As PII emerges in M&A

February 28, 2014, Melbourne

Sajai Singh

Partner

J. Sagar Associates
advocates & solicitors

Delhi | Gurgaon | Mumbai | Bangalore | Hyderabad

J. SAGAR ASSOCIATES
advocates & solicitors

Dumb Gets *Dumber*!

- Managing Computer Resources has come full circle …
- Prior to PC's, Laptops, PDA,s, Smart Phones, etc. terminals were 'dumb'
  - No processing capability or storage capacity
  - 'time share' of main frames was prevalent
- Then came the PC revolution; computer resources became 'distributed'
  - Spread throughout the organization
  - Sharing via floppy discs
- The Internet and the World Wide Web made information sharing easier
- The 'browser' allowed one to browse not just your own PC but others too
- The cloud, thin computers and mobile apps have made the device you work on dumber than before!
- In the meantime, everyone has shared every bit of information!

Personally Identifiable Information

- PII (Personally Identifiable Information) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context
- PII is synonymous with other similar terms and for legal purposes the effective definitions vary depending on the jurisdiction and the purposes for which the term is being used
  - Australian law uses the term ‘Personal information’ under the Privacy Act, 1988 to mean information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion
  - India also utilizes the term ‘Personal Information’ under the Information Technology Act, 2000 and defines it as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a corporate entity, is capable of identifying such person
  - France defines ‘Personal Information’ as any information relating to a natural person who is, or can be, identified, directly or indirectly, by reference to an identification number or to one or more factors specific to the individual

Personally Identifiable Information

- Role of PII in business transactions and strategy is expanding rapidly
  - IT allows information previously considered non-identifiable to be converted into identifiable data and computers and the Internet have today revolutionized not only the amount of information that can be collected, but also the manner in which such information is organized, accessed, analyzed, used and even misused
- Almost every transaction involves PII
  - Each piece of information is a pixel, and the need for data privacy stems from the perceived danger that the wrong person may piece together enough pixels to form, and subsequently misuse, the whole picture
  - Companies contemplating M&A transactions must remember that PII and the legal duty to protect it, extends to its client database, employee health information, IP Addresses and a host of other information; such legal duty creates a liability which survives the transaction
- Increasing emphasis on privacy, in this era of information, has resulted in data protection law catching up with technology
  - Australia, the UK, the US, India and most of Europe, have legislation governing what constitutes PII, who may have it, who may not have it, how to process it and how it may be transferred

J. SAGAR ASSOCIATES
advocates & solicitors

Cross Border M&A

- Cross-border M&A deals pose several privacy issues:
  - **Applicability of national data privacy laws** – specially to foreign companies is a key issue
  - **Disclosures –** that may and may not be made by Target to Purchaser
  - **Notice** - to the Data Subject
  - **Compliance requirements** – of the Purchaser with respect to PII collected by the Target
  - **Web-site Privacy Policies** – Adherence to privacy policy which informs users how data is collected, used, stored, shared and protected
  - **Inadvertent illegal possession of PII** - Purchaser, despite best efforts, may acquire PII illegally; which may prejudicially effect an otherwise smooth M&A
- Few Signs that Privacy Issues require attention in Transaction
  - Does the transaction involve sale or acquisition of customer data?
  - Does the transaction involve operations or personnel located outside your country?
  - Does the transaction involve e-commerce activities?
  - Does the transaction involve sharing PII with a vendor or service provider?
- Overview of Privacy and Data Security Laws Implicated by Transactions
  - Sector-specific approach
  - Federal and State level
  - If the transaction is cross-border, then international privacy and data security laws (and treaties) would need to be considered

Typical Privacy requirements in M&A

- Establishing a legal basis to collect, use, disclose, transfer, or otherwise "process" PII
  - Contractual necessity; in compliance with local legal obligations; consent of individual
  - Practically redacting, aggregation or 'anonymizing' is used to disclose PII; aggregation being best
- Giving notice to the individual about the collection, use, disclosure, transfer of his/her PII
  - Applies to consumers, employees, consultants, or any other individuals.
- Consent may be required to collect or process sensitive PII
  - Also to permit some disclosures / processing
- Entering into contracts with all 'third parties' (including affiliates) who receive or process PII on your behalf, containing appropriate privacy and data security provisions
- Establishing a mechanism for cross-border transfers, where applicable laws (say EU, Australia or Argentina) restrict such transfers
  - Access equals transfer!
- While data security is a common principle of data protection laws, certain countries have also imposed detailed and extensive data security requirements
  - Argentina, Italy, Japan, Norway, Poland, Spain, and Taiwan
  - Number of countries are also adopting security breach notification requirements

Basic M&A Deal Structures

- Typical Structures
  - Asset Purchase
  - Stock / Share Purchase
  - Merger (Reverse or Forward)
- Different transaction structures raise different issues for and place different requirements on, the diligence process preceding the transaction
- Different structures also end in different outcomes with respect to privacy related post-transaction liabilities
  - In a stock purchase transaction, unless otherwise contractually agreed, the seller is not left with any ongoing liabilities of the Target, and all such liabilities, whether known or not known, are transferred to the Purchaser
- Different structures also give rise to different consent issues
  - A stock purchase typically does not trigger a consent requirement unless the Target has specifically agreed to obtain consent of the PII provider during a change of control
- Apart from liabilities and consent, different transaction structures also give rise to distinct post closing obligations
  - UK's Data Protection Act, 1998 enables the Data Subject to access PII collected about him/her/it; therefore, acquiring a UK Target would require the Purchaser to continue to make this information available as it was before

Asset Acquisition

- Purchasers typically favor asset acquisitions
  - Cherry picking of assets possible
  - Liabilities, whether known or unknown, may be left with the seller
  - Certain tax and depreciation benefits
- Sellers don't favour asset acquisitions
  - If all assets sold in transaction, seller may need to liquidate
  - Deal with its remaining liabilities without any assets backing the same
  - There may be tax incidences on gains made and dividend distribution
  - Assignment of key agreements and contracts may pose a challenge, as consent may be required or terms may need to be amended
  - Consents may become a challenge where PII is involved

J. SAGAR ASSOCIATES
advocates & solicitors

Stock Purchase or Merger

- Preferred by the Seller, as all liabilities move to Purchaser
  - Only one level of tax: any gain or loss by either the seller or its stockholders on the stock sale
  - Depreciation benefit may not be available in the same manner as in an asset sale
- Transaction could be:
  - A direct purchase of the seller's stock
  - Sale of stock of a subsidiary by a seller
  - Merger or reorganization
- Stock transfers and reverse mergers may not encounter the same consent issues as an asset acquisition
  - A provision requiring consent to assignment is typically not triggered in connection with the transfer of stock ownership of a company, including reverse mergers
  - A reverse merger could trigger a contract clause requiring consent to assignment in the case of a copyright license agreement and a software license agreement

sajai@jsalaw.com

J. SAGAR ASSOCIATES
advocates & solicitors

Deconstructing a Transaction

- What does the client want out of this deal?
- Buyer
  - Technology, possibly data
  - Employee brain and trust
  - Customer base
  - What is the other side's reputation regarding privacy?
- Seller
  - Concern about customer base
  - What is the other side's reputation regarding privacy?

J. SAGAR ASSOCIATES
advocates & solicitors

Addressing Privacy Issues – Buy Side

- Will PII help business realize its goals for transaction?
- Does the deal require special attention to privacy issues?
  - Importance of acquired data to deal valuation
  - Sensitive or highly-regulated data (e.g., health, children)
  - Volume of personal data
- Who will be responsible for privacy-related issues in diligence and negotiation?
- Does buyer have a standard deal playbook (diligence questionnaires, document requests, etc.)?
- Are there opportunities to use PII to position business for future growth and change?
- Does the Target have a Privacy Policy? Its Effective Date? Date when the PII, being transferred, was first collected?
- Have the employees given consent to the collection, storage, use and transfer of their PII?

Addressing Privacy Issues – Sell Side

- Will it be easy to separate the PII being transferred from other data / information?
- Do you have the right to so separate and transfer?
  - Is the PII assignable? In whole or part?
- Do you anticipate any particular areas of privacy-related scrutiny?
  - Deficient, outdated, or overly restrictive privacy policies
  - Gaps in privacy law compliance
  - Security breaches, privacy litigation, government inquiries
- Who will be responsible for privacy-related issues in diligence and negotiation?
- Consider remediation efforts but exercise caution (especially regarding last-minute privacy policy changes)

J. SAGAR ASSOCIATES
advocates & solicitors

Stages of the Deal

- Bidding
  - Who are the relevant sources of information on PII matters? Are they internal to the Target's organization or at a third-party provider?
  - Does separate counsel (privacy professional) handle issues relating to PII for Target? Does such counsel need to be contacted?
  - How long has each relevant party been involved in handling the Target's PII issues? How can (via consulting multiple sources) historical information be obtained?
- Due diligence
  - Enhance collection about PII, limit collection of and access to PII
- Negotiation
  - Does information learned in DD impact business model, require prompt remediation, require risk shifting?
- Closing
  - Close does not always mean integration (business and legal reasons for delay)
- Integration
  - See due diligence, above

J. SAGAR ASSOCIATES
advocates & solicitors

Bidding Stage

- Target's primary obligation is to properly protect and store its customers', suppliers', and employees' PII
- Purchaser expects detailed information regarding the Target so as to determine whether purchasing the assets of or shares in the Target would be in its interests as well as the price it is willing to pay for them
  - Such information invariably contains some PII and should be made available only through a confidential information memorandum
  - Additionally parties must enter into a non-disclosure agreement in which the Target explains its legal obligations to protect PII in its possession and in which the Purchaser warrants compliance with such obligations
  - Target should disclose any past breaches of PII to the Purchaser at this stage; as such a breach may affect the Target's value
- The Purchaser issues either a Term Sheet or a Letter of Intent, as a non-binding document, that lays out the essential terms of the agreement
  - Usually this document details information the Target must disclose as well as PII it cannot disclose during each stage of the transaction
  - Often Term Sheet also outlines the level of PII Due Diligence that will be undertaken

J. SAGAR ASSOCIATES
advocates & solicitors

Due Diligence Stage

- Perhaps the most important phase of the transaction from a privacy perspective
  - A well structured diligence review can play a key role in augmenting a Purchasers visibility into potential issues regarding a Target's PII
- Local laws and industry standards, dictate privacy requirements during a due diligence review
- The legal duty to protect PII continues on the Target
  - Actions of the Purchaser often trigger a breach of this duty
  - Investigations during due diligence qualify as 'data processing' under Italy's Privacy Code (Legislative Decree 196/2003); triggering consent and security obligations
- The due diligence process presets different issues and concerns to the parties
  - Seller seeks to provide the least amount of sensitive information (thereby exposing itself to the least risk) and confirm and conclude the transaction as soon as possible

    The Purchaser's main agenda is to extract as much information (without triggering a breach) as possible, in order to determine the Target's antecedents and liabilities and identify any critical issues which may affect the value of the transaction

J. SAGAR ASSOCIATES
advocates & solicitors

Due Diligence Essentials

- Key Personnel - While the GC is the primary contact for diligence, s/he may not be the most knowledgeable about PII; other personnel from within and outside are better-equipped to aide in the diligence:
  - Chief Information Officer (CIO), Chief Technology Office (CTO) and Human Resources (HR)
  - Outside privacy counsel
- Key Documents - Documents relating PII, Information systems and databases may not be included in a typical data room
  - Documentation may be with staff not directly involved in the transaction
  - PII related documents in data rooms can become outdated during the diligence process
- Key Third-Parties - Not all PII is always wholly owned by the Target
  - Deciphering rights held by third-party licensors or affiliates can often become tricky
- Key PII Assets – Analyze the nature of information possessed, its type, quantity, location, materiality, jurisdiction where it is held, etc.
- Materiality - In any diligence exercise, attempting to perform diligence on *all* PII in a target's organization can be a daunting task - if not impossible
  - Need to understand PII materiality, its value to the transaction, and Purchaser expectations thereon
- Shared Use Scenarios – For transactions not involving the purchase of the entire target, essential to determine the relevant PII /databases for the portion of the target organization, business, or assets subject to the transaction

Privacy Issues in Due Diligence: Buy Side

- **Buyer wants to establish a clean 'Bill of Health' regarding PII**
- **Collect relevant information** – To accurately assign value to transaction
  - Some jurisdictions legally require this inquiry; has PII moved to those jurisdictions?
  - UK TUPE requires that a new potential employer acquire specific workforce details before the transfer can take place, including the names and age of transferring employees; their pay, hours, any collective agreements; and any grievance or legal action brought against the employer by employees in the last 2 years
- **Assess Target's PII** – Establish if PII possessed by Target is an asset (such as client database etc.) or a liability (involves additional compliance)
- **Assess Target's Compliance** - An assessment of Target's basic compliance with extant privacy laws, such as existing electronic, technical and physical security measures to protect PII is crucial
  - Failure to comply with these obligations at the time after the PII was collected may also potentially limit the subsequent use of the PII and may give rise to possible future liabilities
  - India imposes civil liability for companies who are "negligent in implementing and maintaining reasonable security practices and procedures"
- **Independently Investigate Prior Breach**
- **Review filings with Data Protection Agencies / Authorities**

Privacy Issues in Due Diligence: Buy Side

- **Target focused on bringing certainty to transaction, without 'open-ended' liability obligations**
- **Assess Restrictions over PII** – Via statute, overly restrictive privacy policy or agreement with the provider thereof
  - Often find websites privacy policy declaring that "we will never share your information with any one", if the PII is a key asset in the transaction, any such restriction might affect the value of the asset.
- **Scrutinize Contracts** – For data security obligations, especially in case of any outsourcing contracts.
- **Consider future treatment of PII** – Consider whether intention is to segregate Target and Purchaser PII, post closing
  - If handled separately, then understand costs for the same.
- **Examine Target's privacy policy regarding transfer of PII –** And if the privacy policy imposes any conditions on the Purchaser in connection with that transfer.
- **Analyze applicable Data Privacy Regulations**

Privacy Issues in Due Diligence: Sell Side

- **Consider Applicable Laws** – Target has duty of care during the diligence process not to unlawfully reveal too much information
  - Jurisdictions have varying laws dictating what standard applies to this duty of care
  - Australia, principle No. 9 of the NPPs: Trans-border Data Flows requires an organization to take 'reasonable steps' to ensure protection of information collected, and it must destroy or make anonymous that information after the legitimate purpose has ended
- **Non-disclosure / Confidentiality Agreement –** A contract warranting that the Purchasing will not cause the Target to breach its duty to its Data Subjects becomes essential to resolve the conflicting interests of the two.
  - PII should be disclosed only via secure means, such as a virtual data room
- **Sensitive PII** – Avoid transfer of sensitive PII (e.g. financial details, race, medical details etc.)
  - Many jurisdictions define and specifically regulate sensitive PII
  - India's Reasonable Security Practices Rules defines Sensitive Personal Data or Information as including personal information consisting of passwords, financial information, biometric information medical history etc.

Privacy Issues in Due Diligence: Sell Side

- **Unrelated PII –** Avoid disclosure of any PII which has no nexus with the objects of the due diligence exercise (e.g. home address and telephone number of customers, political affiliations of employees etc).
- **Private Information** – Target should not transfer any information over which the provider may have a reasonable expectation of privacy (e.g. performance review, sexual orientation etc.).
- **Anonymized or aggregated information transfer -** PII may be disclosed in an 'aggregated' or 'anonymized' form to minimize effects of a possible security breach at the Purchasers end.
  - In some jurisdictions (EU) such anonymization of data is mandatory for employee PII transfer
- **Access is transfer** - Unauthorized access would trigger applicable security breach notification requirements, even in absence of actual transfer
- **Requests of Additional Information** – Develop strategies for handling requests for too much information

Drafting Definitive Agreement

- Representations and Warranties (and corresponding Indemnification provisions)
  - Sometimes buyers default in placing too much reliance on these, in order to do the deal
  - R&W in themselves are an imperfect means for buyer to establish a clean record of business
  - Sellers narrow the scope of R&W's making them difficult to interpret
  - Practical challenge to prove a breach of R&W; add to it the liability baskets and caps which limit buyers ability to obtain a meaningful financial recourse
- Some specific R&W's
  - Compliance with Privacy Policies, both internal and external
  - Compliance with material contracts
- Qualifiers & Disclosure Schedules
  - Are seldom detailed enough to bring true visibility into the PII, subject to the R&W
- Covenants
- Changes to business?
- … these need to be negotiated …

sajai@jsalaw.com

Negotiations, post-Diligence

- While the Due Diligence stage is an exercise to find crucial issues, the transaction negotiation stage is an attempt to resolve these issues
  - Information collected during Due Diligence is reflected in the representations and warranties and determines the operative sections of the transaction documents
- Purchaser endeavours to limit taking on obligations of the Target
  - Similarly, Purchaser should avoid liability for past privacy breaches at the Target
  - Target, in an asset purchase indemnifies itself for all future privacy infractions
  - Expressly addressing such obligations and liabilities in the sale or acquisition contract helps prevent confusion and even disputes from arising.
- The key provisions of a definitive agreement related to PII are the representations and warranties

Negotiating Privacy-Related Terms

- Representations and warranties
  - **Statutory Compliance** – That the Target is in compliance with all applicable data privacy laws. Such a representation is crucial in a stock purchase, as liability for statutory violation passes on to the Purchaser
  - **Compliance with Privacy Policy** – If Target collects information from its customers or other users, the Seller makes warranties about policies pursuant to which such information is collected and maintained
  - **Compliance with Material Contracts** – Confirmation on enforceability of and compliance with agreements which relate to PII; and contracts with third party service providers contain required data security and confidentiality obligations
- Disclosure schedule considerations
- Other ways to reduce or allocate risk
  - Closing conditions
  - Indemnities, purchase price adjustments,
  - Holdbacks
- Seller's focus on Qualifiers & Disclosure Schedules

Closing

- By this stage in the transactions both the parties have usually satisfied all the conditions precedent to closing, such as providing notice or obtaining consent of Data Subjects
- A share purchase affects relatively few aspects of data privacy, since the PII itself still belongs to the same company and only the shareholders change
  - While the Purchaser in a share purchase needs to know what its legal obligations are, the obligations themselves will remain the same as before the purchase
- In a cross-border asset purchase, however, the PII actually changes jurisdictions, and laws applicable to both parties apply to how PII is managed and actually transferred
  - These applicable laws will need to be adhered to strictly otherwise both parties may be liable under one if not multiple jurisdictions

Integration

- Poorly executed integration plan can destroy shareholder value (of the purchaser)
- There are pros and cons of merging marketing databases
- Considerations in updating
- Privacy policies/notices
- When and how can buyer use acquired data for marketing purposes?
- Post-closing handling of employee data, personnel files
- Decision-making on system and activity integration

Thank you

Sajai Singh
+91-9845078666
sajai@jsalaw.com