target does not have one.
- Assume that the target company stores credit card numbers for the convenience of customers, *i.e.*, so that they do not have to repeat the card information to telephone operators or re-enter information on-line. While this used to be common, modern credit card processing contracts likely prohibit at least retention of the card number. If the target is keeping the numbers, in addition to breach of contract it may also run afoul of new rules and heavy fines by credit card processors upon any breach of information security. These can include annual audit obligations and increased transaction fees, all of which will increase operational costs and, perhaps, create second thoughts about the acquisition price.

In addition to the contractual point, there is new law, or at least new claims, affecting the ability of companies to keep credit card numbers. The FTC recently alleged that failure of a business to abide by its credit card processing contract, and

the business' retention of credit card data too long, were part of other factors amounting to inadequate security practices and an unfair act.⁷ Although the FTC's basis for bringing that action can be questioned, there are other laws that can apply in particular circumstances. For example, numerous new state laws require notice to affected customers when there has been a breach of information security.⁸ The infamous "ChoicePoint" incident made headlines in February 2005 when ChoicePoint provided notice that it had been duped into selling personal information of almost 145,000 people. It made this disclosure under a 2003 California law (which recently has been followed by non-uniform legislation in at least 17 more states) more than eight months after the breach occurred. While delay can also be a violation, had ChoicePoint been an acquisition target during this period, asking whether it had suffered any security breaches as part of E-DD might have elicited important information. Once the announcement of the incident was made, the ChoicePoint stock lost 1.3% the next day, fell nearly 14% the next week and as of June 2005, was still down more than 12% from the day of disclosure.⁹

4. Won't a representation regarding compliance with all applicable law solve all of this? In an E-DD context, such a representation isn't very helpful for at least two reasons.

First, it may provide legal recourse against a non-compliant target, but that is not the primary goal of DD. The usual goal is to find out what material problems might exist *before* the transaction is completed and, therefore, be able to fix them or assess their impact on the value of the target. To achieve that goal, DD questions should be more specific. Many targets (and many acquirers) do not even know the new laws exist or do not realize the extent to which they impact the target's operations and/or the operations of the post-target company. In that setting, unless specific representations are explored in the DD exercise, the necessary information might not be elicited.

Second, many of the new laws do not *require* anything so cannot be violated—they simply create material *consequences* if the law is ignored. Thus, a target could accurately represent that it is not in violation of law while still being at risk under it. For example, assume the target has a website where customers make contracts (*e.g.*, agree to terms of use or order goods under stated terms that are agreed as part of the ordering process). Those are electronic records and several state and federal laws will affect the records simply because they are electronic (*i.e.*, these laws do not exist for paper records).¹⁰ For example, under federal law e-records *may be denied legal effect, validity or enforceability* if they do not meet federal rules regarding electronic records. There is no "violation" of law if

the rule is not met—the record may simply be susceptible to *challenge*.¹¹ The point is that the target might not have the enforceable or valid contract or other record that it thinks it has—instead, it may have contracts and records that are subject to challenge because that is a consequence of, but not a requirement of, not meeting the new e-rules. Had the acquirer sought a specific representation regarding electronic records and done some E-DD regarding them, it might have paid less for the contracts or added "fix e-records and procedures" to its post-merger to-do list.

5. What's best: due diligence or a mere representation?

"Mere" is a tip-off to my views on the answer to that question, *i.e.*, some of the E-DD liabilities and issues tend to create an affirmative need to investigate instead of relying on representations (depending on the circumstances, of course). Engaging in E-DD is increasingly critical as the legal (and business) risks associated with data and doing business electronically increase. For example, in modern practice a mismatch between privacy policy text and privacy practice,¹² or a failure adequately to protect personally identifying information,¹³ may present greater liability or reputational risk and business disruption than many issues examined in traditional due diligence.

6. What about the lawyers—if they revise the agreement and expand due diligence appropriately, is that all there is to it?

No. Anyone who has been through a merger or acquisition transaction knows that the acquiring party's lawyers need to understand and explain why they have requested a representation or required production of certain material, or their client may be viewed as overreaching and possibly undermine any necessary post-transaction relations. Lawyers for the target have to understand the flip side, *i.e.*, they need to be able to point out why the request is unreasonable, overbroad or irrelevant in the circumstances. To engage in this dialogue, one needs to understand the laws behind an E-DD representation or request and be able to adjust the request according to the actual needs and circumstances. It is unreasonable to expect the merger and acquisition lawyers to find, read, understand, and keep up with all of the new and ever-proliferating laws impacting business done electronically, so the better approach is to engage in educational and training efforts with them and even the client (*e.g.*, how much patience will a client have for a request made by its own side when the client doesn't understand the reason for the request?).

If the foregoing reasons for engaging in educational efforts is not enough, consider the fact that the lawyers and clients may, themselves, violate some of the laws relevant to E-DD because of their lack of education.

See a report by the Canadian Privacy Commissioner at <http://www.oipc.ab.ca/home/DetailsPage.cfm?ID=2076> for an example. The law firms in an acquisition posted too much information in the Canadian equivalent of the U.S. "EDGAR" public filing system which requires posting of all material contracts of the relevant company. A schedule containing personal information (employee names and social security numbers) was posted even though the data was not required for the transaction. The result was a violation of the Canadian Privacy Act and imposition on the law firms and clients of training and procedural requirements, including the appointment of privacy officers.

As should be obvious by now, both concepts, details and the nature of the target, as well as an understanding of the relevant laws relevant to E-DD concepts, are necessary in order to conduct E-DD effectively. One place to start, however, is by updating acquisition agreements and considering changes in the focus of due diligence procedures.

Footnotes

- ¹ See Holly Towle and Raymond Nimmer, *The Law of Electronic Commercial Transactions* (hereafter "*E-Commercial Law*") at Chapter 7.09 (A.S. Pratt & Sons 2003-2005)(explanation of the various tests used by courts to determine general and specific personal jurisdiction issues regarding websites). Although a "personal jurisdiction" analysis differs from a "doing business" analysis, uncertainty with one tends to indicate uncertainty for the other.
- ² See *e.g.*, *E-Commercial Law* at Chapter 7.07(case law regarding domain names as seizable—or not—property).
- ³ For a discussion of the conceptual differences attendant upon information, see *e.g.*, *E-Commercial Law* at Chapter 8.01 (nature of an access contract and applicable law).
- ⁴ See *e.g.*, *E-Commercial Law* at Chapter 3 (Property Rights – Thinking Beyond Intellectual Property).
- ⁵ See *e.g.*, *E-Commercial Law* at Chapter 13.07[4](spam, including federal CANSPAM Act) and see Chapter 12 generally (Privacy) and Chapter 12.19 (Sharing of Information for Unsolicited Marketing).
- ⁶ For more information regarding this issue, see Scott David, "New Challenges in Valuing Customer Lists and Customer Based Assets in the New Economy: Tax and Related Issues." (publication pending). Scott can be reached at ScottD@prestongates.com.
- ⁷ See FTC compliant at No. 9, In the Matter of BJ's Wholesale Club, FTC File No. 0423160 (copy available at <http://www.ftc.gov/opa/2005/06/bjswholesale.htm>)
- ⁸ See *E-Commercial Law* at Chapter 12.17 (see also upcoming update).
- ⁹ Michael Rapoport, "Companies Pay a Price for Security Breaches," *Wall Street Journal* (6/5/05).
- ¹⁰ See *E-Commercial Law* at Chapter 4 ("Laws Validating Electronic Transactions").
- ¹¹ That is not to say that there cannot be violations of law, *e.g.*, in consumer contracts the e-contracting procedure might violate a consumer protection law because of a lack of compliance with a special e-rule. See *E-Commercial Law* at Chapter 11.09 ("E-Sign Consumer Consent Rule").
- ¹² See *E-Commercial Law* at Chapter 12 ("Online Informational Privacy and Data Protection").
- ¹³ See *E-Commercial Law* at Chapter 12.17 ("Security of Information Systems").