



# Data Privacy and Security in M&A and Strategic Transactions

*A Playbook for Managing Consumer, Location, and Health Data as Privacy Risks and Laws Continue to Evolve*

Cynthia Cole & Joy Johns

# Welcome!



**Joy N. Johns**  
Senior Counsel, Data  
Protection & Cybersecurity  
*Eaton*



**Cynthia Cole**  
Partner  
*Baker McKenzie*

# Agenda

- 00** Introduction
- 01** Identifying privacy-related risks in M&A deals
- 02** Key diligence issues
- 03** Addressing data protection risks during negotiations
- 04** Allocating and mitigating privacy risks in M&A transactions
- 05** Ensuring successful integration post-closing

# The Role of Data Privacy in Transactions

Target company's use of data is often a key link in its value chain, but...

## Data as an asset



### Customer data:

- Can help company identify markets for products.
- Create new customer experiences.
- Evaluate success of existing product lines.
- Manage accounts such as loyalty programs.



### Employee / HR data:

- Make informed hiring decisions.
- Maintain safe and secure working environment.
- Assess employee performance.



### Sensitive data:

Many companies in specific sectors need to handle sensitive data to perform core functions – for example, healthcare companies use health data to administer care to patients or to conduct clinical trials.



### Third party data:

company may handle third party data to perform services for customers.



### Data transactions:

Company may transact in data itself by selling it to other parties.

# The Role of Data Privacy in Transactions

...but the use of data also creates a number of areas of significant potential risk.

## Data as a liability



### Putting a target on your back:

Acquiring significant amounts of data make entice threat actors, who target data-rich organizations.



### Costly security measures:

Securing data may be expensive or require changes to organizational conduct and systems.



### Data management obligations:

Collection of data creates potentially costly management obligations under privacy laws, such as responding to data subject requests.



### Notification requirements:

Notifications to regulators if data is compromised – many notification requirements are triggered based on the volume and/or type of data involved.



### Litigation and regulatory enforcement:

Risk of class actions or regulatory enforcement if data is compromised – often, The more data a company possesses, the greater its potential legal and regulatory exposure.



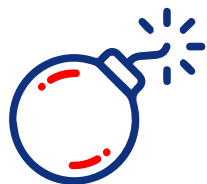
### Reputational injury and loss of value:

Breach or mishandling of data can cause significant reputational harm.

# The Role of Privacy Diligence



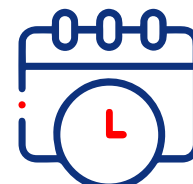
Unresolved risk can:



Undermine  
target value



Stall  
negotiations



Require pre- or  
post-closing covenants

# Focus Areas of Diligence



## Privacy & Security Program

- Is the target subject to industry-specific privacy regimes (e.g., HIPAA, GLBA, FCRA)?
- Does target have privacy notices and policies that comply with relevant privacy laws (e.g., GDPR, CCPA, other state laws)?
- Does the target provide notice of its privacy policy to its employees?
- Does the target engage in targeted advertising? Does it provide opt-outs?
- Is children's data collected? And, if so, does the target have a COPPA compliance program?
- Is sensitive data and/or biometric data collected?
- Does the target sell (including for nonmonetary valuable consideration) personal data to third parties? Does it buy such data?
- Does the target have established procedures to complying with incoming data subject requests?
- Does target have required mechanisms in place for cross border data transfers?



# Focus Areas of Diligence

## Governance practices

- Who is **responsible** for data security within organization? Have they participated in data security training / been involved in the development of data security protocols?
- Has the target made investments in its **information security team** commensurate with its size and the volume and types of data it uses?
- Is the target able to identify the **cybersecurity laws and regulations** that apply to it?
- Has the target appointed a **data protection officer (DPO)**?
- Is there board oversight of DPO?
- Has the target conducted any audits, vulnerability tests, or impact assessments recently?

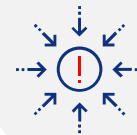




# What Are Reps and Warranties (R&W)?

- R&W are contractual tools that allow parties in a transaction to place the risks of unknown circumstances upon the seller
- They include past and present declarations by the seller about the state of its business operations as of a set date
- R&W give the buyer a more accurate understanding of the quality of seller's business along with any accompanying risk factors
- Seller can be liable for damages incurred by a buyer whose losses are caused by the buyer's reliance on an untrue statement in the R&W
- Buyers prefer extensive R&W to augment their own due diligence investigation of a seller – especially regarding circumstances that buyers cannot foresee or have no reason to know to look for

# Data Privacy R&W



## Data privacy R&W can include:

- compliance with privacy and data security laws
- compliance with contractual requirements
- security of IT assets
- detection of vulnerabilities and breaches
- disclosure of data related claims and investigations
- disclosure of third party data sharing

R&W should be backed by indemnities and address any significant due diligence findings and assumptions

Seller will be liable for damages if the R&W is breached or untrue and the buyer suffers damages as a result

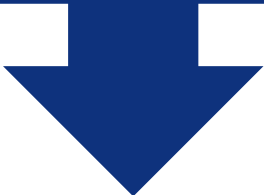
Damages are generally calculated as expectation damages

R&W create large potential liabilities, for example, if a seller is not in compliance with data privacy laws and is hit with a fine


R&W insurance is crucial to hedge against the risk of needing to pay associated costs of a data privacy incident covered by the R&W

# Implementation focus areas


Analyzing and identifying personal data (e.g., including sources of data and data subjects) and the IT assets on which such data resides



Drafting agreements to facilitate the transfer and continued processing of personal data



Developing plans and timelines for providing updated notices and obtaining new consents as required



Implement controls and manage permissions to mitigate heightened data security risk during implementation phase



# Tips for a Successful Post Acquisitions Integration

- 1 Incorporate PAI planning part into your M&A process.
- 2 Define key objectives and engage internal stakeholders across key functions in PAI planning.
- 3 Organize Integration Management Office with designated functional leads and regular status reporting.
- 4 Communicate operating guidelines for pre- and post-closing period.
- 5 Develop a fully vetted macro plan based on key objectives.
- 6 Identify and plan around local country complexities.
- 7 Verify corporate data and good standing of subsidiaries and fix deficiencies.
- 8 Create a micro plan that is a detailed implementation roadmap.
- 9 Establish a centralized process for documenting and closing integration transactions.
- 10 Leverage technology tools for efficiency.

# Practical Tips



- Understand the client's industry and geography and the particular risks that apply
- Use the diligence process to flag areas that need to be addressed in purchase agreement and covenants.



Be aware of extraterritorial effect of laws like the GDPR and CCPA



Identify whether sector-specific cyber and privacy rules apply (e.g., HIPAA, CIRCIA)



Vendor access to data increases vulnerabilities – does the target use vetting and agreements to mitigate increased risk?



Understand your tolerance for risk from the outset

# Practical Tips



## Create an integration plan



Determine whether (and to what extent) buyer and target IT systems need to be integrated



Rely on technical advisors to identify potential issues and solutions for integration



Focus on cyber security in TSA

Click to add text

Click to add text

UC Berkeley  
Center for Law & Technology