PRIVACY AND CYBERSECURITY: A BIG DEAL FOR YOUR BIG DEALS

- Eric Bukstein, CIPP/US, Lead Data/Privacy Counsel, PwC
- Tricia Cross, Senior Counsel, Privacy, Twenty-First Century Fox
- Scott Loughlin, Partner, Hogan Lovells

The views presented in these slides and expressed during this panel are the personal views of the panelists and should not be attributed to their employers.
PANEL AGENDA

- Introduction: Case Study
- Key Transactional Considerations
  - Compliance Obligations
  - Compliance Risks
  - Cybersecurity
- Incorporating Privacy and Security Into Business Transactions
- Dealmaking
  - Pre-Transaction Risk Assessment
  - Pre-Transaction Diligence
  - Scope of Diligence
  - Covenants
  - Reps and Warranties
  - Risk-Shifting Provisions (Indemnity, Limitations on Liability)
  - Termination
  - Ongoing Risk Management
INTRODUCTION: A CASE STUDY

Your company, Alpha, is a multinational hospitality company that operates hotels throughout the world. Alpha hopes to develop innovative new internal consumer targeting and marketing tools by pursuing a partnership with Beta, a private venture-backed (and well-funded) Silicon Valley company that commercializes artificial intelligence (AI) technologies.

In the partnership, Alpha will provide its data—both internal data and data relating to hotel customers. Beta will deploy its cloud-based AI software to crunch the data. Together, Alpha and Beta will develop new tools for Alpha to implement that will be designed to identify past Alpha customers who are likely to be repeat visitors to Alpha hotels.
INCORPORATING PRIVACY AND SECURITY INTO BUSINESS TRANSACTIONS

Role of privacy and security professionals in transactions:

- Compliance review
- Due diligence
- Negotiation
- Risk assessment
- Tools for commercial lawyers
KEY TRANSACTIONAL CONSIDERATIONS: COMPLIANCE OBLIGATIONS

Deals that involve data sharing trigger compliance obligations.

- Vendor oversight
- International data transfers
- Required contractual terms
KEY TRANSACTIONAL CONSIDERATIONS: COMPLIANCE AND CYBERSECURITY RISKS

Inappropriate use, maintenance or disclosure of data can be costly.

- Government investigations and consent decrees
- Fines - both civil and criminal
- Lawsuits and significant reputational harm
- Compromise of valuable data assets
DEALMAKING: PRE-TRANSACTION RISK ASSESSMENT

Identify the importance of the business objectives and the significance of the data-related risks.

- Value and sensitivity of the data
- Compliance obligations
- Exposure in the event of compromise
DEALMAKING: PRE-TRANSACTION DILIGENCE

Why perform due diligence of vendors and data partners?

- Satisfying legal obligations
- Fulfilling contractual obligations
- Complying with public-facing policies
- Avoiding liability
- Protecting your reputation
DEALMAKING: SCOPE OF DILIGENCE

How extensive should diligence be?

- Commensurate with the sensitivity of the data

Scale diligence efforts appropriately:

- “Paper only” review of key policies
- Risk assessment and audit reports
- Full audit of the vendor
DEALMAKING: COVENANTS

When providing data, consider:
- Confidentiality
- Limitations on uses and disclosures
- Definitions of data and other terms
- Protections and safeguards

When receiving data, consider:
- Is there data you do not want?
  - Highly regulated data; data that carries large liabilities
- Can you handle the privacy/security obligations the other party seeks?
- Will you have sufficient data rights to accomplish your goals?
DEALMAKING: DATA BREACH NOTIFICATION

Important elements:
- Definition of a “breach”
- Data breach triggers and notification
- Timeline
- Content of notices
- Required remediation response and investigation
DEALMAKING: REPS AND WARRANTIES

Compliance:
- Appropriate limitations on processing
- Required jurisdictional terms
- International data transfers
- Compliance with laws

Security:
- Information security program
- Specific security safeguards
- Security assessments and vulnerability remediation
DEALMAKING: RISK-SHIFTING

Negotiation dynamics:
- Leverage
- Scope of parties’ relationship

Indemnity:
- Breach damages, notification obligations, and credit monitoring
- Forensic, legal, and PR expenses
- Regulatory investigation and enforcement (fines and penalties)
- Private lawsuits
SAMPLE INDEMNIFICATION CLAUSES

Pro-customer:
Vendor shall defend, indemnify, and hold harmless Customer, its affiliates and related entities, and its and their respective officers, directors and employees from and against all liabilities, obligations, losses, damages, costs, fees, penalties, fines, charges or other expenses of any kind (including but not limited to reasonable outside attorneys’ fees) resulting or arising from, relating to or in connection with any third-party claim resulting from: (a) the unauthorized disclosure of or access to Customer’s data or other confidential information; or (b) a breach of the confidentiality or data security terms in this agreement by Vendor.

In addition to its indemnification obligations above, Vendor shall reimburse Customer for all out-of-pocket costs and expenses reasonably incurred by Customer as a result of a data breach, including the costs of (a) preparing and sending notifications to individuals or governmental authorities; (b) providing credit monitoring services to individuals affected by the data breach; and (c) investigating the data breach.
SAMPLE INDEMNIFICATION CLAUSES

Pro-vendor:
Each party (the “Indemnifying Party”) shall defend, indemnify, and hold harmless the other party (the “Indemnified Party”) and its officers, directors and employees from and against all losses, damages, penalties or fines resulting from any third-party claim alleging that: (a) the Indemnified Party’s confidential information was accessed or acquired without authorization to the extent that such access or acquisition was the result of the Indemnifying Party’s breach of its obligations under this agreement; or (b) the provision of personally identifiable information to the Indemnified Party by the Indemnifying Party under this Agreement violates applicable law or the rights of any third party.
DEALMAKING: RISK-SHIFTING

Limitations of liability:

- Caps on damages
- Limits on types of damages
- Carve outs
SAMPLE LIMITATION OF LIABILITY CLAUSES

Pro-customer:
Except with regard to (a) the unauthorized access to or acquisition of Customer’s data; (b) the violation of the confidentiality or data security terms of this agreement; (c) a party’s violation of law; (d) a party’s negligence or intentional misconduct; or (e) a party’s indemnification obligations under this agreement, in no event shall either party be liable to the other party for any indirect, consequential, special, or punitive damages, whether arising under tort or contract, and in no event shall either party’s total liability to the other party under this agreement exceed the greater of total fees paid or payable by Customer to Vendor during the preceding X months or $X.
SAMPLE LIMITATION OF LIABILITY CLAUSES

Pro-vendor:
In no event shall either party be liable for any indirect, consequential, special, or punitive damages, or for any damages arising from the loss of revenue, profits, goodwill or data, or the cost of substitute services, whether arising under tort, contract, strict liability or indemnification and regardless of whether such party was informed in advance of the possibility of such damages. Subject to the foregoing, in no event shall either party’s total liability under this agreement exceed the total fees paid by Customer to Vendor during the preceding X months.
DEALMAKING: ONGOING RISK MANAGEMENT

Risk mitigation does not end when the deal signs.

- Access to internal reports
- Access to third-party reports (e.g., SSAE, vulnerability scans)
- Customer audits
DEALMAKING: TERMINATION

Termination rights:
- Events triggering termination rights
- Cure period vs. immediate
- Relationship to overall business deal

Post termination obligations:
- Survival
- Return/destruction requirements
- Transition
QUESTIONS?

Thank you!