

“Deciphering Due Diligence: Tackling The IT Issues
That Can Cripple A Business Transaction”

General Overview of IT issues in M&A Transactions

Edward A. Deibert
Howard Rice Nemerovski Canady Falk & Rabkin
San Francisco, California
(edeibert@howardrice.com)

- I. General background of IT issues in an M&A Transaction
 - A. IT related M&A activity is currently increasing.
 - 1. National Venture Capital Association reported that the information technology sector led the venture backed M&A landscape during the first quarter of 2010 with 81 deals and a disclosed total dollar value of \$2.3 billion. Overall, the number of venture-backed M&A exits in the period were the highest since records began in 1975. 31 disclosed venture-backed M&A exits averaged \$180.2 million, 21% higher than the total average disclosed transaction value for all of 2009.
 - 2. KPMG and Ernst & Young each issued reports anticipating significant growth in global IT M&A activity for the rest of 2010.
 - B. IT can be relevant to a transaction in many different ways:
 - 1. Acquiring the seller’s IT could be a principal business objective for the transaction. The seller’s IT could help the acquirer:
 - a. Acquire market share;
 - b. Expand product lines;
 - c. Gain Access to Key Customers;
 - d. Acquire state of art operating facilities;
 - e. Acquire brand reputation; or
 - f. Establish differing Capabilities.

2. IT could pose a risk in connection with the transaction that needs to be addressed.
 - a. The seller may have failed to own or operate its IT properly. The seller may not have obtained all of the necessary rights to own the IT systems that it uses or the seller may have violated the agreements pursuant to which the seller owns its IT.
 - b. Issues may arise in connection with the transfer of the IT in the transaction. There may be consents required to assign the IT to the purchaser which may be difficult or expensive to obtain. Alternatively, there may be restrictions on the use of the IT once in the hands of the acquirer.
3. IT issues could arise following closing of the acquisition.
 - a. There may be some transition period during which either the acquirer or the seller needs to provide services to the other related to the IT.
 - b. The acquirer will need to develop a plan for integrating the acquired IT into its business following closing.

II. The launch of an M&A transaction.

- A. Understanding the value of the IT and its relationship to the transaction is critical at the outset of the engagement. The acquirer needs to consider and determine:
 1. the main business objectives of the merger or acquisition and the key benefits expected from the transaction in order to understand the value;
 2. the ways in which IT can help the business realize its goals for the transaction; and
 3. the opportunities that exist to use technology to position the business for future growth and change.
- B. On the other side, if a seller is disposing of a business unit, subsidiary or significant assets, the seller must also evaluate and understand the IT systems in order to:
 1. consider the difficulty in separating the IT being transferred from the rest of seller's IT;
 2. ensure that it owns or holds the right to use the IT being transferred in the transaction; and

3. determine the assignability of all or portions of any license agreements or other technology underlying the IT.
- C. Also critical for both parties is assembling the correct team at the outset.
1. Need to identify the correct personnel at the acquirer to conduct diligence, assess the seller's IT and determine whether the IT will help fulfill the value proposition behind the transaction. Need to include legal, technical and finance personnel as part of the team.
 2. Similarly need to include the correct seller personnel in order to be able to explain the IT and the technology upon which it rests, to disclose issues related to the IT and to understand how a sale of a portion of the business could impact the seller's remaining business operations.
 3. Weigh risks of bringing people over the wall vs. being able to identify key critical issues.
 4. Can benefit greatly by identifying an integration team at the outset and including them in the early stages of the transaction to help identify risk and benefits from the acquisition and difficulties in integrating the seller with the acquirer.
- D. Conducting diligence. Once the value proposition is understood and the correct team is assembled, diligence can be conducted in a more directed and valuable way.
1. Diligence will not rely just on a form diligence request list.
 2. Diligence can consist of a technical, legal and financial analysis of the seller's IT and underlying intellectual property.
 3. Key issues to consider include: ownership of the IT, assignability of the IT and ability to integrate the IT into the acquirer's system.
- III. Structuring the Transaction. The next key element of the transaction is determining the structure of the acquisition: will the transaction be structured as an asset or a stock acquisition. Certain issues related to the seller's IT can be determinative in resolving this issue.
- A. Acquisition of Assets.
1. Acquirers typically favor asset acquisitions.
 - a. An acquirer can attempt to acquire only certain specified assets and liabilities and to leave all other assets and liabilities with the seller, whether known or unknown, with the seller.

- b. Asset acquisitions also often provide an acquirer with certain tax benefits. An acquirer gets to allocate the purchase price among the seller's assets, increasing the acquirer's basis in the assets. The acquirer can then depreciate the value of the assets following the closing.
 - 2. Asset acquisitions are often disfavored by sellers.
 - a. If all of its assets are sold in the transaction, a seller is left with the need to liquidate following the transaction and to deal with its remaining liabilities.
 - b. In the event a seller has a gain on the sale of its assets, the seller will typically be subject to additional tax liabilities from an asset sale. There is a tax on any gain from the asset sale and an additional tax on the distribution of the proceeds to the seller's stockholders.
 - 3. Asset acquisitions, however, can prove challenging in the context of the assignment of key agreements and contracts. Each of the seller's agreements, including all license agreements, will need to be reviewed to determine whether any issues arise in connection with an assignment of the agreement, such as required consents or amendment of terms. The parties may need to consider alternative structures if there are consents required and there is any risk in obtaining those consents, including any consents required to transfer the IT of the seller.
- B. Stock purchase or merger transaction. A stock purchase or merger can include a direct purchase of the seller's stock, the sale of the stock of a subsidiary by a seller or a merger or reorganization transaction. Mergers can either be reverse, with the seller surviving the merger, or forward, with the seller merging into the acquirer or a subsidiary.
 - 1. Sellers typically favor stock purchases and merger transactions.
 - a. Unless otherwise contractually agreed, the seller and its stockholders are not left with any ongoing liabilities of the company that is sold.
 - b. The seller has only one level of tax: any gain or loss by either the seller or its stockholders on the stock sale.
 - 2. Acquirers may not be as happy about a stock transaction or merger.
 - a. All of the liabilities of the seller, whether known or unknown, are transferred in the transaction and the acquirer could ultimately be liable for them.

- b. In most stock transactions, the acquirer acquires the seller's basis in its assets and, following the closing of the acquisition, can only depreciate any remaining basis the seller had in its assets. The acquirer can only take advantage of its likely higher basis in the stock following closing if the acquirer later disposes of the stock. Forward mergers, however, are typically treated as asset acquisitions for tax purposes.
 - 3. Stock transfers and reverse mergers do not encounter the same consent issues as an asset acquisition.
 - a. A provision requiring a consent to assignment is typically not triggered in connection with the transfer of stock ownership of a company, including reverse mergers, absent specific language in an agreement requiring consent following a change of control or a merger, including where the seller survives.
 - b. Two cases dealing with the license of intellectual property, however, questioned whether a reverse merger can trigger a consent to assignment provisions. See *Cincom Systems, Inc. v. Novelis Corp.*, 581 F.3d 431 (6th Cir. 2009); *SQL Solutions, Inc. v. Oracle Corp.*, No. C-91-1079 MHP, 1991 WL 626458 (N.D. Cal. Dec. 18, 1991), which both held that a reverse merger could trigger a contract clause requiring consent to assignment in the case of a copyright license agreement and a software license agreements, respectively.
 - c. Provisions in licenses which require a consent in connection with an assignment including by operation of law, however, can be triggered in connection with a forward merger.
- IV. Drafting the definitive acquisition agreement: key issues in the agreement related to IT.
- A. The key provisions of the definitive agreement related to IT are the representations and warranties.
 - 1. The seller typically makes an exhaustive set of representations and warranties related to its business, covering a number of different issues including IT.
 - 2. The representations and warranties related to IT typically fall within one of the following categories:
 - a. Intellectual Property. IT systems consist of third party licensed technology and internally developed technology. The seller

typically makes representations about this technology in at least three respects:

- (i) Ownership: the seller either owns or has the valid right to use all of the intellectual property underlying the IT.
 - (ii) Non-infringement: the seller's intellectual property and the use thereof does not infringe, misappropriate or otherwise violate the rights of any third party.
 - (iii) Third party infringement: no third party is infringing the intellectual property of the seller.
 - (iv) Identification: the disclosure schedules identify the various pieces of technology making up the IT and list any registered patents, copyrights or trademarks included therein.
 - (v) Miscellaneous: in the event that there are any additional specific issues with respect to the IT at issue, additional specific representations covering those issues are included.
- b. Privacy Policies. To the extent the seller collects information from its customers or other users, the seller also makes representations about the policies pursuant to which such information is collected and maintained, including representations about compliance with its privacy policies and compliance with the laws related to the collection of user information. This is an area about which people are becoming increasingly concerned, especially given increasing regulations by several states and the European Union on the collection of user information. A sample privacy representation is attached at the back of the outline.
 - c. Compliance with Material Contracts. To the extent not otherwise covered by the general intellectual property representation and as part of a representation about the seller's material contracts, the seller also makes representations about the enforceability of and compliance with the agreements pursuant to which the technology underlying the IT is licensed to the seller.
- B. Purpose of the representations and warranties. The representations and warranties about the IT in the definitive acquisition agreement serve three main purposes:
- 1. Diligence. In addition to the diligence conducted by the acquirer, the acquirer has the opportunity to craft the representations and warranties

in a manner to require the seller to disclose additional information with respect to its IT, such as prior litigation or actions taken to contest the validity of any registration of the intellectual property underlying the IT.

2. Closing Conditions. The representations and warranties also serve as a basis to protect the acquirer from having to close an acquisition in the face of information discovered or events arising after signing the definitive purchase agreement.
 - a. To the extent there is any period between signing the definitive acquisition agreement and closing of the acquisition, the agreement will typically include a closing condition that looks at the continued accuracy of the representations and warranties.
 - b. There are differing standards of closing conditions used in various agreements. Under these different standards, the closing condition is not met unless at the closing either: the representations and warranties are true in all respects; they are true in all material respects; or, to the extent there is a breach in a representation, that breach has not had a material adverse effect on the seller.
 - c. If something is either discovered or occurs with respect to the IT after the date of the acquisition agreement and before closing the acquisition (such as an infringement suit being filed), the acquisition agreement provides that the acquirer is not required to close the transaction until the issue is resolved. The agreement can also provide that the acquirer may terminate the acquisition agreement if the issue is not cured or capable of being cured within a defined period of time.
3. Post-closing indemnification. In most private company acquisitions, the representations and warranties will survive for some period following the closing of the acquisition. The representations and warranties then serve as a basis for the acquirer to seek recovery from the seller or its stockholders to the extent some issue arises after closing of the acquisition and during the period in which the representations and warranties survive and causes the acquirer damages.

V. Post-Closing. Planning for the day following the closing needs to be addressed as early as possible during negotiations of the acquisition.

A. Transition Services.

1. If an acquirer is buying something less than the entirety of the seller (like a business, subsidiary, or set of assets), then the parties will need to determine if either party needs to provide anything to the other in order to keep the business running following closing. Some key questions include:
 - a. Until replacement IT is obtained and in order to continue to operate the seller's business or the business being acquired, does the seller need continued access to the IT transferred to the acquirer or is there a portion of the IT retained by seller that the acquirer needs?
 - b. Does the business being transferred rely on services provided by the seller to operate or does the business provide services to the seller that the seller needs?
2. Agreements providing access to the IT and providing these services can be complicated to negotiate and implement.
 - a. The specific terms of the transition services agreement must be set forth:
 - (i) the services to be provided,
 - (ii) the access or sub-license of technology that is needed,
 - (iii) the length of time for the transition period, and
 - (iv) any costs or charges to be incurred.
 - b. Need to ensure that the party agreeing to provide the services is allowed to do so under any relevant contracts. Oftentimes a seller will agree to provide transition services following closing only to find out that the underlying license agreement prohibits seller from providing a sub-license to that technology or providing services on an outsourced basis to a third party.
 - c. During negotiation of the transition service agreement, the acquirer may also learn for the first time that it is not acquiring all of the technology needed to operate the business following closing. Such realization can lead to renegotiation of the terms of the underlying deal.

- d. The length of the term and the price to be charged can also be the basis of difficult negotiation because the acquirer typically does not believe it should pay additional amounts after acquiring the business and the seller will believe that it should be finished having to operate the business after it is sold.

B. Integration.

1. A poorly executed integration plan can create or destroy shareholder value from the transaction.
2. Acquirer needs to determine the level of integration effort that will be undertaken and a process for that integration:
 - a. Preservation of businesses: Only certain corporate functions and technology are merged to achieve certain amount of economies of scale. Overall, however individual companies or business units remain separate.
 - b. Moderate integration/combination: Key functions and technology are consolidated using the most effective of either party, but day-to-day operations of the businesses remain autonomous.
 - c. Full/consolidation, combination or transformation: All functions, technology and personnel of the businesses are integrated. Under a consolidation, all functions are integrated into one of the businesses. A combination requires finding the most effective functions of either entity to form an efficient model for the integrated whole. Finally, a transformation allows the parties to transform the entirety in a completely new way of operating.
3. The information gathered throughout the transaction from the planning stages, through the diligence effort and closing of the acquisition will be used in providing for an effective integration.

Attachment A
Sample Representation and Warranty On Privacy:

Privacy. Section XX of the Disclosure Schedule contains a list of each Privacy Policy and identifies, with respect to each Privacy Policy, (i) the period of time during which such privacy policy was or has been in effect, (ii) whether the terms of a later Privacy Policy apply to the data or information collected under such privacy policy, and (iii) if applicable, the mechanism (such as opt-in, opt-out, or notice only) used to apply a later Privacy Policy to data or information previously collected under such privacy policy. Sellers have provided Purchaser true and complete copies of each Privacy Policy. Seller has complied at all times and in all respects with all of the Privacy Policies and with all applicable Legal Requirements pertaining to privacy (including the obtaining, storing, using or transmitting of User Data), User Data, Personal Data or Employee Data. Neither the execution, delivery, or performance of this Agreement (or any of the Ancillary Agreements) nor the consummation of any of the Transactions, nor Purchaser's possession or use of User Data, will result in any violation of any Privacy Policy or any applicable Legal Requirement pertaining to privacy, User Data, Personal Data or Employee Data. Section 4.09(j) of the Disclosure Schedule also identifies and describes each distinct Business Database (in whole or in part) containing advertiser, customer, personal, user or employee data, the types of data in each such Business Database and the security policies that have been adopted and maintained with respect to each such Business Database. No breach or violation of any such security policy has occurred or, to the best of the Sellers' Knowledge, is threatened, and there has been no unauthorized or illegal use of or access to any of the data in any of such Databases.

"Privacy Policy" means each of the Seller's external or internal, past or present, privacy policy, including any policy relating to (i) the privacy of users of the Business or of any website operated in connection with the Business, (ii) the collection, storage, disclosure and transfer of any User Data or Personal Data, and (iii) any employee information for employees performing services relating to the Business.

"Personal Data" shall mean a natural person's name, street address, telephone number, e-mail address, photograph, social security number, driver's license number, passport number, or customer or account number, or any other piece of information that allows the identification of a natural person.

"User Data" means any Personal Data or other data or information collected by or on behalf of Seller from users of the Business or of any website operated in connection with the Business.

"Employee Data" means any Personal Data or other data or information collected by or on behalf of Seller from employees of the Business.

“Deciphering Due Diligence: Tackling the IT Issues That Can Cripple a Business Transaction”—American Bar Association Annual Meeting (August 6, 2010)

PRIVACY AND DATA SECURITY ISSUES IN M&A, OUTSOURCING, AND OTHER BUSINESS TRANSACTIONS

Christine Lyon, Morrison & Foerster LLP

1. A Few Signs that Privacy Issues Require Attention in Your Transaction

- (a) Does the transaction involve sale or acquisition of customer data?
- (b) Does the transaction involve operations or personnel located outside the U.S.?
- (c) Does the transaction involve e-commerce activities?
- (d) Does the transaction involve sharing personally identifiable information (“PII”)¹ with a vendor or service provider?

2. Overview of Privacy and Data Security Laws Implicated by Transactions

- (a) United States:
 - (i) Sector-specific approach at federal level, including:
 - (1) Health Insurance Portability and Accountability Act (HIPAA): Applies to covered entities (health plans, health care clearinghouses, health care providers); regulates use and disclosure of protected health information; imposes detailed privacy and data security rules on covered entities and their business associates.
 - (2) Gramm-Leach-Bliley Act (GLBA): Applies to financial institutions; regulates use and disclosure of nonpublic personal information about consumers; imposes detailed privacy and data security obligations.
 - (3) Children’s Online Privacy Protection (COPPA): Applies to operators of websites or online services that collect information from children under the age of 13; regulates collection, use, disclosure, and security of PII about children.
 - (ii) State laws tend to apply across sectors, including:
 - (1) State medical privacy laws (e.g., California’s Confidentiality of Medical Information Act, Texas Medical Privacy Act²).

¹ For purposes of this outline, “PII” is any information that relates to an identified or identifiable person. This includes not only information that directly identifies the person (such as his/her name or Social Security number) but any information that is associated with or can be traced back to that person.

(2) California Online Privacy Protection Act³: Requires operator of commercial website or service to post a privacy policy containing certain details. See also the California “shine the light” law, which requires certain disclosures related to the sharing of PII with third parties for third party direct marketing purposes.⁴

(3) State data security laws: Massachusetts data security regulations,⁵ Nevada encryption law,⁶ more general data security laws of other states (e.g., Arkansas, California, Connecticut, Indiana, Maryland, Oregon, Rhode Island and Utah).⁷

Practice Pointer for Contract Negotiation: These data security laws usually require the data “owner” to include data security obligations in its contracts with service providers or other third parties. This needs to be addressed in drafting outsourcing and service provider contracts. It is also a good area to explore when conducting due diligence of privacy/data security practices.

Practice Pointers for Due Diligence:

- MA regulations and NV law require encryption of covered personal data (such as SSN, credit/debit card or financial account number, and driver’s license number) on laptops and portable storage devices, and in electronic transmission—an area to explore when conducting due diligence of privacy/data security.
- MA regulations (which became effective March 1, 2010) require risk assessment, written information security programs (including physical and administrative safeguards, not just IT security), service provider contracts, employee policies, documentation of breach incidents and responses—all useful information to request when conducting due diligence.

(4) State security breach notification laws: Nearly every state now has a security breach notification law. Past security breach incidents usually require disclosure during due diligence. Prospective sellers or vendors should be prepared to show remedial action, possibly accompanied by third party assessment of improved security protocols.

² Cal. Civ. Code §§ 56–56.37; Texas H&S Code §§ 181.001–181.254. Links to U.S. and international laws referenced in this outline are available through Morrison & Foerster’s free online privacy library, at www.mofoprivacy.com.

³ Cal. Bus. & Prof. Code §§ 22575–22578.

⁴ Cal. Civ. Code § 1798.83.

⁵ 201 Mass. Code Regs. §§ 17.01–17.05. For additional information, please refer to our attached article, “Compliance Date for Massachusetts Data Security Regulations Rapidly Approaching: Are You Ready to Comply?”

⁶ Nev. Rev. Stat. §§ 603A.200 – 603A.201. For additional information, please refer to our attached article, “Nevada Requires Encryption of Personal Information in Transit and in Storage on Portable Devices.”

⁷ Ark. Code § 4-110-104; Cal. Civ. Code § 1798.81.5; Conn. Gen. Stat. § 42-471; Ind. Code §§ 24-4.9–3-3.5; Md. Com. Law Code §§ 14-3502–14-3503; Or. Rev. Stat. § 646A.622; R.I. Gen. Laws § 11-49.2-5; Utah Code Ann. § 13-44-201.

(b) International:

(i) Over 60 countries have data protection laws or are actively developing such laws, including:

(1) EMEA: Each of the 27 Member States⁸ has its own unique data protection laws, plus Israel, Morocco, Norway, Russia, Serbia, South Africa (pending), Switzerland, Tunisia, Turkey (pending), Ukraine.

(2) Americas: Argentina, Brazil (pending), Canada, Chile, Colombia, Costa Rica (pending), Ecuador (pending), Mexico, Paraguay, Peru, Uruguay.

(3) Asia-Pacific: Australia, China (pending), Hong Kong, Japan, Malaysia, New Zealand, Philippines, South Korea, Taiwan, Thailand (pending), Vietnam (pending).

(ii) These laws often cover all personally identifiable information—even easily accessible PII such as people’s names or business card information. Most of these laws apply across all sectors, and apply equally to offline or online data practices.

(iii) Typical requirements include:

(1) Establishing a legal basis to collect, use, disclose, transfer, or otherwise “process” PII (such as contractual necessity, compliance with local legal obligations, consent of the individual).

(2) Giving notice to the individual about the collection, use, disclosure, transfer of his/her PII. This can apply to consumers, employees, consultants, or any other individuals.

Practice Pointers for Due Diligence:

- When conducting a due diligence review of a company with operations in jurisdictions with data protection laws, be sure to request copies of the data protection notices given to employees, customers, etc.
- As discussed in Section 3(a)(ii)(1) below, this notice obligation may be a challenge when the parties wish to exchange information about individuals who are not aware of the prospective transaction (e.g., a potential merger).

(3) Consent may be required to collect or process sensitive PII (e.g., race, medical information, religious or philosophical beliefs) or to permit certain types of disclosures or processing.

⁸ For ease of reference, the 27 current EU Member States are Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

(4) Entering into contracts with all “third parties” (including affiliates) who receive or process PII on your behalf, containing appropriate privacy and data security provisions.

(5) Establishing a mechanism for cross-border transfers, where applicable laws (e.g., in the EU, Australia or Argentina) restrict such transfers. (Note that access equals transfer: if someone in another country can access the data, this effectively constitutes a “transfer” to that country.)

(6) Data security is a common principle of data protection laws, but certain countries have also imposed detailed and extensive data security requirements (e.g., Argentina, Italy, Japan, Norway, Poland, Spain, and Taiwan). A growing number of countries are also adopting security breach notification requirements.⁹

Practice Pointer: Compliance with EU privacy laws, such as EU solutions for cross-border data transfers, is not sufficient to ensure compliance with all other global data protection laws. A number of countries impose stricter and/or additional requirements, beyond those required in EU Member States. It is important to consider the privacy requirements in each applicable country.

3. Key Privacy and Data Security Issues in M&A: Seller-Side Issues

(a) Limitations on pre-closing disclosure of PII, including employee data:

(i) U.S. issues:

(1) All disclosures of PII should be covered by a non-disclosure agreement and made via an approved secure means, such as a virtual data room.

(2) Avoid sharing PII that would trigger a security breach notification requirement in the event of unauthorized access (e.g., SSNs, driver’s license numbers, credit/debit or financial account numbers, medical or health insurance information).

(3) Avoid sharing PII that cannot lawfully be used for the purpose for which it would be provided (e.g., avoid disclosing age, race, national origin, disability, or similar protected information about employees), or that is irrelevant for that purpose (e.g., home address, home telephone number or PII about dependents).

(4) Avoid sharing PII in which an employee may have a reasonable expectation of privacy (e.g., personnel files, performance reviews). Note that this analysis can vary by state.

⁹ As of this writing, Australia; Alberta, Canada; Germany; Japan; Norway; Taiwan; United Arab Emirates; and Uruguay have adopted mandatory security breach notification requirements. Australia, Canada, Denmark, Ireland, New Zealand, and the United Kingdom have adopted voluntary security breach notification guidelines, although there are current proposals for Ireland and the UK to convert to a mandatory breach notification approach.

(ii) International issues:

(1) Data protection laws require a legal basis to disclose PII to a third party—in most cases, the only option is to obtain the individual's consent:

a. In order to obtain valid consent to disclosure, the individual would need to be informed of the recipient(s) and the purposes for which the PII is being shared. There is usually little difficulty in obtaining consent of senior-level executives involved in deal, but it may not be feasible to obtain from rank-and-file employees or other individuals.

b. Practical strategy is to limit the disclosure of PII, such as through use of aggregated or “anonymized” data.

Practice Pointer for Due Diligence: If the data can be associated with an individual, it's PII. For instance, even if the seller redacts names from an employee list, it may still be possible to identify individuals based on unique job title or other unique combinations of data elements. Aggregated data is often better than redacted or “anonymized” data, from a privacy compliance perspective.

c. Various countries have their own guidance about due diligence disclosures of employee data. A few examples:

i. EU: Where feasible, PII should be shared only in aggregate, anonymous format. Prior to sharing any PII, the target company should provide notice and obtain consent. Where individuals have consented to the use of their PII for due diligence purposes, the information must not be used for other purposes. (Note that each Member State has its own local requirements.) Works council consultations also may be needed in certain cases.

ii. Japan: Prior to closing, PII may be provided only with the employee's prior consent. Valid consent requires disclosure of the name of the company to which the PII will be provided.

iii. Argentina: It may be permissible to transfer basic employee details without the employee's consent, but the employee must be notified of the identity of the recipient and the purpose of the transfer.

(2) Any permitted disclosures of PII must be covered by a non-disclosure agreement and should be made via an approved secure means, such as a virtual data room.

(b) Preparing to address common due diligence requests related to privacy and security.

Practice Pointer for Due Diligence: Representative examples of due diligence requests related to privacy and data security:

- Copies of all current and prior versions of privacy policies, notices, training materials and manuals, including website policies, relating to the collection, use, sale, lease or transfer

(including cross-border transfer) of personal information of customers and others.

- Any agreements with customers, service providers and other vendors relating to the collection, use, sale, lease or transfer (including cross-border transfer) of personal information.
- Copies of all registrations filed with any data protection authority or regulator relating to personal information of any customers, service providers or other vendors.
- List of any alleged breaches of any of the company's privacy policies or privacy obligations.
- Any agreements or policies related to cross-border transfers of personal information among the company and its affiliates.
- Description of electronic, technical and physical security measures to protect personal information.
- Any instances in which the company has provided notice to an individual, customer or regulator relating to a security incident or the unauthorized access to or acquisition of personal information.
- Any complaints, inquiries, consent decrees, citations, fines, administrative actions or litigation regarding privacy or data security.

(c) Identifying any potential restrictions on Seller's ability to transfer customer PII to the acquiring entity:

(i) Check whether Seller's privacy policies reserve the ability to transfer PII in connection with a sale of business. Does the privacy policy require Seller to impose any conditions on the buyer in connection with that transfer?

(ii) Note that the Federal Trade Commission has taken the position that material changes to a privacy policy require individual consent, and international data protection laws may effectively require consent as well.

4. **Key Privacy and Data Security Issues in M&A: Buyer/Investor-Side Issues**

(a) Asset purchase:

(i) Buyer needs to ensure that Seller can lawfully transfer/disclose the PII to Buyer/NewCo at closing, particularly customer PII.

(1) Restrictions may arise if Seller's privacy policy was overly restrictive and did not reserve the ability to transfer PII in connection with a sale of business or assets. (As noted above, it may not be sufficient to make last-minute unilateral changes to the privacy policy, if material.)

(2) Restrictions also may arise under privacy or data protection laws, such as notice and consent requirements.

(3) If such restrictions exist, consider whether they affect valuation (e.g., consider requiring Seller to obtain consent, and negotiate a purchase price adjustment).

(ii) Buyer should assess Seller's basic compliance with privacy laws because failure to comply with these obligations at the time the PII was collected may potentially limit the subsequent use or disclosure of PII.

(b) Stock or equity purchase:

(i) Buyer should perform a more comprehensive analysis of the target's compliance with privacy and data protection laws, given liability concerns.

(ii) Buyer should consider whether it would seek to share the target's customer data among Buyer and its affiliates, and whether there are limitations on such sharing. If the customer data is a key asset, such limitations may affect the value of that asset:

(1) Data protection laws may limit sharing even among affiliates and/or require the individual's consent to such sharing (e.g., Korea).

(2) If the data would be shared among affiliates for the affiliates' direct marketing purposes, this may implicate California's "shine the light" law (see Section 2(a)(ii)(2) above). Additionally, the direct marketing activities may require the individual's consent in various jurisdictions (e.g., EU Member States,¹⁰ Japan, and Korea).

Practice Pointer: PII obtained from Seller/Target may be subject to different restrictions on use and disclosure than PII that Buyer has collected directly. These differences can arise from different privacy policies, different applicable laws, different contractual obligations, etc.

- Is Buyer prepared to segregate the PII from Seller/Target from the rest of its PII, and continue to handle it differently?
- Does Buyer intend to take measures (such as obtaining consent) to bring use and disclosure of the acquired PII more into line with its own practices? If so, when will these measures be taken? Does Buyer seek to require cooperation/assistance by Seller?

5. Key Privacy and Data Security Considerations When Outsourcing Data

(a) Fundamental principle: ***You can outsource the processing, but not the liability***—liability remains with the data controller/owner.

(i) Owner/service provider distinction under U.S. data security laws.

(ii) Controller/processor distinction under international data protection laws.

¹⁰ For example, please refer to our attached article, "German Data Protection Landscape is Changing," for information about Germany's increasingly strict rules concerning marketing-related uses of PII.

(1) Definitions:

a. Data controller: A person or entity that (either alone or jointly with others) decides how and why PII is processed.

b. Processor: A person or entity that merely processes PII on behalf of a controller.

(2) As a general principle, controllers are directly governed by data protection laws and processors are governed by contractual obligations imposed by the controller.

a. Controller/processor distinction is not based on “ownership” of PII, but on control over use and processing of the PII.

b. It is possible for the service provider to be deemed a “joint controller,” if it exercises control over the PII (e.g., by subcontracting) or uses the PII for its own purposes.

(b) Contractual protections will depend on the types of PII that will be shared with (or accessible to) the provider:

(i) Data covered by federal or state data security laws? (*See* Section 3(a)(ii)(3).)

(ii) Data covered by international data protection laws? (*See* Section 2(b).)

(iii) Data covered by the Payment Card Industry Data Security Standard (PCI DSS) or similar requirements?

(iv) Data held on behalf of third parties to whom the Company owes contractual or other legal obligations?

(c) Why it isn’t sufficient for a customer to rely on general reps and warranties about compliance with “all applicable laws”:

(i) Most of these obligations fall on the owner/controller, not the service provider/processor:

(1) The service provider/processor’s compliance with applicable laws does not necessarily fulfill all obligations that fall upon the owner/controller.

(2) Accordingly, the applicable obligations should be specified, beyond the usual provisions about compliance with applicable law. This also aids in enforcement of contractual rights and remedies.

(3) Where the outsourced data might be subject to breach notification laws, the customer will also want to include protections in the event of a security breach, as well as indemnification:

a. The data owner generally bears the burden of notifying affected individuals of a breach, even if the breach occurs due to the acts or omissions of the service provider.

b. Customers may seek to negotiate contractual protections, such as requiring the service provider to issue these notices at the customer's instruction, to pay for the costs of such notice and any other reasonable remedial measures, and to indemnify the customer for any losses or costs if the breach arose from the service provider's acts or omissions in violation of the contract.

(ii) State, federal, and international laws may require appropriate due diligence in selecting service providers, and ongoing supervision of service providers. Particularly if the vendor will be handling sensitive data, it may not be sufficient to rely solely on the terms of the contract as a means of verifying that the data will be adequately protected.

(d) Cross-border data transfers:

(i) Evaluate whether PII will be transferred to, or accessible from, additional countries—keeping in mind the broad definition of PII in most countries. Does the transaction implicate data protection laws that may limit such transfers (e.g., in the EU, Australia, Korea, Argentina and Taiwan)?

(1) Options for cross-border transfers from the EU may include Safe Harbor program (only covers transfers to the U.S., however), EU model clauses¹¹ or ad hoc contracts approved by the applicable data protection authorities, and individual consent (disfavored in the employment context). Each has its own pros and cons.

(2) Keep in mind that options for cross-border transfers from other countries are often more limited. Each country must be considered separately.

Practice Pointer: The EU is not the only jurisdiction that limits cross-border transfers or sharing of PII. Additionally, many of the EU options for cross-border transfers would not be valid in other jurisdictions (e.g., EU model clauses, Safe Harbor provisions, binding corporate rules). Accordingly, other countries' cross-border restrictions must be analyzed and addressed separately.

¹¹ The EU recently updated its model clauses for transfers to service providers, better reflecting the common use of subcontractors. For additional information, please refer to our attached article, "The New Set of EU Model Clauses for Service Providers." Links to the new set of model clauses and other references may be found at www.mofoprivacy.com, under "European Union."

(e) Special challenges for cloud computing:

(i) In principle, cloud computing is just another variation on traditional data hosting/outsourcing models.

(ii) In practice, cloud computing arrangements tend to offer less control and thus less protection for PII.¹²

(1) Risks of subjecting PII to other countries' data protection laws:

a. PII processed in other countries may become subject to the data protection laws of those countries (e.g., U.S. data stored on servers in EU, and other more restrictive jurisdictions).

b. In principle, local laws may even prohibit PII from being transferred back to the country of origin, if deemed to provide "inadequate" privacy protections:

(1) Concerns about potential access/inspection demands or service interruptions by local governments, legal process.

(2) How do you impose required contractual protections, when you don't even know who may own the equipment on which the PII is stored?

(iii) Open issue of whether cloud models will evolve to provide greater options for customers in addressing these privacy and security concerns.

6. Additional Resources

(a) Privacy Library (www.mofoprivacy.com): Links to federal, state, and international privacy laws, regulations, and guidance.

(b) Supplemental attached materials (also available at www.mofoprivacy.com):

(i) "Compliance Date for Massachusetts Data Security Regulations Rapidly Approaching: Are You Ready to Comply?" (February 2010).

(ii) "Nevada Requires Encryption of Personal Information in Transit and in Storage on Portable Devices" (June 2009).

(iii) "German Data Protection Landscape is Changing" (July 2009).

(iv) "The New Set of EU Model Clauses for Service Providers" (April 2010).

(v) "Cloud Computing and Outsourcing: Is Data Lost in the Fog?" (June 2009).

¹² For a more extensive discussion, please refer to our attached article, "Cloud Computing and Outsourcing: Is Data Lost in the Fog?"

Client Alert.

February 2010

Compliance Date for Massachusetts Data Security Regulations Rapidly Approaching: Are You Ready to Comply?

By Miriam H. Wugmeister and Nathan D. Taylor

Many U.S. state laws require that businesses adopt reasonable measures to protect personal information and/or dispose of personal information in an appropriate manner. The data security regulations issued by the Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”), however, impose far more detailed and comprehensive data security requirements than most, if not all, other states. With the compliance date for the Massachusetts data security regulations—**March 1, 2010**—only two weeks away, organizations would be well advised to take a fresh look at their policies and procedures.

The regulations were originally issued in September 2008, with an initial compliance date of January 1, 2009. OCABR, however, amended the regulations several times. In amending the regulations, OCABR not only made substantive changes, but also extended the compliance date several times. All indications are that OCABR will not extend the compliance date again and that compliance with the regulations will be required on March 1, 2010.

While the regulations (and the previous revisions to the regulations) are described at greater length in earlier Morrison & Foerster Legal Updates ([“New Massachusetts Regulation Requires Encryption of Portable Devices and Comprehensive Data Security Programs,”](#) [“Massachusetts Delays Effective Date of New Data Security Regulations,”](#) [“Massachusetts Amends Burdensome Service Provider Oversight Requirements of New Data Security Regulations and Delays Compliance Date Again,”](#) and [“Massachusetts Amends Its Data Security Regulations Again: Burdensome Service Provider Oversight Requirements are Back”](#)), the following provides a brief overview of certain important requirements of the regulations.

The Massachusetts data security regulations apply to any person that receives, maintains, processes, or otherwise has access to “personal information” relating to a resident of Massachusetts in connection with the provision of goods or services, or in connection with employment. For purposes of the regulations, the term “personal information” is defined as an individual’s first name or initial, and last name, in combination with any one of the following data elements: (1) Social Security number; (2) driver’s license number or state-issued identification card number; or (3) financial account, credit card, or debit card number, with or without any required security code or password that would permit access to the account.

The Massachusetts data security regulations impose a number of significant administrative responsibilities on covered businesses. For example, a covered business must:

- develop, implement, maintain, and monitor a comprehensive, written information security program that contains administrative, technical, and physical safeguards to ensure the security and confidentiality of records containing personal information;
- conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of electronic, paper, and other records containing personal information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks;

Client Alert.

- designate one or more employees to maintain the information security program;
- regularly monitor to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of, personal information;
- take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the regulations and any applicable federal regulations, including requiring service providers by contract to implement and maintain such security measures (there is a limited safe harbor for the contract requirement until March 1, 2012); and
- educate and train employees regarding personal information security.

Beyond its general, risk-based information security program requirement and related administrative requirements, the Massachusetts data security regulations also require that a business implement a number of detailed and specific technical security controls. Among other things, the regulations require that an organization must:

- implement reasonable restrictions on physical access to records containing personal information and storage of such records in locked facilities, storage areas, or containers;
- implement secure user authentication protocols and access control measures for computer systems;
- encrypt all transmitted records and files containing personal information that will travel across public networks and that will be transmitted wirelessly;
- encrypt all personal information stored on laptops and other portable devices; and
- maintain firewall protections, operating system security patches, and malware and virus protection.

In light of the complexity and specificity of the regulations as a whole, as well as the fast-approaching compliance date, compliance efforts should remain a high priority for businesses that handle personal information relating to Massachusetts residents. Businesses that have not taken steps to address compliance with the Massachusetts data security regulations should quickly begin to take such steps. For those businesses that have taken steps to address their compliance with the regulations, consider revisiting the compliance program to ensure it complies with the detailed regulations set to take effect at the beginning of next month. Massachusetts law may be the most detailed, but it is certainly not the only state regulation relating to the security of personal information, and it will not be the last.

Morrison & Foerster has a world-class privacy and information security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by Chambers and Legal 500 as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, and subscription service Summit, please visit: <http://www.mofo.com/privacy--data-security-services>

Client Alert.

Contact:

Miriam H. Wugmeister
212) 506-7213
mwugmeister@mofo.com

Nathan D. Taylor
(202) 778-1644
ndtaylor@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, Fortune 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last six years, we've been included on *The American Lawyer's* A-List. *Fortune* named us one of the "100 Best Companies to Work For." We are among the leaders in the profession for our longstanding commitment to pro bono work. Our lawyers share a commitment to achieving results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

Nevada Requires Encryption of Personal Information In Transit and In Storage on Portable Devices

Vanessa Waldref and Nathan Taylor

Privacy + Data Security

8/25/2009

Client Alert

In 2005, Nevada enacted a data security law that required businesses to encrypt customer personal information before electronically transmitting it outside of an internal secured network.^[1]

Nevada recently amended this law to also cover personal information not related to customers, and to require data collectors that conduct business in the state to encrypt data storage devices containing personal information that they move outside the secured physical and logical boundaries of the entity.^[2] Data storage devices include, among other things, computers, cellular phones, and thumb drives. The amended Nevada encryption law goes into effect January 1, 2010.

New Amendments Expand Encryption Requirements

Nevada's first encryption law was adopted at the same time as the state's data breach notification law, which requires businesses to alert Nevada residents to the unauthorized access or acquisition of their personal information.^[3] The 2005 legislation required the encryption of all customer personal information transferred electronically outside of the secure system of a business, with the exception of fax transmissions.^[4]

The new law expands the original encryption requirement to both customer and non-customer personal information, and also requires encryption of all personal information that is transferred "beyond the logical or physical controls" of a business or its data storage provider on any data storage device. The amended statute also extends encryption obligations to all "data collectors" doing business in the state, a category that includes governmental agencies, institutions of higher learning, corporations, financial institutions, retail operators, or "any other type of business entity or association" that deals with non-public personal information.

Additionally, these amendments include a technical standard for encryption that was absent in the original statute, and requires businesses that accept credit or debit cards to meet the Payment Card Industry Data Security Standard.

Overview of the Nevada Law

The "personal information" covered by the Nevada encryption law is the same information that is subject to that state's security breach notification law, namely: "a natural person's first name or first initial and last name in combination with any of the following: (a) Social Security number or employer identification number; (b) driver's license number or identification card number; or (c) account number, credit card number or debit card number, in combination with any required

security code, access code or password that would permit access to the person's financial account." Personal information does not include "the last four digits of a social security number or publicly available information that is lawfully made available to the general public."

The new law defines a "data storage device" as "any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself." Data collectors in Nevada should note that the definition of data storage device is expansive, and is not limited to portable devices, such as laptops and blackberries. The encryption requirements also apply to CDs, DVDs, desktop computers, and servers that contain personal information that are, for example, moved to another office location.

Putting these provisions together, data collectors that do business in Nevada must use encryption for: (1) all electronic transmissions of personal information, except faxes, outside the secure system of the data collector; and (2) any movement of a data storage device containing personal information outside the confines of the workplace of the data collector or its data storage contractor.

Nothing in the Nevada statute limits its application to personal information of Nevada residents that is transmitted or stored by a data collector. Accordingly, the Nevada encryption law could be interpreted as applying to a covered entity's transmission or storage on a portable device of any personal information, regardless of where the subject of that information resides.

Also, the Nevada encryption law does not define the scope of a "data collector doing business in this State." However, in addressing whether a foreign corporation had satisfied qualification requirements under Nevada law, the Nevada Supreme Court interpreted "doing business" in Nevada by adopting a two-pronged standard: (a) the nature of the company's business in the state; and (b) the quantity of business conducted by the company in the state. In that case, the Court noted that assessing whether a foreign company is "doing business" in the state is "often a laborious, fact-intensive inquiry resolved on a case-by-case basis."^[5]

Encryption Standard

Under the new law, data collectors seeking to comply with the encryption requirement for either electronically transmitted personal information or information transferred on a storage device must use encryption that meets a certain standard. Specifically, data collectors must use an encryption technology "that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data." Data collectors must also use established standards to ensure "appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption."

The amended law will provide a damages liability safe harbor for covered entities that meet the data encryption requirements for the electronic or data storage device transfer of personal information. This safe harbor, however, will not apply for businesses that face a data breach resulting from gross negligence or intentional misconduct.

Businesses That Accept Credit Cards Must Comply with Industry Standards

The new law requires that data collectors doing business in Nevada that accept credit or debit card payments for goods or services must comply with the Payment Card Industry Data Security

Standard. This Standard is a set of industry self-regulatory data security standards for merchants and other businesses that accept credit card and debit cards as payment, and merchant banks and other financial services businesses that process payment card transactions.

Unless a business engages in gross negligence or intentional misconduct, the new law will provide a safe harbor from damages liability for security breaches if a covered business complies with the Payment Card Industry Data Security Standard.

On its face, the new law appears to provide that data collectors that accept credit cards or debit cards as payment are only required to comply with the Payment Card Industry Data Security Standard and not the Nevada encryption requirements. Specifically, the statute provides that the encryption requirements only apply to data collectors to whom the Payment Card Industry Data Security Standard do not apply. It is not clear whether the Nevada legislature intended such a result. The more likely intent may have been that data collectors that accept credit or debit card payments must comply with the encryption standards with respect to personal information to which the Payment Card Industry Data Security Standard would not otherwise apply, including, for example, employee personal information and non-payment card financial information.

New Trends in Data Security Measures

Many state laws, like a number of federal statutes and regulations, mandate that businesses take reasonable data security measures to safeguard personal information. For example, the California Security Safeguard Act^[6] applies to a company that owns or licenses unencrypted “personal information” about California residents and, in general, requires the company to implement and maintain “reasonable security procedures and practices” to protect such data. Texas and Rhode Island^[7] have enacted similar laws requiring companies to adopt procedures relating to information security. Only Nevada and Massachusetts specifically mandate the use of encryption to protect personal information.

As states respond to an increasing public concern about the safety of personal information and the threat of identity theft, Nevada’s encryption requirements may signal a new trend. Companies subject to the Nevada law should take steps to develop compliance procedures that meet the new encryption requirements and that are also consistent with general data security obligations mandated under federal law and the laws of other states.

[1] Nev. Rev. Stat. § 597.970 (2005).

[2] Nevada Senate Bill 227, which is available [here](#).

[3] Nev. Rev. Stat. § 603A et seq.

[4] The new law maintains this “fax” exception and defines “facsimile” as “an electronic transmission between two dedicated fax machines using Group 3 or Group 4 digital formats that conform to the International Telecommunications Union T.4 or T.38 standards or computer modems that conform to the International Telecommunications Union T.31 or T.32 standards.”

[5] *Executive Mgmt. Ltd. v. Ticor Title Ins. Co.*, 38 P.3d 872 (Nev. 2002).

[6] Cal. Civ. Code § 1789.81.5(b).

[7] R.I. Gen. Laws § 11-49.2-2(2) (2006); Tex. Bus. & Com. Code § 48.102(a) (2006).

German Data Protection Landscape Is Changing

Karin Retzer

Privacy + Data Security

7/9/2009

Client Alert

PDF Version

Against the backdrop of widely reported data breaches, and with the September 2009 federal election drawing close, the German Parliament has voted for significant changes to existing data protection laws, including new requirements for credit checks, location tracking services, and telemarketing. Other amendments, including the introduction of U.S.-style data breach notification procedures and employee privacy rules, together with a prohibition on address trading without consent, are all under discussion. The following article summarizes recent privacy-related amendments in Germany, as well as a number of new developments that are in the pipeline.

New Rules for Scoring Techniques

With new rules on scoring techniques adopted June 12, the German Parliament has finally regulated a common practice. What is scoring exactly? The most frequently used type is a credit score or credit check that is based on a statistical analysis of a person's payment history, current income, etc. to determine the creditworthiness of that person. Banks and credit card companies use credit scores to evaluate the potential risk posed by lending money to consumers and thus mitigate losses due to bad debt. Credit scoring is, however, not limited to banks. Other organizations, such as online retailers, mail order services, mobile phone providers, employers and landlords, may use the same techniques.

To date, credit scoring had not been specifically regulated and, while very common, was carried out in a somewhat grey legislative area.

Further, despite pressure from industry and the German *Länder* (the federal states) the new rules also apply to consumer scoring techniques employed mainly for marketing purposes, such as the use of address data to customize marketing campaigns, but also to insurance providers for determining insurance eligibility and premiums.

The amendments, incorporated in the Federal Data Protection Act (the Bundesdatenschutzgesetz, or BDSG)[1] will become effective April 1, 2010.

In an effort to increase transparency, the amendments provide that individuals must be notified in advance if their data are to be used for scoring purposes. Where individuals' address data are used, the provision of notice to the individual must be documented. Upon request, individuals must be provided with detailed information including the data used, an "understandable explanation" about the scoring technique employed, and the credit scores that have been recorded over the past six months. Moreover, an individual's credit score may not be lowered just

because of exercising a right to access credit check information held about him or her (which is common practice in the United States).

The new rules allow financial institutions to share certain credit data with others, and in particular credit agencies, based on mere notice. Consent is no longer necessary.

The use of scoring to determine the conclusion, performance, or termination of contractual relationships, such as the eligibility for a credit, is permitted where (i) there is evidence that data pertaining to an individual can be used to conduct certain mathematically scientific probability calculations (a requirement that may be particularly problematic for marketing scoring), and (ii) general data protection requirements have been complied with. For the latter, opt-in consent may be required.

The new rules also establish, for the first time, when credit information may be used for scoring purposes. In brief, an individual's payment history information may be used and shared for scoring purposes if a previously adjudicated court insolvency order is in place, if an individual has formally acknowledged a debt, or if an individual has been provided with two or more unpaid demand letters sent over a time span of at least four weeks. Sharing of payment history information between affiliated entities is subject to the same requirements.

Substantial financial penalties for failure to comply with the new requirements have been introduced.

Opt-In for Consumer Telemarketing

The German Parliament also approved penalties amounting to €50,000 (approx. \$71,000) for failure to obtain opt-in consent prior to contacting consumers by telephone for marketing purposes. According to the legislative materials, these penalties may be imposed on telemarketing agents and service providers, their customers, or any other organization engaged in telemarketing.

Under the existing Act against Unfair Trade Practices (the Unlauterer Wettbewerbsgesetz, or UWG), telemarketing to consumers is already subject to opt-in consent. The bill amending the UWG^[2] requires that such consent contain "a declaration of will," and may not be determined merely based on the individual's behavior. The wording of the bill also clearly states that each and every call by telemarketers, even the very first one, would be covered by these restrictions. Telemarketing to businesses is permitted if it may reasonably be concluded that the recipient wishes to be contacted.

Further, marketers who fail to display their telephone numbers on caller ID systems may be fined up to €10,000 (approx. \$14,000).

The amendments also enable consumers, who have not been appropriately informed of their right to withdraw from a service contract concluded at a distance (such as over the phone or via the Internet), to exercise this right of withdrawal, even in cases where portions of the services have already been rendered. This right would only expire when all portions of the services have been performed at the request of the consumer.

The right to withdraw could also extend to contracts concluded over the phone relating to the delivery of newspapers, periodicals, and magazines, or for gaming and lottery services. Such contracts are expressly excluded from the right of withdrawal provided for in the European Union Distance Selling Directive 97/7, but withdrawing from them looks set to become easier in

Germany in the future. As so often happens, German consumer law would therefore be going further than corresponding EU law.

The German Federal Network Agency, which monitors developments in national telecommunications, gas, electricity, and railway markets, has been charged with supervising the new law. The generally held view is that these requirements will apply to telemarketing to German recipients, irrespective of the location of the provider. These amendments are expected to enter into force, without any transition period, at the end of July once published in the Official Journal.

Location Tracking Services

Amendments to the Telecommunications Act (the Telekommunikationsgesetz, or TKG)[3] which were approved recently by the German Parliament will seriously impede navigation, friend-finder, and other mobile services that require the continuous transferring of the user's location.

The amendments first require that telecommunications providers obtain "express, distinct, and written" consent from subscribers if the location of his/her device is tracked and transferred to other subscribers, including to third parties (other than the value added-service provider). As a result, providers who offer subscribers the option of having their locations determined and forwarded (e.g., for friend-finder services or for tracking a misplaced device) will need to obtain distinct, written consent from these subscribers. Under German law, this means pen on paper or qualified digital signatures, since e-mail or click through consent is not sufficient. Moreover, the word "distinct" indicates that the consent wording may not be included in general subscriber terms and conditions, but must be separated from such text.

Second, the amendments permit providers to track a subscriber's location a maximum of five times. After the fifth time, the subscriber must be notified before further location tracking can take place (unless he/she has opted out of such notice). In addition, the law requires providers to accommodate the needs of disabled persons, such as by providing specific telephone tools for hearing-impaired persons.

The Network Agency has been charged with enforcing these rules, and failure to comply with the consent and notice requirements may result in penalties of up to €300,000 (approx. \$420,000). Arguably, all location tracking services currently aimed at the German market are within the scope of the new requirements, including services provided by operators outside Germany.

These amendments will become effective once signed by the German president and published in the Official Journal. No transition period is provided for in the law.

Breach Notification, Strict Rules for Marketing, and Other Amendments

Designed to prevent and address recent data breaches, the German government has proposed further amendments to the Federal Data Protection Act[4] that, if approved by the Parliament, will provide for (i) the introduction of a mandatory breach notification regimen, (ii) the requirement to obtain opt-in consent for the secondary use of contact details for marketing purposes and in particular for data trading, (iii) increased enforcement, as well as (iv) a voluntary data protection audit scheme. However, due to the ongoing debate in Parliament and much criticism from industry, the bill amending the BDSG may not be voted into law before the summer break and the general elections. This means that under German constitutional rules the new government will have to present the bill anew.

notification requirements in cases where any of the following sets of data are leaked: sensitive data, criminal records, bank account or credit card data, or personal data subject to legal privilege (e.g., data held by lawyers, doctors, journalists, etc.). The proposed rules only require notification in cases where the data leakages may lead to "serious impediments for privacy and other individual interests." The legislative commentary states that the types of data, as well as the possible results of the breach (such as damages or identity theft), must be taken into account when assessing whether such "serious impediments" exist. Both the data protection authorities, as well as all individuals concerned, must be notified "immediately" (as soon as reasonably possible) after containment and as soon as such notification no longer impedes law enforcement (principle of responsible disclosure). In cases where a broad public is concerned, public announcements in at least two national newspapers may replace individual notices. These announcements must be at least half a page tall. The notice should include information on the data leakage, possible results of the leakage as well as measures being taken to mitigate damages.

The breach notification requirement also extends to electronic communications providers and telecommunications operators in any case where user data (e.g., registration data obtained by a Web site operator) are leaked. Interestingly, public authorities are exempt from breach notification.

The provision of potentially greatest commercial significance is the abolition of the "list privilege," whereby contact details are traded amongst marketers. According to industry representatives, the proposed amendments would effectively kill legal trade in marketing data. Data collected prior to the entry into force of the amendments may continue to be processed until July 2012. After that date, opt-in consent will be required, even for existing databases in which organizations may have invested significant resources, and data may need to be destroyed.

Under the list privilege system, data brokers as well as other organizations, process data lists consisting of names, addresses, dates of birth, professions, and other specified data for marketing and market research purposes, without prior opt-in consent. The draft amendments would make any processing of such data for marketing purposes, including market research, subject to opt-in consent.

The draft does provide an exception allowing processing based on opt-out consent in cases where (i) the details are used for marketing and market research purposes in relation to products or services of the data controller (which presumably excludes marketing and market research for affiliates), and (ii) all data have been collected directly from the individual. Marketing for charities as well as business-to-business (B2B) marketing seem to be exempt too, provided that the marketing is sent to the individual's work address and that it relates solely to products and services intended for commercial use. However, the wording for the B2B exception is awkward in that it restricts the exception to entrepreneurs and contractors, and does not seem to permit marketing to employees of larger enterprises. Where marketing or market research is permitted with opt-out consent, individuals must be able to opt out upon establishment of the relationship. Under existing law, opt-out options only had to be provided when follow up marketing contacts were made, not beforehand.

Where opt-in consent is required, consent must be provided in writing or through qualified digital signature. Electronic consent is permitted if documented and if individuals are easily able to retrieve the wording of their consent and or withdraw it at any point in time. Where specific circumstances render oral consent permissible, for example during a telephone conversation, the amendments now propose that such oral consent must be confirmed in writing.

Marketing consent must also be separate from other declarations (including the general data

Morrison & Foerster LLP

protection consent), and a separate signature, tick or click must be provided (and the confirmation obtained) in order to process data for marketing and market research purposes. Withdrawal of consent may not be subject to stricter requirements than those governing the entering into of the agreement. The rule under German law is that consent must be in writing, meaning pen on paper or by use of a qualified digital signature.

Last, the provision of products or services may not be made conditional upon providing consent for marketing, unless the individual may purchase similar products or services under reasonable conditions elsewhere, that is, where the provider has no monopoly and market conditions are not such that other providers impose the same requirement for consent. No further guidance is provided as to what would constitute "reasonable conditions" or "similar" products or services.

The draft also contains a number of proposals that are aimed at strengthening compliance and enforcement: Internal data protection officers (DPOs) may not be terminated during their term as DPOs, or during the 12 months thereafter, unless there is an "important cause" requiring immediate termination. Organizations must also compensate DPOs for training courses. Penalties are increased to €50,000 for failure to comply with formalities and to €300,000 for other data protection breaches (approximately \$70,000 and \$420,000, respectively). The draft expressly stipulates that higher penalties should be assessed to ensure that the penalties exceed the commercial gains that organizations may make from breaches. Further new penalties have been introduced, including for failure to comply with the restrictions on processing for marketing and market re-search purposes; or for failure to have detailed written data processing agreements in place with a data processor, irrespective of the location of that processor, and irrespective of whether the processor is an independent service provider or an affiliated entity. According to the German authorities, a master agreement between the parent and the provider is insufficient in cases where data relating to the German affiliate are processed.

Finally the amendments propose the introduction of a voluntary data protection audit with auditing and certification conducted by independent certified firms, in turn monitored by data protection authorities. The government would be charged with setting up a regulatory committee to develop guidelines for data security regulations covering private sector companies.

Employee Privacy

The German government has also reopened the debate on a proposed law to protect employee data, in response to recent breaches. Secretary of the Interior, Wolfgang Schäuble, who made the announcement Feb. 16, stated that this law should address issues relating to the monitoring of employee communications and Internet usage in the workplace, as well as the use of video surveillance and GPS navigators tracking workers in company cars, and, in particular, the processing of personnel files and health data. "In certain cases, employers need to have the right to control employees," Schäuble said, "but it is a question of the right proportionality."

Peter Schaar, head of Germany's Data Protection Commissioner's Office in Bonn, alluded to recent breaches of employee data, stating that data "provided in the context of a work relationship should not be used for other matters," and that the new law, if passed, would tighten restrictions on employee data in Germany.

The proposed law would come after a decade of fruit-less lobbying by privacy advocates about the need for an employee data protection act in Germany. Given this, it is still unclear whether the law will ultimately be enacted. Schäuble himself has warned that substantive discussions will only begin after the general elections. Until then, Schäuble has merely invited the German Labor Minister, the Minister for Economics, the Federal Data Protection Commissioner, and

representatives of trade and industry to evaluate "whether there is a need for an employee data protection law."

Conclusion

Given the current economic circumstances and the volatility of the German data protection landscape, organizations need to remain vigilant regarding data protection issues. Compliance with data protection and security requirements, while more and more challenging, is clearly the focus of growing scrutiny, and penalties for non-compliance are increasing.

Reproduced with permission from Privacy & Security Law Report, 8PVLR27, 07/06/2009.
Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com/>

Footnotes

[1] Gesetz zur Änderung des Bundesdatenschutzgesetzes. Available (in German) [here](#).

[2] Gesetz zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen. Available (in German) [here](#).

[3] Erstes Gesetz zur Änderung des Telekommunikationsgesetzes und des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln. Available (in German) [here](#).

[4] Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften. Available (in German) [here](#).

The New Set of EU Model Clauses for Service Providers

By Anthony Nagle, Karen Retzer, and Gemma Anderson

Introduction

After years of discussions, EU regulators have issued a new set of Standard Contractual Clauses to legitimize the transfer of personal data to countries outside the European Economic Area (EEA).¹ The new set of clauses reflects the reality that organizations subcontract and may be of particular use in the outsourcing arena and for intra-group transfers to centralized service centers. For the first time, organizations that outsource services involving personal data can transfer that data to their suppliers located outside the EEA, and those suppliers can in turn pass it to subcontractors for further processing, without the need for the customer organization to take any further steps. Such sub-processing of data is built into the terms of the new contractual clauses.

Decision 2010/87/EU² (the "Decision"), adopted by the European Commission in February 2010 (the "New Model Clauses") updates and replaces the prior existing Standard Contractual Clauses for Processors, approved by Commission Decision 2002/16/EC (the "Old Model Clauses") for the transfer of personal data outside the EEA by data exporters (the "Controllers") to data importers processing data on behalf of Controllers ("Processors").³

One of the key changes introduced by the New Model Clauses is that in certain situations the transfer of personal data from a non-EU service provider to its sub-processors will be "automatically" covered by the terms of the New Model Clauses.

Although some concerns regarding the New Model Clauses remain, the outsourcing industry (or organizations interested in centralizing data processing within the corporate family to affiliates located outside of the EEA) are likely to view the new changes as a positive step which provides further clarity about how organizations can comply with the EU data protection laws that govern such personal data transfers.

Customers and suppliers will need to incorporate some new processes and governance arrangements into their outsourcing and/or data transfer arrangements, in order to ensure they comply with all of the changes introduced by the New Model Clauses.

The previous transfer regime

Prior to February 2010, the European Commission had approved three sets of model contractual clauses: two types of Controller-to-Controller model contract clauses and one set of Controller-to-Processor model contract clauses (i.e., the Old Model Clauses).

However, to the ire of Controllers and Processors alike, the European Commission had never put in place any contract clauses to cover the transfer of personal data from Processor-to-Processor or Processor-to-sub-processor, which is a common feature in most data processing arrangements, in particular in outsourcing and intra-group transfers outside the EEA. When the Old Model Clauses were being developed, the European Commission also failed to build in a mechanism that would provide an automatic "flow-down" of provisions to sub-processors; this could have allowed adequacy⁴ to be achieved under Article 25. In the absence of such a mechanism, Controllers and Processors have been complaining that they have to put additional contractual arrangements in place with sub-processors (i.e., in addition to the main services contract and processing agreements between the Controller and Processor), or that they have to

Beijing

Paul D. McKenzie	86 10 5909 3366
Jingxiao Fang	86 10 5909 3382

Brussels

Karin Retzer	32 2 340 7364
Teresa V. Basile	32 2 340 7366
Antonio Seabra Ferreira	32 2 340 7367

Hong Kong

Gordon A. Milner	852 2585 0808
Nigel C.H. Stamp	852 2585 0888

Los Angeles

Mark T. Gillett	(213) 892-5289
Michael C. Cohen	(213) 892-5404
David F. McDowell	(213) 892-5383
Russell G. Weiss	(213) 892-5640

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Chris Coulter	44 20 7920 4012
Suzanne Horne	44 20 7920 4014

New York

Gabriel E. Meister	(212) 468-8181
Joan P. Warrington	(212) 506-7307
John F. Delaney	(212) 468-8040
Madhavi T. Batliboi	(212) 336-5181
Marian A. Waldmann	(212) 336-4230
Michiko Ito Crampe	(212) 468-8028
Miriam Wugmeister	(212) 506-7213
Sherman W. Kahn	(212) 468-8023

Northern Virginia

Daniel P. Westman	(703) 760-7795
Timothy G. Verrall	(703) 760-7306

Palo Alto

Bryan Wilson	(650) 813-5603
Christine E. Lyon	(650) 813-5770

San Francisco

Roland E. Brandel	(415) 268-7093
James McGuire	(415) 268-7013
William L. Stern	(415) 268-7637
Jim McCabe	(415) 268-7011

San Diego

Mark R. Wicker	(858) 720-7918
----------------	----------------

Tokyo

Daniel P. Levison	81 3 3214 6717
Jay Ponazecki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

Washington, D.C.

Andrew M. Smith	(202) 887-1558
Cynthia J. Rich	(202) 778-1652
Julie O'Neill	(202) 887-8764
Nathan David Taylor	(202) 778-1644
Obrea O. Poindexter	(202) 887-8741
Oliver I. Ireland	(202) 778-1614
Reed Freeman	(202) 887-6948
Richard Fischer	(202) 887-1566

implement other adequacy arrangements to ensure their compliance with Article 25. The New Model Clauses were developed to address this gap.

New Model Clauses: What are the main changes?

Sub-processors

The most significant change introduced by the Decision is that, for the first time since the Model Clauses were introduced, non-EU Processors are expressly authorized to appoint sub-processors, providing the following conditions are met:

1. the Processor informs the Controller of its intention to sub-contract all or part of the processing and obtains the Controller's prior approval in writing;
2. the sub-processor may only affect processing operations specified in the main contract between the Controller and the Processor, *i.e.*, the sub-processing cannot relate to a different set of processing requirements;
3. the Processor must enter into a written contract with the sub-processor which imposes the same obligations on the sub-processor as are imposed upon the Processor by the main agreement with the Controller, including the incorporation of third party beneficiary rights against the sub-processor (which will allow individuals to establish contractual claims directly against the sub-processor, but will be limited to the sub-processor's own processing operations), and the application of the law of the relevant EU Member State where the Controller is established, *i.e.*, this will be the governing law of the sub-processing contract. The New Model Clauses contain a guidance note which states that the requirement to enter into a written contract with the sub-processor may be satisfied by the sub-processor co-signing the contract entered into between the Controller and the Processor;
4. the Processor must give copies of its contracts with the sub-processor to the Controller;

5. the Controller must retain and annually update a list of sub-processing agreements concluded by, and with notification from, the Processor and this list shall be available to the Controller's DPA upon request;
6. the Controller must make available any contract for sub-processing to a data subject upon request (excluding commercial information); and
7. DPAs have audit rights against the Processor and sub-processor for the purpose of confirming whether the Processor and sub-processor have destroyed or returned all personal data to the Controller at the end of the contract.

Significantly, the New Model Clauses define sub-processor as "*any processor engaged by the data importer or by any other sub-processor of the data importer*", meaning that, to the relief of outsourcing customers and suppliers, entire chains of sub-processors (including sub-sub-processors and so on) will be covered by the New Model Clauses. This is something not all Member State DPAs have permitted in the past, for example, Hungary did not previously permit chains of sub-processors.

Liability

The liability provisions have also been updated by the Decision to reflect the introduction of sub-processing arrangements.

Processor to Controller. If the sub-processor fails to fulfill its protection obligations, the Processor remains fully liable to the Controller for the performance of the sub-processor's contractual obligations.

Controller/Processor/sub-processor to data subjects. Under the New Model Clauses, individuals may bring claims for a breach of their third party beneficiary rights or the provisions regulating the appointment and processing activities of a sub-processor against the sub-processor, where both the Controller and the Processor have factually disappeared, or ceased to exist, or become insolvent (although the claim will be limited to the sub-processor's own data processing operations).

New notice requirements

The New Model Clauses introduce a requirement to notify individuals about transfers to Processors if sensitive data are transferred. Sensitive data include information such as details on racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in trade unions, health conditions and sex life, or information on judicial proceedings and criminal records. Also, perhaps in response to requests from US authorities, there is a new obligation imposed on the Processor to notify the Controller if it receives requests for disclosure from authorities. The Processor must also immediately inform the Controller about security breaches or access requests from individuals.

When do the New Model Clauses take effect?

The New Model Clauses will come into force on May 15, 2010. Notably, the New Model Clauses completely replace the Old Model Clauses and will not operate in parallel with them (in contrast to the two prior approved sets of Controller-to-Controller model clauses). Existing Controller-to-Processor contracts will continue to be valid only for the period that the transfers and data processing operations that are the subject matter of the contract remain unchanged. Although the precise extent of the "change" required to invalidate existing contracts is unclear, parties wishing to make changes to their processing agreements after May 15, 2010 will be required to enter into a new contract that complies with the New Model Clauses.

Also, for arrangements that include the use of sub-processors, the parties face the choice of either redrafting the arrangement with the Processor based on the New Model Clauses, or entering into Model Clauses with each sub-processor. As a result, and given the frequent use of sub-processors in existing service contracts, particularly in the outsourcing arena, many organizations will need to amend their existing agreements by putting the New Model Clauses in place for their outsourcing arrangements.

Practical considerations for customers and suppliers

The Decision expressly states that the New Model Clauses do not apply to Processors established in the EU (*i.e.*, those who perform processing on behalf of the Controller established in the EU) who sub-contract their processing to sub-processors established in countries outside the EEA. The approach of individual Member States of the EU will no doubt vary in this regard. One of the practical implications is that if a Processor is located within the EU and the sub-contractors that process data on its behalf are located outside the EU, the Controller may need to directly enter into the New Model Clauses with the sub-processor to comply with its obligations (unless it chooses another adequacy approach as outlined above). Controllers will need to understand how personal data flows in their outsourcing and/or data transfer arrangements to enable them to identify the correct processing entities that will need to enter into the New Model Clauses.

Although the New Model Clauses will be welcomed overall by Controllers as another tool to achieve compliance where sub-processing is involved, for some Member States, the New Model Clauses will place more onerous requirements on Controllers and on Processors to put arrangements in place with its sub-processors.

Controllers must make any contract for sub-processing available to individuals upon request, and this would include the New Model Clauses or any specific sub-processing agreements. However, the Controller does not have to make detailed security requirements for the processing (those that are contained in “Appendix 2” of the New Model Clauses) available to individuals, but it must provide a summary of those security requirements upon request. If the New Model Clauses or the sub-processing agreements contain any commercial information, it may be removed from the documents before providing them to the individuals. As a matter of good governance and to ensure the Controller can address any requests promptly, when the

New Model Clauses are being signed, Controllers and Processors may agree upon an appropriate version to make available to individuals who request a copy.

The Processor must also notify the Controller if: (i) it receives a request for disclosure from authorities (unless there is a confidentiality requirement); (ii) it receives an access request from individuals; or (iii) there is a security breach. The impact of this requirement is that a Processor may need to develop new governance arrangements with its sub-processors so that it gains access to this information as quickly as possible to enable it to promptly pass such information up the chain to the Controller.

The New Model Clauses permit DPAs to audit the full chain of sub-processing and (where appropriate) make binding decisions on the Controller, Processor and sub-processor under the applicable data protection law. In addition to the list of sub-processing agreements that the Controller must maintain as described above, the Processor is required to inform the Controller promptly of the existence of legislation applicable to it or any sub-processor, preventing any audit of the Processor or any sub-processor by the Controller’s DPA. In practice, these requirements will place an additional burden on Processors and their sub-processors to establish whether their local legislation impacts the audit rights to which they will be agreeing under the New Model Clauses and any separate sub-processing agreements.

Finally, after May 15, 2010, Controllers will need to use the New Model Clauses for transfers to non-EU Processors and, with respect to existing contract arrangements, Controllers will need to be aware of, and monitor any amendments to, existing Controller-Processor arrangements that might trigger a requirement to amend existing contracts to include the New Model Clauses. Controllers should already be working with their Processors to establish the current “baseline” status of their processing arrangements relating to transfers outside the EEA and should then continue to monitor that baseline position from May 15 onwards, putting the New Model

Clauses in place, if and when required, e.g., where sub-processors are used. ■

- 1 The European Economic Area (EEA) is comprised of the 27 EU Member States (currently Austria, Belgium, Bulgaria, the Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom), Iceland, Liechtenstein, Norway and Switzerland.
- 2 Commission Decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to Processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593).
- 3 A Controller is an organization that makes decisions about what information is collected, how it is used, with whom it is shared and where it is processed and is typically the customer. A Processor is an organization that acts on the instructions of a Controller and is typically a service provider.
- 4 Directive 95/46/EC (the “Directive”) restricts cross-border transfers of personal data to third countries outside of the EEA that have been found to ensure an “adequate” level of protection. To date, the European Commission has deemed adequate the laws of Argentina, Canada, the Channel Islands (Guernsey and Jersey), the Isle of Man, Switzerland, as well as the United States, where organizations comply with the Safe Harbor accord. The Directive also provides several exceptions that allow for transfers of personal data outside the EEA where there is no “adequacy” determination in place for the relevant jurisdiction, including use of the template Model Clauses.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, Fortune 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last six years, we’ve been included on *The American Lawyer’s* A-List. *Fortune* named us one of the “100 Best Companies to Work For.” We are among the leaders in the profession for our longstanding commitment to pro bono work. Our lawyers share a commitment to achieving results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

www.mofo.com

©2010 Morrison & Foerster LLP

Cloud Computing and Outsourcing: Is Data Lost In the Fog?

Julian Millstein and Matthew King

Licensing + Technology Transactions, Outsourcing, Privacy + Data Security

6/15/2009

Client Alert

Cloud computing is here. And if it isn't at your company yet, it soon will be. Cloud computing is simply the latest version of the historical use of technology to increase flexibility and reduce costs. By providing a bundled and scalable solution of software, infrastructure, data storage and communication, cloud computing providers allow companies to reserve cash, avoid expensive IT commitments, efficiently scale usage based on need, and launch new services quickly. However, there is truly no free lunch - at this point in its development, outsourced cloud computing fails to address important questions of legal risk associated with knowing where data is stored and transmitted. This Alert discusses several of these issues, which must be considered by companies turning to third-party cloud computing solutions.

First, of course, we need to define what we are talking about, because there are many definitions of "cloud computing." Recently, a CIO we know defined it as a computing utility of virtual servers that are controlled by an organization and accessible to end-users via the Internet. We define cloud computing as the provision of business applications that are accessible via the Internet using software and data stored on virtual servers. Cloud computing offers a commoditization of business technologies: infrastructure as a service, software as a service, and platform as a service, all online and in a Web 2.0 framework. When a third party controls any aspect of the "cloud," issues are created regarding data security, privacy and legal compliance. In a way, this has been the case ever since fixed data lines were replaced by communication solutions that bundled data from several companies. The third party tries to fully exploit the efficiencies of virtualization and commoditization of several traditionally proprietary functions (infrastructure, platform and software), but creates substantial legal risk at the same time.

The benefits of third party solutions to commercial applications are well established. From third-party software solution providers who leveraged the requirements of multiple customers, to outsourced infrastructure providers who invest in faster and better technology solutions than is possible for any single customer, third parties have always been able to use efficiencies of scale and commoditization to drive down the costs of providing a function. However, with these benefits come risks, some of which are highlighted below.

Data Storage and Transfer

In a conventional outsourcing arrangement, the customer can negotiate control over the location of its data, including where backup operations will be conducted. This knowledge allows the customer and provider to know which regulatory schemes apply and to comply with the relevant data transfer laws. Outsourced cloud computing, however, can be delivered at a cost-effective price because the provider can move data around the world, perhaps splitting it up and sending it to different locations, depending on capacity, use and bandwidth. This freedom may result in non-compliance with the myriad worldwide regulations pertaining to storage and transfer of data.

Historically, the negotiation of risk between a provider and customer in an outsourcing arrangement usually relied on the customer requiring the provider to adopt certain processes that would result in data transfer regulatory compliance. Absent these requirements, providers were “not in the business” of concerning themselves with the specific legal data obligations applicable to the transfer and storage of the customer’s data. But over time, providers have realized that to be responsive to customers, and still obtain economies of scale, they must integrate these requirements into their more generic solutions. Eventually, then, we believe cloud computing providers will internalize substantial parts of data transfer regulatory compliance into their commoditized offerings, accepting that the cost of compliance can be leveraged across a large-enough user community and built into the price.

For example, one early cloud provider allows the customer to have some control over where data is stored for selected services, through “availability zones.” Because data transfer laws are country-specific, a cloud provider could store data in certain, pre-determined geographic regions (for example, the European Economic Area) and comply with the requisite transfer obligations for moving data out of the area. This way, data could be transferred endlessly within a cloud provider’s European servers without running afoul of any data protection laws, because data is only stored only in a specifically requested region.

Data Security

Data security and data protection is always a major concern in any outsourcing arrangement. Outsourcing contract schedules specify exacting security management techniques that must be utilized by the provider. And, again, much of this is driven by data protection regulations for sensitive data, whether financial or personal. How can this be handled with a cloud computing solution? The CEO of Cisco has said that cloud computing “is a security nightmare and it can’t be handled in traditional ways.”[*] For most companies, data security and data protection are the biggest barriers to outsourcing cloud computing for any applications that involve sensitive or confidential data.

As with ASP, telecom transport, and Service Bureau agreements, cloud computing agreements will tend to be one-sided and not easily negotiated. For example, one cloud provider contract that is entered into online is non-negotiable and very provider-friendly: The provider makes no representations as to data security; places sole responsibility for security, protection and backup of data on the customer; and disclaims all liability for unauthorized access, use, corruption, deletion or loss of any data.

Therefore, contracts with cloud outsourcing providers will require more due diligence and involve less negotiation of terms and conditions. Customers should be concentrating on whether the cloud solution keeps them in regulatory compliance, and ultimately customers will rely on the provider’s documentation of its solution as being compliant (either directly – as with a software release for banking or healthcare software - or indirectly, as in defining with specificity the locations where data will be stored). Consequently, a failure of the provider to keep the customer in compliance could be a failure of the service to comply with its own specifications, and result in a contractual damage remedy.

In due diligence, as in any outsourcing arrangement, reviewing the provider’s solution to determine control of access to the data is crucial. Does the provider’s solution allow you to limit access rights to your data, and monitor access so you know who accessed what and when? What are the specifications regarding encryption? How frequently is data archived, and are all applications and software kept current with the most recent security updates? Do service-level

agreements include maintenance of security systems as a measured performance obligation?

Changing Providers

Another risk that must be considered in contracting for outsourced cloud computing services is to assure business continuity upon termination of the service. Most negotiated outsourcing agreements have negotiated exit plans and transition services, including delivery of data in a format that can be utilized with another provider or an in-house solution. A typical cloud service provider agreement would not address these concerns. For example, an online cloud provider contract allows the provider to terminate the agreement at any time and have no obligation to maintain your data. At best, it promises not to *intentionally* erase any of your data for 30 days. This will not do. You must negotiate for termination services, including transition to another provider or in-house, and you should make sure data is routinely delivered to a back-up provider to ensure continuity of service in the event of a catastrophic failure.

Other Risks

Cloud computing solutions have many risks in common with other outsourced solutions, but these risks are harder to mitigate through negotiation. For example, outsourcing means transferring the measurement and reporting of service levels to the provider, relying on the provider's infrastructure to deliver key performance information. In a cloud solution, however, there is even less room for customization. Similarly, unless carefully negotiated, most outsourcing agreements yield inadequate compensation to the customer if things go wrong or the relationship doesn't work out; yet the cloud relationship tends to provide less room for negotiation of alternative remedies than a traditional outsourcing relationship does. Thus, where negotiated language is hard to achieve but the price of the cloud solution is too good to pass up, consider management of the risks through use of alternate providers, and similar techniques.

Suggestions

Because your company is liable for the way its data is handled, take steps to ensure that the cloud provider is complying with its obligations. Here are some data protection measures that are helpful when using cloud computing outsourcing:

1. Determine if cloud computing outsourcing is right for your application. If the function you seek to outsource involves sensitive information, it may not be the right choice. There will be transactions where cloud computing simply does not make sense until a robust offering that includes compliance is available.
2. Encrypt data before you send it to the cloud. Industry professionals agree that this is a good way to limit potential risk.
3. Control access to the data. Make sure that the provider has limited the people who can access your data, and ensure that access is properly monitored.
4. Keep in mind e-discovery obligations and the possible need to retrieve electronic records from the provider on relatively short notice.
5. Comply with all necessary regulations. Because your company bears the brunt of complying with data protection laws, make sure you know where data may be stored. The cloud provider must give you this information so you can assess the risk of non-compliance. If the provider does not share this information, then no sensitive information should be

transmitted.

6. Control data location, if possible. This is the best way to ensure that the provider (and, by extension, the customer) is complying with data security laws. Limit the cloud to a definitive set of locations.
7. Make sure the provider is updating its protection systems, both as required by the contract and in accordance with industry best practices.
8. Ensure appropriate disaster recovery and business continuity plans are in place. Require the provider to archive your data so that it can be accessed if the system goes down.
9. Backup and/or store your data periodically with a party other than the cloud provider.
10. Use technology and compliance audits to be sure that data is secure and that systems are properly integrated.
11. Have clear procedures in place for the return of data in the event of termination or provider bankruptcy.
12. Actively monitor the relationship, and utilize service levels to ensure that the provider is complying with its obligations. Cloud computing outsourcing is no different from any other type of outsourcing in this regard: Success requires the customer to actively manage and oversee the relationship!

Footnotes

[*] R. McMillan, "Cisco CEO: Cloud Computing a 'Security Nightmare'," available at http://www.csoonline.com/article/490368/Cisco_CEO_Cloud_Computing_a_Security_Nightmare_

“Deciphering Due Diligence:
Tackling The IT Issues That Can Cripple A Business Transaction”

Diligence of Software and IT Systems “Inside” the Firewall

Jason Haislmaier, Holme Roberts & Owen LLP

I. INTRODUCTION.

A. Role of Diligence. A fundamental tension exists in any technology-based M&A transaction between the position of the buyer and that of the target company. The buyer will typically be interested establishing a clean “bill of health” regarding the software, information technology (IT) systems, and other technology relevant to the transaction. The target on the other hand is typically focused on bringing certainty to the transaction and “tightening-down” on open-ended liability obligations.

In this context, buyers will often default to placing a great deal of reliance on representations, warranties, and indemnification provisions in the M&A agreement to help establish a clean record. In the context of an M&A transaction in which software and IT systems represent a material part of the value of the transaction, however, representations and warranties alone are an imperfect means for a buyer to accomplish this goal. Sellers will typically push-back against overly-broad reps and warranties, typically narrowing the scope of the reps and warranties and often rendering them difficult to interpret at all. Likewise, disclosure schedules covering software and IT systems are seldom detailed enough to bring true visibility into the software or IT systems subject to the rep or warranty. As a result, it is often a practical challenge to even prove whether a breach of a rep or warranty has actually occurred. Even in the case that a breach can be proven, liability baskets and caps typically limit the ability of a buyer to obtain meaningful financial recourse for the breach.

Thus, a buyer’s protection and ultimate recourse in the case of a breach of a rep or warranty will typically be quite limited – and often simply too later to provide any meaningful recourse at all. A well-structured diligence review can thus play a key role in augmenting a buyer’s visibility into potential issues regarding a target’s software and IT systems. Properly timed, diligence can occur well before reps and warranties come into play, at a stage where stopping or materially modifying the transaction to account for issues identified by the diligence review is still truly possible.

B. Goal of Diligence. Buyers conducting diligence reviews of software and IT systems are encouraged to keep an open and active mind-set. At the outset, a buyer should establish the expectation with the target that the diligence review will be about facilitating the transaction rather than stopping it. In this context, a buyer should consider enlisting the target to help the buyer in obtaining and analyzing information about the nature and quality of the target’s relevant software and IT systems. Based on this information, the buyer may choose to seek assistance from the target to identify potential issues relevant to the value of the transaction and to develop solutions or mitigation plans for those issues.

Rather than looking at diligence as something to be avoided, targets often do far better to view diligence as an opportunity to assist the buyer in understanding and developing plans to address and mitigate relevant issues. In many cases, airing issues early in a transaction can serve to lessen the impact on the transaction itself, allowing time for the issue to be addressed on a technical issue rather than through changes to reps, warranties or indemnifications, price adjustments, or stopping the transaction entirely.

II. PRELIMINARY CONSIDERATIONS.

A. Transaction Structure. Prior to beginning any M&A diligence review, including one regarding software or IT systems, it is critical to identify and understand the structure of the transaction. Typical M&A structures will include:

1. Asset purchase
2. Stock sale
3. Merger (e.g., reverse or forward merger)

Simply put, different transaction structures will raise different issues for, and place different requirements on, the diligence review preceding the transaction. For example, while all transactions merit diligence of software and IT systems that are material to the value of the transaction, asset sales will often merit a more detailed review of software and IT systems, and relevant rights held in those software and IT systems, to ensure that no relevant rights or assets are left out of the transaction.

B. Identification and Location of Key Diligence Resources.

1. Initial Questions. Prior to commencing a diligence review, it can be helpful to develop a list of questions regarding the resources that will be needed to complete the review. For example:

- (a) Who are the relevant sources of information on matters involving software and IT systems matters (e.g., in-house counsel, IT personnel, or outside counsel)? Are those resources located within the target's organization or at a third-party provider?
- (b) Does separate counsel handle issues relating to software or IT systems for the target (versus traditional IP issues)? Will it be necessary to contact this counsel to complete the diligence review?
- (c) How long has each relevant party been involved in handling the target's software and IT issues? Is it necessary to consult multiple sources to obtain historical information required by the buyer?

2. Key Personnel. While the general counsel (or other in-house counsel) is often the primary contact for diligence, he or she may not be the most knowledgeable about software and IT systems. Often, other personnel within the target's organization (or outside of the target's organization) will be better-equipped to aide in the diligence of software and IT systems. For example:

- (a) Chief Information Officer (CIO)
- (b) Chief Technology Office (CTO)
- (c) Human Resources (HR)
- (d) Outside IT, IP, technology, or privacy counsel
- (e) Outside technical experts

Even in the case where the target does not employ outside technical experts, it may be necessary to include such experts on the diligence team. Identifying particular areas of buyer concern early in the diligence process and determining whether outside technical experts will be needed to augment the core legal team to address these areas of concern is often one of the keys to a successful diligence review.

3. Key Documents. Documents relating to software and IT systems may not be included in a typical data room. Care should be taken to avoid overlooking these documents. For example, documentation relating to the warranties, service levels, or performance characteristics applicable to IT systems may need to be obtained from IT staff who are not directly involved in the transaction. Likewise, IT-related documents in data rooms can become outdated during the diligence process. It is important to scope out the location of key IT-related documents, particularly those that may fall outside of a typical diligence request or data room.

4. Key Third-Parties. Almost no software or IT system is entirely developed or owned by the target organization making use of that software or system. Rights held by third-party licensors of software and providers of IT systems are thus relevant to nearly all software and IT diligence reviews – and deciphering those rights can often be one of the trickiest issues in the transaction. Make an early identification of third-party rights holders or providers who play a key role the successful operation of the organizations' IT systems (or who may be in a position to hold up the deal).

5. Key Assets. Of course, a detailed schedule of the key software and IT systems subject to the transaction will ultimately be required in the definitive M&A agreement. However, you should determine early on in the transaction (as early as possible) the nature of the material software and IT systems of the target organization. This can include the type, quantity, location, materiality, jurisdiction of those assets as well as other information relevant to those assets. Often, the time and manpower required for the diligence review will be directly related to the nature of the assets being reviewed.

C. Materiality. As with any diligence exercise, attempting to perform diligence on *all* software and IT systems in a target's organization can be a daunting task - if not impossible. It is essential to understand how material any given software or IT system is to the business of the target organization subject to the transaction and the value being conveyed to the buyer in the transaction. It is then equally important to tailor the level of detail and the areas of focus of the diligence review based on this information, taking into account buyer expectations, budgets, and other factors as part of the process. For example:

1. If a given software application accounts for a significant portion of the target's revenue, then a priority is to focus on the rights held in that application and the steps taken to secure those rights. The diligence review may even include an automated scan or technical review of the application to validate the origin of the software code included in the application.
2. If the buyer's objective is to expand the use of a third-party IT system used by the target into new business verticals or new markets, review of relevant agreements with that third-party to determine that the rights granted are broad enough to support these objectives will be a priority.
3. If a large volume of software is used to support the target's business, it is important to understand which items of software to focus on. For example, while it may not be practical to review all software licenses, the choice may be made to begin with development agreements relating to custom-developed software, leaving so-called "off the shelf" software for later review.

D. Buyer Software and IT Systems. In addition to focusing on the software and IT systems of the target, a diligence review will often cover the buyer's software and systems as well. Issues of technical integration and compatibility can take varying lengths of time to resolve, particularly where the target's software and IT systems will be integrated into existing buyer systems. These issues should be discovered early so that they can be addressed prior to closing of the transaction. Likewise, where target software or IT systems are found to duplicate those of the buyer, the diligence review should include an analysis of whether these redundancies can be eliminated. In many cases, buyers find that they can more easily and efficiently expand their use of existing software or systems rather than bringing on a duplicate system from the target - and thus find that they can reduce the purchase price by excluding duplicate target software or systems from the transaction.

E. Shared Use Scenarios. Particularly in the case of an asset purchase or another transaction not involving the purchase of the entire target organization, it is essential to determine early on whether any of the software or IT systems relevant to the portion of the target organization, business, or assets subject to the transaction will be required for operation of the portion not subject to the transaction. These scenarios can often prove tricky and nearly always require that additional documents be prepared and signed beyond the standard M&A agreements.

- 1. Division of Ownership.** In the case of software or IT systems used by both the portion of the target's organization or business being acquired and the remaining target organization, each party will likely prefer to be the owner of the software or IT systems. Different measures are applied to determine which party should retain ownership of the assets (e.g., whether the asset is "necessary" to either business versus being "essential" to the business or only "reasonably required"). Ownership is preferably negotiated up-front but in any case should be determined early in the transaction following identification of a software or IT system to be subject to a shared use scenario.
- 2. License or Rights of Use or Access.** Parties facing a shared use scenario will typically put in place a license agreement (or some other applicable form of agreement) to address the shared use of software or IT systems. Care should be taken to draft the license or other agreement to fit the needs of the parties for the particular software or IT system. For example, if a party only needs to use the particular software or IT system for a limited time post-closing (e.g., until it can transition to a new system) the license may be more transitional in nature rather than a longer term agreement.
- 3. Joint Ownership.** Joint ownership arrangements may appear to be more palatable than licensing arrangements, but can be equally or more difficult to administer in practice. Likewise, joint ownership may not be possible given the nature of certain software or IT systems.
- 4. Transition Services.** In addition to a license or other agreement covering use of or access to the particular software or IT system, and particularly if any IT services are to be shared, it is typical to also enter into a "transition services agreement" where one of the parties to the transaction continues to provide certain programs or services to the other party (for example, data processing or storage) until that party can provide the service itself or transition to a new provider of these services. These agreements too should be carefully negotiated to fit the particular needs of each party for transition services.
- 5. Third-Party Limitations.** As noted above, almost all software and IT systems comprise portions provided by third-parties. Many third party software licenses or IT services agreements prohibit the use of the licensed program or IT system providing services to others. Take care to evaluate up front all relevant third-party agreements to ensure that they do not conflict with the terms of any planned license agreement or transition services arrangement between the parties.

III. AREAS OF FOCUS. While not all of the following areas will be relevant in the context of each diligence review involving software or IT systems, the following areas should be considered for inclusion based on their importance to the buyer and relevance to the value being conveyed in the applicable transaction.

A. Hardware and Networks.

- 1. General Considerations.** The term "IT system" can have multiple meanings but all typically include elements of computer hardware and devices (e.g., servers, routers, switches, etc.) linked by communications channels to form a network. In the case of an IT system "inside" the firewall of the target, this network would typically reside within one or more data centers owned or operated by the target

The hardware and networks forming the core of any IT system are thus of central concern in the diligence review of any IT system. IT systems are, however, quite diverse in terms of their purpose, architecture, operation, and use. An initial concern of any diligence review is necessary to obtain information about both the IT system and the value placed on that system by the buyer in the transaction

Key diligence issues and questions, are often highly-technical in nature – many times meriting outside technical expertise to assist the legal diligence team, as noted above

- 2. Key Diligence Information.** Examples of key information to consider in the diligence review of hardware and networks are listed below

- (a) Logical and physical diagrams of applicable IT systems included in the transaction (and relation to or dependencies on any systems not included in the transaction)
- (b) List of hardware and equipment comprising the IT systems included in the transaction
- (c) Methods and protocols for remote access to IT systems
- (d) Agreements and contracts (See, also, Section III.C. **(Agreements)** below):
 - (i) Purchase or license of IT systems
 - (ii) Hosting and connectivity services
 - (iii) Support, maintenance, and monitoring of IT systems
 - (iv) Service levels and IT system performance (including, uptime, bandwidth, and performance guarantees and limits)
- (e) Actual performance statistics for IT systems (e.g., for 2 years preceding the transaction)
- (f) Schedule of periodic audits and reviews of IT systems (e.g., for 2 years preceding the transaction)
- (g) Information regarding ongoing or planned development and testing projects involving target IT systems
 - (i) Schedule of ongoing or planned development and testing involving the IT systems
 - (ii) Logical and physical diagrams of applicable development, testing, and staging environments
 - (iii) Description of methodologies and techniques used for systems development
 - (iv) Description of methodologies and techniques used for security testing of the IT systems (and introduction of subsequent changes and enhancements)
 - (v) Configuration management and change control procedures
 - (vi) Copies (or sampling) of change control requests (e.g., for 2 years preceding the transaction)
 - (vii) Metrics and performance statistics relating to development and testing environments
- (h) Disaster recovery and business continuity procedures

B. Software.

1. General Considerations. Software deployed inside the firewall of a target (i.e., within the target's own IT systems) is often given less scrutiny in diligence reviews than software distributed to customers of a target. This approach would seem to be justified by the fact that greater revenue has historically been driven through the distribution of software rather than the operation of IT systems behind a firewall (for example, in the case of a traditional software vendor). The advent of "software as a service" and so-called "cloud" computing models, through which the functionality of software is provided to users as a service over a network, has removed much of this justification. While diligence for software distributed beyond a target's firewall remains important, diligence for software used in the target's IT systems must be reviewed to determine its relevance to the value being conveyed in any M&A transaction.

2. Key Diligence Information. Examples of key information to consider in the diligence review of software are listed below.

(a) List of software used in the business of the target subject to the transaction, categorizing the software as having been obtained through one of the following means:

- (i)** Target-owned
 - (a)** Internally developed
 - (b)** Purchased
- (ii)** Third-party
 - (a)** Licensed
 - (b)** Unlicensed
- (iii)** Jointly-owned;
- (iv)** Unlicensed (describe)
- (v)** Other (describe)

(b) List of software used in the business of the target subject to the transaction, categorizing the software as being deployed in one of the following means:

- (i)** Internal – target access only
- (ii)** Internal – third-party accessible
 - (a)** General public (i.e., not subject to agreement other than web site terms of use)
 - (b)** Under contract (i.e., subject to written or electronic agreement)

Note: Because the scope of these materials is limited to software “inside” the firewall, other “external” forms of deployment are not covered by these materials but would be relevant to a typical diligence review.

(c) Components and modules within key software applications.

(d) Agreements and contracts relevant to the software used in the business of the target subject to the transaction (See, also, Section III.C. **(Agreements)** below):

- (i)** Licenses (including “click-through” agreements),
- (ii)** Development agreements
- (iii)** Contractor agreements
- (iv)** Assignments
- (v)** Warranties and guarantees
- (vi)** Indemnification agreements and commitments
- (vii)** Support and maintenance agreements

(e) Software documentation and manuals

(f) Software escrow agreements (or other agreements concerning access or use of source code for the software)

(g) List of internal security policies that relate to the operation or use of the software

(h) Information regarding ongoing or planned development and testing projects involving target software.

- (i)** Schedule of ongoing or planned development and testing involving the software
- (ii)** Description of methodologies and techniques used for software development

- (iii) Description of methodologies and techniques used for security testing of the software (and introduction of subsequent changes and enhancements)
- (iv) Configuration management and change control procedures.
- (v) Copies (or sampling) of change control requests (e.g., for 2 years preceding the transaction)
- (vi) Metrics and performance statistics relating to development and testing environments
- (i) Description of user groups, roles, geographical locations and permissions

3. Code Scans. One of the more recent diligence tools available to aide in software due diligence is the automated code scan. These scans comprise software tools that scan software code for various factors – including the presence of third-party and open source software, the general structure of the code itself, and even flaws in the integrity of the code. Many of these scanning tools have evolved to the point where the scan can even be accomplished without requiring the target to disclose its source code. However, as with many searches (e.g., traditional patent or trademark searches), code scans are still known for generating (very) long lists of information and can require substantial effort and expertise to narrow the list and identify actual issues or problems. Nonetheless, code scans can be an invaluable tool to aide any M&A software diligence review.

C. Agreements.

1. General Considerations. As noted throughout these materials, software and IT systems are often comprised of applications and components obtained from multiple third-party licensors and providers. The means by which the target obtains rights to these third-party applications and components is typically through a license or services agreement with the third-party licensor or provider. A thorough due diligence program will thus include a review of all material agreements to which the target is a party.

2. License Agreements. Often, the most significant agreements in a diligence review of software and IT systems will be license agreements. License agreements under which the target is the licensee are important because they enumerate the rights that the target has (and acquiring party will obtain) in the subject software or IT system. Licenses can appear in many types of agreements, many of which do not actually include the word “license” in the title. For example:

- (a) Distribution agreements
- (b) Manufacturing agreements
- (c) Development agreements
- (d) Joint ventures
- (e) Consulting or independent contractor agreements
- (f) Settlement agreements

Increasingly, other agreements relating to software and IT services also include licensing provisions material to the business of the target. These agreements can include website links, advertising, affiliate relationships, co-branding, promotional, content provider, electronic data interchange, syndication, etc.

3. Service Agreements.

(a) IT Services. While an assessment of the rights in the software or IT system itself is a critical part of the diligence review of any software or IT system, the obligation of the third-party licensor or provider of the software or IT system to provide related services such as maintenance, support, training and consulting is often equally important.

(b) Cloud Computing and Software as a Service. Increasingly, software and IT systems are provided as services, rather than as licensed assets, often termed “cloud computing” or “software as a service” agreements. A diligence review of such agreements has thus become increasingly critical. Issues relating to diligence of these agreements is covered under the “IT issues and Due Diligence ‘Outside’ of the Firewall” portion of the materials for this presentation.

4. Open Source Software Licenses. The use of open-source software has become ubiquitous in IT systems. Open source licenses are now commonly seen in nearly all M&A transactions, including even transactions involving non-technology companies. The unique nature of open source software licenses merit special consideration in addition to traditional proprietary license agreements to which the target may be subject.

There are currently over 70 different approved open source licenses, as well as many more non-approved variants on these licenses. Common approved open source licenses include as the GNU General Public License (GPL) versions 2.0 and 3.0, Mozilla Public License (MPL), Common Development and Distribution License (CDDL), Apache License (version 2.0), Berkley Software Distribution (BSD) License, and MIT License. It is important to remember that each of these open-source licenses has its own unique terms and conditions – each with unique implications regarding the distribution and use of the software licensed under that license.

Diligence reviews should seek to understand and obtain information regarding:

- (a)** The open source software used by the target.
- (b)** The relevant open source licenses under which this software was procured.
- (c)** The owner or source from which the open source software was obtained.
- (d)** The target IT systems or software with which the open source software is used or into which the open source software has been integrated.
- (e)** The nature of the use or integration of the open source software with the target’s other software or systems.
- (f)** Any modifications made to the open source software.

In particular, many of these points will be of increased importance depending on the particular open source license at issue. For example, under a so-called “copy-left” license such as GPL version 2.0 or 3.0, distributions to third parties of a software program that is derived from the open source code must be made under the same terms as that open source license, often at little or no charge.

If open source software is used in important applications within the target or if the disclosures regarding open source are called into question, it is becoming increasingly common to use third-party code scanning tools to perform an automated review of the target’s software code to identify any open source software used in the code. Likewise, depending on the use of the open source software, review of open-source issues may require consulting IT and open-source specialists.

5. Affect of the Transaction. A critical part of the review of any license agreement will involve whether and to what extent the target’s licensed rights will be adversely affected by the transaction. As noted above, the nature of the transaction structure can be very important when assessing this issue. For example:

- (a)** If the transaction is a stock purchase, provisions that terminate the agreement upon a change of control are relevant.
- (b)** In addition to triggering a change of control provision, if the transaction is an asset purchase, the transaction will likely trigger an anti-assignment clause.
- (c)** Both forward and reverse mergers will also trigger a change of control provision and,

(i) in the case of a forward merger, case law suggests that the merger will also be treated as an assignment with respect to licenses, perhaps triggering an anti-assignment provision (see *Cincom Systems, Inc. v. Novelis Corp.*, 581 F.3d 431 (6th Cir. 2009)).

(ii) in the case of reverse mergers, a split of authority exists. A 1991 California decision (unpublished) treats the transaction similar to a forward merger for purposes of an anti-assignment clause in a software license (see *SQL Solutions, Inc. v. Oracle Corp.*, No. C-91-1079 MHP, 1991 WL 626458, at *1 (N.D. Cal. Dec. 18, 1991)). Other cases, however, find that no assignment has occurred (see *PharMetrics, Inc. v. Source Healthcare Analytics, Inc.*, 21 Mass.L.Rptr. 526 (Mass. Super. Ct. September 5, 2006)).

Understanding the importance of the software or IT systems subject to the agreement in question to the business or operations of the target will be necessary to assess whether rights potentially lost due to a change of control or anti-assignment clause are material (or even critical) to the transaction.

Understanding other options to potentially replace the software or system in question will also be important. For example, if a software license will be forfeited or may be terminated on the closing of the transaction, does the buyer have a comparable replacement for the program? Is the software off-the-shelf and easily replaceable or is it highly customized?

If the licensor's consent is needed for license rights to continue post-closing, what is the relationship between the licensor and licensee? Would consent be easily obtainable without additional consideration? Is the licensor a competitor of the buyer, therefore posing a challenge to obtaining such licensor's consent?

6. Additional Diligence Information. Examples of other important terms to consider in diligence reviews of agreements relating to software and IT systems include:

- (a) Parties to the agreement.
- (b) Software or IT systems involved.
- (c) Territory.
- (d) Exclusivity and non-competes.
- (e) Field of use.
- (f) Fees or royalties (payable or receivable) and other financial terms.
- (g) Term (expiration date) and termination rights.
- (h) Limitations of liability (or lack thereof)
- (i) Indemnifications (both provided and received by the target)
- (j) Governing law and jurisdiction.
- (k) Any other provisions that could adversely impact the transaction or future operation of the target business, such as most favored nations provisions.

D. Information Security.

1. General Considerations. As is the case with data privacy (covered below), information security has become an increasingly important issue to any diligence review of software and IT systems. As with the other areas relevant to the diligence review of software and IT systems, information security policies, procedures and systems are of a highly technical nature and often require the involvement of outside security experts to assist the legal team in their diligence efforts.

2. Key Diligence Areas. Examples of key information to consider in the diligence review of information security procedures and systems are listed below.

- (a) Procedures and systems for intrusion detection and prevention

- (b) List of routers included in the IT system including locations, manufacturer, model and rules
- (c) List of firewalls including locations, manufacturer, model and rules
- (d) List of access control policies, mechanisms and network segmentation
- (e) List of intrusion detection systems including manufacturer, model and rules (including network and host based detectors)
- (f) List of intrusion prevention systems (not included above) giving locations, manufacturers, model and rules
- (g) Product documentation and manuals relevant equipment and systems
- (h) List of server logging systems and storage locations
- (i) Schedule of vulnerability assessments, penetration tests, code reviews and audits
- (j) List of anti spyware and malware systems including locations, licenses, update policy, incident reports, and activity logs
- (k) Schedule of actual information security breaches, exposures, and other incidents, as well as relevant countermeasures adopted
- (l) Copy of incident management procedure and details of any automated remediation capabilities

E. Data Privacy.

1. General Considerations. It is important to inquire about the target business's general data privacy protections and relevant privacy policies. This is especially important for target companies that handle the personally identifiable information (PII) of employees, clients, customers, or other third parties.

Note that issues relating to data privacy and security considerations are covered under the "Privacy and Security Issues" portion of the materials for this presentation. Please refer to the materials regarding "Privacy and Security Issues" for additional information on privacy and security topics.

2. Key Diligence Issues. Examples of key information to consider in the diligence review of data privacy protections and policies are listed below.

- (a) Key information to obtain during the diligence review will include copies of:
 - (i) Network and IT system access policies.
 - (ii) Data privacy policies (Note: Web site data privacy policies covered below).
 - (iii) Disaster recovery and business continuity plans for IT systems.
 - (iv) Network and data security and protection policies.
 - (v) Audit reports regarding IT systems (including, as applicable, SAS 70 reports).
- (b) In addition to understanding relevant information security policies, it can also be critical to make an inquiry regarding actual practices and instances of noncompliance with or failure of relevant policies, including unauthorized access to or use of IT systems and information stored on those systems. Key areas of inquiry will include:
 - (i) Leaks of confidential business information (including personally identifiable information or PII).
 - (ii) Instances of hacking or other unauthorized access to IT systems.
 - (iii) Improper dissemination of business information (including PII) or dissemination of business information in violation of applicable policies.

- (iv) Any other unauthorized access or use of business information or data.

3. Data Privacy Regulations. The ongoing increase in regulations relating to the collection and security of data and information, particularly PII, merits specific consideration in the diligence of data privacy protections and policies. Particularly in the case of a leak or security breach, the buyer should seek to understand the implications for the target's business (and any post-closing implications for the buyer) under applicable regulations.

Various laws and regulations governing the collection and security of certain types of information may be implicated depending on the target business (note that the nature of the buyer's business may also be relevant if the information acquired in the transaction from the target will become subject to regulations applicable to the buyer's business post-close). For example, in the U.S. both the healthcare and financial services industries are highly regulated through the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), respectively. Likewise, the majority of all states have implemented some form of data privacy or breach notification law. Outside of the U.S., regulation of information privacy is even more pervasive. For example, both Canada and the European Union, for example, regulate exchanges of PII regarding their residents.

The IT diligence team should determine whether and to what extent coordination will be needed with the regulatory diligence team to address this issue. In addition, where information is being exchanged across international boundaries, it may be merited to consult local counsel regarding applicable regulations governing those transfers.

4. Web Site Privacy Policies.

(a) **General.** In addition to a terms of use or terms of service, it has become standard for web sites to include a privacy policy disclosing and explaining the data and information collection and use practices employed on the site. Some jurisdictions, such as California, have even enacted specific laws requiring certain disclosures regarding web site data collection and use.

(b) **Purpose and Scope.** A privacy policy serves the purpose of informing users of a web site about how the web site owner or operator collects, uses, stores, shares and protects data and information from users of the site.

The policy will typically cover and distinguish between data, and information can include both non-personally identifiable (de-identified) data as well as PII. The policy will make a distinction between the collection of PII and non-personally identifiable information and address the rights and obligations of the web site operator as to each form of information.

(c) **Diligence Issues.** In the context of a diligence review, and depending on the value or materiality of any user data or information to the transaction, it is important for a diligence review to note:

- (i) Whether the target organization has a privacy policy for all web sites (and whether it has maintained a privacy policy at all times during the operation of those sites)
- (ii) The effective date of each privacy policy.
- (iii) Whether each policy is up to date (particularly with specific laws, such as those in California referenced above).
- (iv) The update process employed for each privacy policy, particularly the notices (if any) provided to users of the relevant web sites.
- (v) The terms under which the data and information collected under each version of the privacy policy may be transferred in the context of a transaction such as the one at hand.

With particular note to the last point above, the law relating to privacy of web site user data has evolved to require that a privacy policy address the web site operator's right to transfer information collected through the site upon a sale, merger, or other corporate transaction for the operator to have the right to make such a transfer. With the increasing focus on user data in M&A transactions, it is thus critical to at minimum confirm that all relevant privacy policies of the target permit a transfer of user data under the structure of the transaction at hand.

IV. ADDITIONAL AREAS FOR CONSIDERATION. In addition to the primary areas of focus set forth in Section III above, the following areas may also be relevant for inclusion in a diligence review of software and IT systems “inside” the firewall of the target, based on their importance to the buyer and relevance to the value being conveyed in the applicable transaction. Each of the following areas are, however, typically the subject of additional specific diligence reviews and are thus not covered in depth in these materials.

- A.** Employees and contractors involved with relevant software and IT systems.
- B.** Intellectual property rights applied for or obtained for relevant software or IT systems.
- C.** Insurance coverage for operation of relevant software and IT systems.
- D.** Laws and regulations applicable to relevant software and IT systems.
- E.** Technical standards applicable to relevant software and IT systems.
- F.** Litigation, investigations, and other disputes involving relevant software and IT systems.



IP INSTITUTE


Cloud Computing

June 4, 2010

Jason D. Haislmaier
jason.haislmaier@hro.com



Hinkle, Roberts & Owen LLP
Attorneys at Law




This presentation is intended for general informational purposes only and should not be construed as legal advice or legal opinion on any specific facts or circumstances, nor is it intended to address specific legal compliance issues that may arise in particular circumstances. Please consult counsel concerning your own situation and any specific legal questions you may have.


The thoughts and opinions expressed in this presentation are those of the individual presenters and do not necessarily reflect the official or unofficial thoughts or opinions of their employers.

For further information regarding this presentation, please contact the presenter(s) listed in the presentation.

Unless otherwise noted, all original content in this presentation is licensed under the Creative Commons Attribution-Share Alike 3.0 United States License available at: <http://creativecommons.org/licenses/by-sa/3.0/us>.



SOME RIGHTS RESERVED

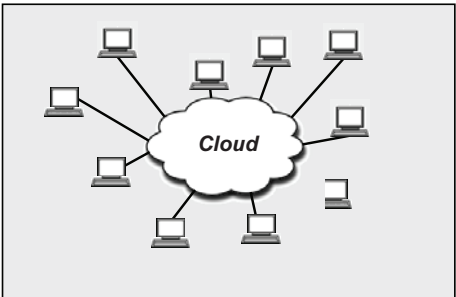


Cloud Computing

HBO

Why
"Cloud?"

HBO



HBO

amazon web services

IBM

GOGRID

terremark

ORACLE

Gmail

What is it?

Cloud

appnexus

rockspace

Google Apps

NETSUITE

Microsoft Virtualization

VMware vCloud™


flexiant

hp


tercera

salesforce


Appistry



"I'm not sure my goal for today is going to be to actually explain it to you, but I do want to make sure that people understand that I think everybody in our industry accepts it's the next major transition point in terms of how IT gets done."

Steve Ballmer
CEO, 
Speaking at a Microsoft event in Singapore

Copyright © 2010 Warner Bros. Entertainment Inc.




What is Cloud Computing?

Key Characteristics

- The "cloud" is a metaphor for the Internet
- True "cloud computing" includes specific features and functionality
 - Computing resources or functionality
 - Delivered as a service over a network
 - Dynamically provisioned on-demand by the cloud provider
 - Device and location-independent access
 - Little or no initial capital expense (thin client)
 - Subscription-based
 - Payment based on use (often as you go)
- Still a very new and rapidly expanding model

Copyright © 2010 Warner Bros. Entertainment Inc.




What is Cloud Computing?


Potential Benefits


- Increased access to applications, data, and functionality anywhere, at anytime, from any device connected to the Internet
- Reduced hardware and infrastructure costs
- Reduced software costs
- Increased software availability
- Reduced need for physical and digital storage space
- Reduced need for expertise in or control over the technology infrastructure
- Reduced support costs
- Increased processing power

Copyright © 2010 Warner Bros. Entertainment Inc.



What is Cloud Computing?






What is Cloud Computing?

NIST Definition

- Evolving computing paradigm
 - April 24, 2009 – Initial NIST draft definition

Cloud Computing, n.

A pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five key characteristics, three delivery models, and four deployment models.



What is Cloud Computing?


NIST Definition

- Evolving computing paradigm
 - April 24, 2009 – Initial NIST draft definition
 - October 7, 2009 – Current NIST draft definition (v15)

Cloud Computing, n.

A pay-per-use-model for enabling ~~available~~, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, ~~and~~ services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is ~~comprised~~~~composed~~ of five ~~key~~~~essential~~ characteristics, three ~~delivery~~~~service~~ models, and four deployment models.


- Definitions, use cases, technologies, issues, risks, and benefits will continue to evolve



What is Cloud Computing?

NIST Definition


- Large ecosystem – many models, providers, and markets
- On-demand self-service
- Ubiquitous and broad network access
- Thin client interface (e.g., a web browser)
- Pooled resources
 - Location independent
 - Multi-tenant model
 - Dynamically assigned (and re-assigned) resources
 - Reduced user control or knowledge of physical resources
- Rapid provisioning (high elasticity)
- Pay as you go
 - Metered, fee-for-service, or even advertising based revenue models
 - Systems monitor, control, and (in theory) optimize resource usage
 - "Infinite" capabilities available for purchase in any quantity at any time



What is Cloud Computing?

Deployment Models

- Private cloud ("Internal" cloud)
 - Cloud infrastructure is owned or leased by a single organization
 - Operated solely for that organization
- Community cloud
 - Cloud infrastructure is shared by several organizations
 - Supports specific user community that has shared concerns (e.g., project, mission, security requirements, policy, and compliance considerations)
- Public cloud
 - Cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group
- Hybrid cloud
 - Cloud infrastructure is a composition of two or more clouds (private, community, or public)
 - Unique entities bound together by standardized or proprietary cloud technology enabling data and application portability



What is Cloud Computing?

Delivery Models

- Software as a Service (SaaS)
 - Software running on a cloud infrastructure
 - User does not manage or control underlying cloud infrastructure (or even individual software application capabilities)
 - Limited user-specific application configuration settings
- Platform as a Service (PaaS)
 - User-created applications running on a cloud infrastructure
 - User-selected and controlled applications and hosting environments
 - Programming languages and tools chosen by the provider
 - User does not manage or control underlying cloud infrastructure
- Infrastructure as a Service (IaaS)
 - Processing, storage, networks, and other fundamental computing resources running on cloud infrastructure
 - User selects and configures operating systems, storage, applications, and networking components (e.g., firewalls, load balancers)
 - User does not manage or control underlying cloud infrastructure

HBO

Everything as a Service?
(EaaS)

HBO


Who's ^{not} using it?

Cloud

HBO


What should you do about it?

Cloud




Many similarities
to existing delivery models
Many differences
from existing delivery models

Copyright © 2011 Warner Bros. Entertainment Inc. All Rights Reserved.



Understand the similarities
Understand the differences
Understand why they matter

Copyright © 2011 Warner Bros. Entertainment Inc. All Rights Reserved.




Understanding Cloud Computing

Many Legal Issues – New and Not So New

- Cloud computing represents a true paradigm shift from existing delivery models
- Paradigm shift does not mean an entirely new paradigm
- Cloud computing shares many legal issues in common with existing delivery models, but poses new legal challenges
 - Cross-border issues
 - Service levels and performance
 - Data protection, rights, and usage
 - Privacy and security
 - Legal compliance issues
- Lessons learned from traditional software licensing and IT outsourcing agreements can be (very) applicable to the cloud

Copyright © 2011 Warner Bros. Entertainment Inc. All Rights Reserved.




Understanding Cloud Computing

Inherent Legal Tension

- Cloud services are designed for mass market use
- Cloud provider business models rely on the adoption of a standard platform
- Standard mass-market contracting terms are used to facilitate this model
 - Non-negotiable agreements (often “click-through”)
 - Little opportunity to conduct meaningful diligence
 - Risk generally shifted to user through provider-favorable terms
 - Few definable obligations or responsibilities
 - Strong limits on liability (including direct liability)
 - Terms often subject to change with little notice
- Cloud services have evolved very rapidly
- Increasingly utilized by customers to fill sophisticated, mission critical roles
- These roles often give rise to unique service requirements and the need for specialized contract terms



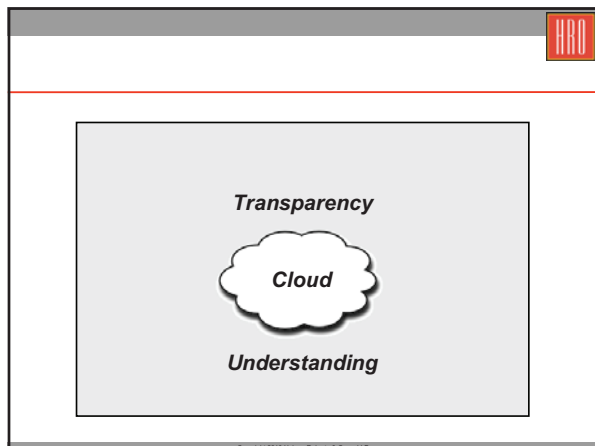
Cross-Border Legal Issues

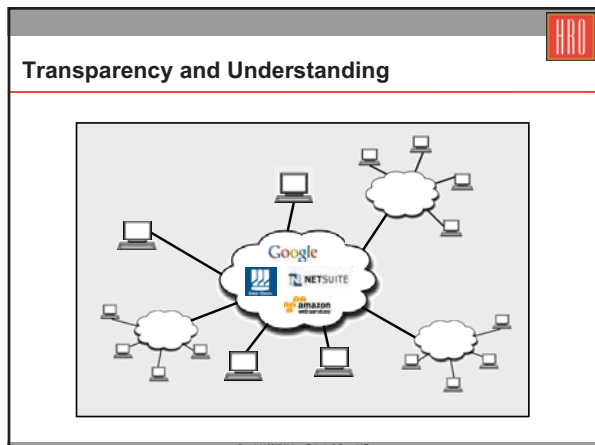


Cross-Border Legal Issues

Cloud Services Are Inherently Cross-Border

- Cloud computing services are inherently “stateless”
- Data storage and processing are dynamically and constantly re-provisioned
- Servers located in multiple different locations (often in different countries)
- Data never anywhere, but always somewhere
- Can and does create jurisdictional and regulatory issues
 - Cross-border data flow
 - Applicable regulations
 - Potentially conflicting regulations
- Transparency and control can become very important
 - Specified locations for data storage and processing
 - Limitations on changes to architecture
 - Notice of changes
 - Required audit trail for all data






Transparency and Understanding


Understand The Nature of the Services

- Cloud services model often relies on multiple providers
 - Offer expanded cloud service offerings
 - Provide additional capacity
- Cloud service agreements often additionally include broad subcontracting rights
- Liability and responsibility for subcontractors often limited (or disclaimed entirely)
- At minimum, no contractual privity
- Seek reasonable limitations and notices
- Require liability of the cloud provider for acts of subcontractors
- Use negotiations to conduct diligence and understand how the services are being provided



Performance and Service Levels

Copyright © 2010 HRO. All Rights Reserved.




Performance and Service Levels

Standard Platform, Standard Service Levels

- Cloud provider business models rely on the adoption of a standard platform
 - Standard service offerings
 - Standard performance and service levels
- Cloud providers are typically reticent to negotiate customized performance and service levels
- Flexibility grows with the volume of services
- Definite room to negotiate in the context of private clouds
- Options typically exist

Copyright © 2010 HRO. All Rights Reserved.



Performance and Service Levels

Establish the Level of Performance


- Strong parallels to IT outsourcing agreements (even though the service levels themselves may differ)
- Express performance metrics and service levels
 - Include in the agreement, not by reference
 - In force for the entire term of the agreement
 - Performance in accordance with established specifications
 - Specified service levels for key services
- Even if service levels are not negotiable, consider other options
 - Heightened reporting requirements
 - Root cause analysis and reporting
 - Additional options for termination
- At minimum, understand relevant levels of service and how they compare to your requirements and expectations

Copyright © 2010 HRO. All Rights Reserved.



***Business Continuity
and
Disaster Recovery***

Copyright © 2016 HRO. All Rights Reserved.




Business Continuity and Disaster Recovery

What Happens When the Provider Fails


- How long could you operate without:
 - Access to cloud services?
 - Copies of your data?
- Take the time to diligence the BCP
- Include the BCP by reference in the cloud services agreement
- Set minimum requirements for the BCP
- Restrict changes to the BCP
 - Notice and opportunity to review and approve changes
 - Added right of termination if changes are inconsistent with your policies
- Include audit rights to ensure implementation of the BCP
- Consider data back-up through a secondary provider
- No exceptions (including force majeure)

Copyright © 2016 HRO. All Rights Reserved.




Data

Copyright © 2016 HRO. All Rights Reserved.




*It's all about
Data*

Copyright © 2010 Amazon, Inc. or its affiliates. All rights reserved.



*Do you know **where** your data is?
Do you know **what** data is yours?
Does your **provider** know?*

Copyright © 2010 Amazon, Inc. or its affiliates. All rights reserved.



Data

Ownership and Rights

- Not always standard that all "data" belongs to the customer
- Becoming an increasingly lucrative business for cloud providers to take (and later monetize) rights in user data
- Not unlike the early days of IT outsourcing
- Define "data"
 - Data and information that is provided
 - Derived data and information ("meta-data")
- Specify ownership rights
- Grant provider specific rights in the data
 - Use as required to provide the services
 - Limited (if any) use for other purposes
 - Prohibit (or specify limits on) monitoring and access to data
- Protect data as confidential information

Copyright © 2010 Amazon, Inc. or its affiliates. All rights reserved.

Data

Audit Trail

- Cloud services rely on dynamic provisioning of data storage and processing
- Data is often “on the move” between physical resources
- Understand your need to know how, where, when, and by whom your data has been:
 - Stored
 - Transferred
 - Accessed
 - Altered
- Map requirements in the cloud services agreement to
 - Policies and procedures
 - Applicable laws and regulations
 - Other requirements (litigation holds?)
- Confirm that the cloud provider can provide the required audit trail

Privacy and Security

Privacy and Security

How secure is cloud computing?

Privacy and Security

2009-2010 survey measuring attitudes on cloud computing:

- 86% of senior business leaders excited about the potential of cloud computing
- >90% of these respondents voiced concern about the security, access, and privacy of data in the cloud
- Majority of all respondents believe the U.S. government should establish laws, rules, and policies for cloud computing

Privacy and Security


"We need government to modernize the laws, adapt them to the cloud, and adopt new measures to protect privacy and promote security. There is no doubt that the future holds even more opportunities than the present, but it also contains critical challenges that we must address now if we want to take full advantage of the potential of cloud computing."

Bradley Smith
Senior VP and General Counsel

Privacy and Security

Cloud Computing Advancement Act
(as proposed)


- Improve privacy protection and data access rules to ensure users' privacy;
- Reform and strengthen the Electronic Communications Privacy Act to define and provide stronger protections for consumers and businesses;
- Modernize the Computer Fraud and Abuse Act so law enforcement has the tools it needs to go after hackers and deter online crimes;
- Create "truth-in-cloud-computing principles" to ensure that consumers and businesses will know whether and how their information will be accessed, used and protected; and
- Pursue multilateral framework to address global data access issues



Privacy and Security

Cloud Services Raise Unique Security Issues


- Cloud services depend on leveraging a "multi-tenant" architecture
 - Data from each user is typically stored on a single virtual server
 - Multiple virtual servers run on a single physical server
 - Data from multiple users is stored on each physical server
- Data security depends on the integrity of the "virtualization"
- Traditional network and physical security concerns also apply
- Not always possible to specify architecture itself but can dictate practices



Privacy and Security

Trust But Verify

- Compliance with applicable privacy and security laws and regulations
 - Understand applicable laws and regulations
 - Provide means to inform provider
 - Address changes to laws and new laws
- Obtain and review copies of provider privacy policies and security procedures
 - Compare with your internal policies and procedures?
 - Use the cloud services agreement to address any gaps
- Specify data security controls (or document existing controls)
 - Encryption standards and practices (data "at rest" and "in motion")
 - Data segregation practices
 - Physical security procedures
 - Audit and reporting requirements (SAS 70)
 - Security breach notifications




Legal Compliance





Cloud computing services “challenge the presumption that a company possesses, or even controls, all of the digital business information for which the law may impose duties to preserve and produce, and potentially jeopardize a company’s ability to preserve and produce required records and electronically stored information.”


Cloud Security Alliance,
Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009



Legal Compliance

Preserve the Ability to Comply


- Cloud services necessarily require allowing the cloud provider to maintain and control your data for legal and regulatory purposes
- Users often do not know what infrastructure they are using or where it is located
- Cloud provider may not know where your data is – may only have the ability to retrieve it
- Courts are not likely to forgive legal obligations regarding document preservation because your data is “in the cloud”
- Burden is on you to understand your potential legal obligations and to require appropriate compliance from the cloud provider



Cloud Issues

Specify Assistance From Cloud Provider

- Preservation, location, and access
- Cite applicable standards for compliance
 - Internal document retention policies
 - Laws and regulations
- General litigation “cooperation” clause
 - General data preservation
 - Cooperation with discovery requests
 - Compliance with litigation holds
- Heightened obligations as needed for lawsuits, investigations, and other legal proceedings:
 - Access to and location of data
 - Limitations on government and third-party access
 - Notice requirements regarding requests for access
 - Ability to monitor or even assume control of legal proceedings




Termination and Transition

Copyright © 2016 Amazon Web Services, Inc. All rights reserved.



“Lock-In”

Copyright © 2016 Amazon Web Services, Inc. All rights reserved.




Termination and Transition

Control Termination and Transition

- Cloud services agreements are often characterized by shorter, subscription-based terms
- Control termination triggers and prohibit abrupt or uncontrolled terminations
- Architecture of cloud platforms creates additional practical barriers to termination and transition
 - Increasing calls for uniform standards for cloud interaction and interoperability
 - Standards for data retention, storage, and formatting still vary by provider
- Make compatibility and interoperability an issue
 - With your own systems
 - With your customer’s systems
 - With third-party systems
 - Compatibility with future standards


Copyright © 2016 Amazon Web Services, Inc. All rights reserved.




Termination and Transition

Provide for Transition Assistance

- Provide for transition assistance following termination
 - All services provided during the term of the agreement
 - Assistance needed to transition to a new provider
- Obtain visibility into services provided
 - Software and hardware used to provide services
 - Applicable software licensing terms
 - Relevant subcontractors
- Paying for termination assistance is far better than not having it at all




Liability Limitations




Liability Limitations

Seek Reasonable Liability Limitations

- Cloud services agreements include strong limitations on liability
 - Exclusions of incidental, special, indirect, and consequential damages
 - Exclusions even of direct damages
 - Limitations on overall liability (and service-specific liability)
 - Disclaimers of all warranties and service levels (services provided "as-is")
- Limitations often extend to specific liabilities
 - Security breach
 - Data loss
 - Service outages
 - "Force majeure" events
- Unlike traditional outsourcings or licenses, many of these limitations do not make sense in the context of cloud services




Closing Thoughts



Closing Thoughts

*Cloud computing
is a **paradigm shift**
not a **panacea***



Closing Thoughts

Paradigm Shift, Not a Panacea

- Not all cloud services are created equal
- Not all cloud services should be subject to the same terms
- Reputation alone does not offer protection
- Cloud services is include outsourcing of responsibility
- Leverage concepts from traditional software licensing and IT outsourcing
- Expressly cover the issues that matter to your business
- Your use of cloud services (and the sophistication and importance of those services) is likely to grow
- Having flexibility and additional rights, even if you have to pay for them, is preferable to not having them at all

Thank You.

jason.haislmaier@hro.com

@haislmaier



Hulse, Roberts & Owen LLP
Attorneys at Law

“Deciphering Due Diligence: Tackling the IT Issues That Can Cripple a Business Transaction”— Outsourcing, the Clouds and Due Diligence Process

Michael J. Dunne – Day Pitney LLP

June 26, 2010

I. Outside the Four Walls

A. General Overview

In a sense, the approach to managing computer resources has come full circle. Before the personal computer (PC), lap tops, PDAs and Smart Phones, terminals were all “dumb.” The user’s terminal possessed no processing capability or storage capacity. A terminal simply provided a means to interface with a central processor that a number of “dumb” terminals all shared. For instance, many colleges and universities in the Northeast United States all “time shared” a main frame computer at Dartmouth. Students had to log on at predetermined times. Such early resource sharing was used mainly because it was just too expensive for each school to purchase and maintain its own main frame. Businesses often followed the same approach of time sharing computer resources with many businesses organized to provide what was commonly called service bureau data processing services. Consider the early ADP and EDS business models.

Then along came the PC revolution and computer resources became “distributed” – spread throughout an organization. Each “terminal” was its own computer, but it was isolated from the other computers. Sharing was by way of “floppy discs.” Then the Internet and the World Wide Web became universally available and popular. Sharing of information and processing from one PC to another and to “servers” and central processing became as easy as an e-mail attachment or file transfer. Floppy discs became

a relic of a bygone era in computing and CD and DVDs became a media more for entertainment than commercial business.

Along with the advent of the World Wide Web came the “Browser,” the new means of reaching out from your PC to obtain information or processing from a different computer. Much like the dumb terminals from the early days of computing, the browser turns the user’s access device into a “dumb terminal” that is simply a means of interfacing with a centralized or remotely located computer. “Thin computers” and “thin clients” became the much heralded concept. An organization could reduce its overall cost of ownership for IT assets by purchasing PCs that were thinned down to just those capabilities the users would need locally (i.e., on the PC) and the ability to reach out (often by use of a browser) to other central computer resources within, or even outside, the organization.

Along this continuum of changes in computer resources and the approaches to managing and implementing those resources, businesses have constantly sought ways to minimize the costs of the IT resources necessary for their particular business. Vendors of computer resources have constantly sought ways to attract new business by offering new or rewrapped solutions to assert that their solution helps reduce the cost of providing necessary IT resources.

Various approaches to managing IT resources have been and are used to reduce the cost and improve the efficiency. One of the main approaches pursued by businesses has been to use IT resources or related resources owned or managed or owned and managed by third parties.

Numerous approaches with various names and acronyms have been advanced by the IT industry. As an approach and its name catch on and become the term and approach of the time, many vendors attempt to cram their solution within the name. Such

efforts by vendors often result in confusion among vendors and users. A list of the more recent approaches would include the following:

- Outsourcing
- ASP (Application Service Provider)
- SaaS (Software as a Service)
- Infra-structure as a Service (IaaS)
- Co-location Services
- Remote Hosting
- Cloud Computing.

All of the above approaches, have one key attribute in common. In each case, the responsibility for some aspect of a business's IT resources rests with a third party.

Practice Pointers for Due Diligence:

- Consider whether NDAs will be needed with third parties that provide computer resources to the target. Will due diligence efforts lead to inquiries of third parties or just review of documentation? Will requests and consents for transition services be needed?
- Many, if not most, of the issues that need to be reviewed and analyzed with respect to IT resources within a business's four walls, will also need to be reviewed and analyzed with respect to IT resources that are obtained from outside the four walls. For example, in due diligence of a outsourcing arrangement, the acquirer will want to consider such issues as: are the contracts assignable; are the IT resources sufficient for the going forward purpose of the business; are the software and other IT resources current or will they need to be upgraded; is the software compliant with any regulatory requirements, etc.

The common key attribute of relying on a third party, leads many people to question whether there is more of a marketing purpose in each new name rather than any substantive difference in the approach. While with some vendors that analysis may be more true than not, nonetheless, there are real substantive differences when the terms are properly used. There are also very important similarities. From a due diligence perspective, both the similarities and differences need to be considered and addressed when planning and executing a due diligence effort with respect to a target business.

B. Principal Outside the Wall Approaches

Understanding the similarities and differences among the various ways businesses may use and rely on third parties to provide and/or support the business's information technology resources, can be critical to a successful due diligence effort. With that in mind, a review of the principal approaches follows.

1. Outsourcing. Outsourcing is probably one of the most used and, to some, the most misused, term in the world of information technology. If one tried to propose a definition for the term, the proposed definition would undoubtedly come under attack as inaccurate, incomplete or over broad or as having some other deficiency. With that caveat stated, one general definition could be something like:

A process used in an effort to reduce costs by transferring work traditionally done within a business to an outside vendor.

Outsourcing in general can involve more than just IT resources. It can include business processes, manufacturing, or administrative services, such as human resources. Basically, any aspect of a business may be "outsourced." With respect to IT resources, the term is used to cover a large expanse of transfers, such as a business simply having a third party print and mail its bills to an insurance company transferring all of its IT

related resources (e.g., hardware, software, building facilities and personnel) to a third party and then contracting with that third party for it to provide the same services that had been provided when the resources were owned and employed internally.

Regardless of size or scope, an outsourcing arrangement will be governed by a contract between the business and the outsourcer(s). The contracts are traditionally heavily negotiated, lengthy and very complex. Depending upon the size and scope of the outsourcing, the nature of the work outsourced and whether it is critical or ancillary to the business's core competency, the contract may address many issues that prove critical to an acquirer. In significant outsourcings, the contract should address a number of critical points, including (not, necessarily, in order of priority):

- **Technology refresh** – if the contract is of any material duration, what obligation does the outsourcer have to upgrade the technology being used to provide the outsourced services and at what cost to the target business?
- **Service Levels** – does the business have a means to measure and control the quality of the services being provided by the outsourcer and remedies for substandard services? Are the Service Levels fixed in stone or adjustable as the business and the services change over the duration of the outsourcing arrangement?
- **Privacy and Security** – are necessary and appropriate obligations in place to comply with regulatory requirements and/or corresponding obligations to the business's customers?
- **Business continuity and disaster recovery** – what obligations does the outsourcer have in those areas? Are there redundant sites, mirror sites, hourly, daily, weekly, etc. back-ups?
- **Termination** – under what circumstances (breach only, convenience) and what are the ramifications (liquidated damages, not addressed)?

- **Scalability** – what obligations does the outsourcer have to increase its services (e.g., expand computer capacity, increase band width) and on what time frame and at what cost to the business?
- **Location** – where are the outsourcer’s resources located? Does the location or locations impose any regulatory/legal/contract compliance issues/concerns/risks?
- **Rights to Resources** - does the outsourcer or business own the hardware and facilities? Which party owns the rights to or licenses for the software; what happens to the IT resources upon expiration or termination of the contract?
- **Cost Computation** – how are the fees, charges and other amounts due to the outsourcer computed; number of seats, number of users, set fees, gross revenues? Are there mandatory upgrade fees, etc.?
- **Compliance** – what obligation does the outsourcer have to keep the resources compliant with laws and regulations applicable to the target’s business?

Practice Pointers for Due Diligence:

- Certain aspects of IT due diligence are best conducted by subject matter experts (SME). For example, if Service Levels are considered important, it would be best to have a SME, such as an actual user from the acquirer, review the SLAs to determine if they cover the appropriate metrics.
- Determining the true costs of many outsourcing arrangements can be very complex. Consequently, acquirers can have a tendency to rely on historical costs for a projection of its future costs. Such reliance could be a trap. For example, outsourcers are often willing to provide significant discounts up front that may run a number of years and then make those discounts up on the back end of the initial term of the contract. Such arrangements can result in significant increased costs in

the out years.

- A review and analysis of the contract provisions should only be the starting point for a thorough due diligence effort with respect to an IT outsourcing arrangement. In addition to reviewing the governing documents, due diligence should ask for and review such information as:
 - Historic monthly/quarterly/annual performance reports from the outsourcer with respect to the SLAs
 - Historic monthly/quarterly/annual incident reports, including a description of the type, level and the resolution of each incident
 - If privacy and security are a concern, consider the acquirer's compliance group following their process for a regular outsourcing due diligence, including on-site inspection of the outsourcer's facility and review of outsourcer's security policies and procedures

2. ASP; SaaS; Remote Hosting. To some extent the approaches represented by the terms APS (application service provider), SaaS (software as a service) and Remote Hosting, cover the same approach or very similar approaches. Basically, in each approach, the vendor, pursuant to a contract, provides access to software that is running on its computers. The contracts are usually less complex than traditional outsourcing contracts, but often cover many of the same points; such as SLAs, technology refresh, business continuity and disaster recovery, privacy and security, scalability, rights on termination, etc. In the ASP and SaaS approaches the vendor usually owns the software and, rather than licensing a copy of it to the business, provides the software as a type of service. Rather than granting a license to use the software, the contract may provide that the business is subscribing for a service relative to the features and functionality that the software performs. In Remote Hosting, the vendor, similar to an ASP or SaaS arrangement, may own the rights to the software, or, in other instances, may have no rights to the software and instead is charging the target business a fee for hosting the

target business's software on the vendor's computer network. Remote Hosting was originally offered by software vendors as a means of reducing the capital costs to their potential customers by eliminating the need to acquire the hardware normally associated with acquiring the vendor's software.

Practice Pointers for Due Diligence:

- Consider which entity owns or otherwise has the rights to the IT resources and what happens to those resources and how the business's needs would be addressed upon termination of the contract.
- Consider if the IT resources are compatible with those of the acquirer and if the acquirer's needs could be transferred to the ASP, SaaS or Remote Hosting solution or if the target's data, information and use of IT resources could be transferred to the Acquirer's IT systems. In either case, consider engaging an SME to assist in the review.

3. Cloud Computing. Cloud computing is the newest concept with respect to reaching outside the organization for IT resources and support. While there is no agreed upon definition for Cloud computing, in its purest form, cloud computing may be thought of as follows:

An approach to computing that provides for the automatic expansion and contraction of the computer resources being used based on the demands of such use.

In a white paper posted on its web site, the National Institute of Standards and Technology, an agency of the United States government, has provided the following as a definition of cloud computing:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five **essential characteristics**, three **service models**, and four **deployment models**.

<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>

In additional detail, the NIST paper provides the following in an attempt to place boundaries around the cloud and its definition:

“Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling. The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level

of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or

storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).”

<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>

Cloud computing differs from outsourcing, ASP, SaaS and Remote Hosting in significant ways. For example, in the typical cloud arrangement, the agreement is a click and accept, non-negotiated agreement. Additionally, there are no SLAs or the SLAs and any associated remedies are very weak from a user's standpoint. The cloud's elasticity is accomplished from tying together multiple data centers. The multiple data centers are often geographically separated to obtain the advantages that such separation provides, and the data center's resources may actually be provided by a third party or numerous third parties under subcontract arrangements with the cloud provider. As a result of those and other differences:

- The business may be unable to obtain provisions and obligations necessary to comply with privacy and security requirements;
- The business may have no recourse for poor quality services other than to terminate the agreement;
- As the location of the business's data at any given moment may be uncertain, the business may be unable to assure its compliance with security and privacy related laws and regulations and may find its data and information subject to unexpected government disclosure;
- Data ownership and the cloud provider's obligation to return the data may not be addressed or may be insufficiently addressed.

The differences, however, can become blurred based upon the deployment model. For example, private clouds can be very similar to ASP, SaaS or Remote Hosting arrangements with detailed agreements containing appropriate SLAs and restricting the jurisdictions in which the data may be transferred, processed or stored.

Practice Pointers for Due Diligence:

- Consider what services are provided in the cloud and whether they involve data or information covered by privacy and security laws and regulations
- The contracted arrangement may be governed by a “click and accept” agreement that needs to be obtained and reviewed
- Direct contact with the vendor to resolve questions may be very difficult