Privacy and Data Security for M&A Transactions

March 24, 2017

Reed Freeman, WilmerHale

Eric Hwang, WilmerHale

Christopher Rose, WilmerHale

Ruby Zefo, Vice President Law and Policy Group, Associate General Counsel and Chief Privacy and Security Counsel, Intel Corporation

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Agenda

- Overview
- Identifying Key Privacy and Data Security Issues
  - Deal Impacting Issues (Privacy first, then Data Security): *Problems affecting valuation or viability of the deal*
  - Integration Planning Issues (Privacy first, then Data Security): *Problems to be addressed post-close*
- Language on Privacy and Data Security in Acquisition Agreements

- Appendix: Privacy and Data Security Due Diligence Checklist

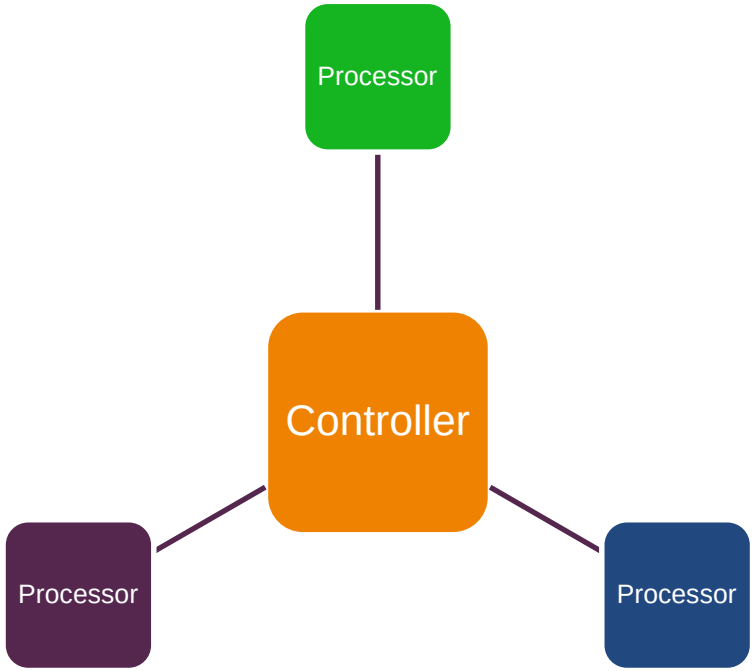
Overview

- All companies have data about customers, clients, employees, investors, partners and vendors
  - Regulations vary by jurisdiction
    - US privacy law is a patchwork of jurisdiction-specific and sector-specific laws, FTC consent orders, litigated decisions, and FTC reports
    - EU privacy law is comprehensive, and applies to almost all data about people collected in the EU
    - Asian privacy law is emerging, and many jurisdictions are taking an EU-style approach

- Privacy and data security risks will be present, at some level, in almost any transaction

Overview

- Identify the target's status in the data-processing ecosystem:
  - A "controller" collects its own data and makes decisions about how the data is used
  - A "processor" receives data from others and may only use the data for specific purposes
  - Many companies are both – they control data about their employees and process data on behalf of customers
- Understand the post-deal landscape – will the target be integrated or kept separate?
  - Impacts transfers, sharing, disclosures, etc.



Deal Impacting Issues: Sharing Employee Data

- Transfer of employee data after the deal
  - Cross-border implications
  - New notices to employees about processing needed?
- Control of employee data
  - Records retention
  - Managing access and amendment rights

Deal Impacting Issues: Past Privacy Representations

- External and internal privacy statements and notices
  - Do they align with the target's actual practices?
  - Are required notices or disclosures missing or inadequate?
  - Representations made at the point of collection run with the data, regardless of who owns it, until the data subject agrees otherwise
  - Historic data collection notices by the target may:
    - Limit permissible uses of personal data by the acquirer
    - Preclude the data's sale or disclosure to third parties

Deal Impacting Issues: Transfer Limitations

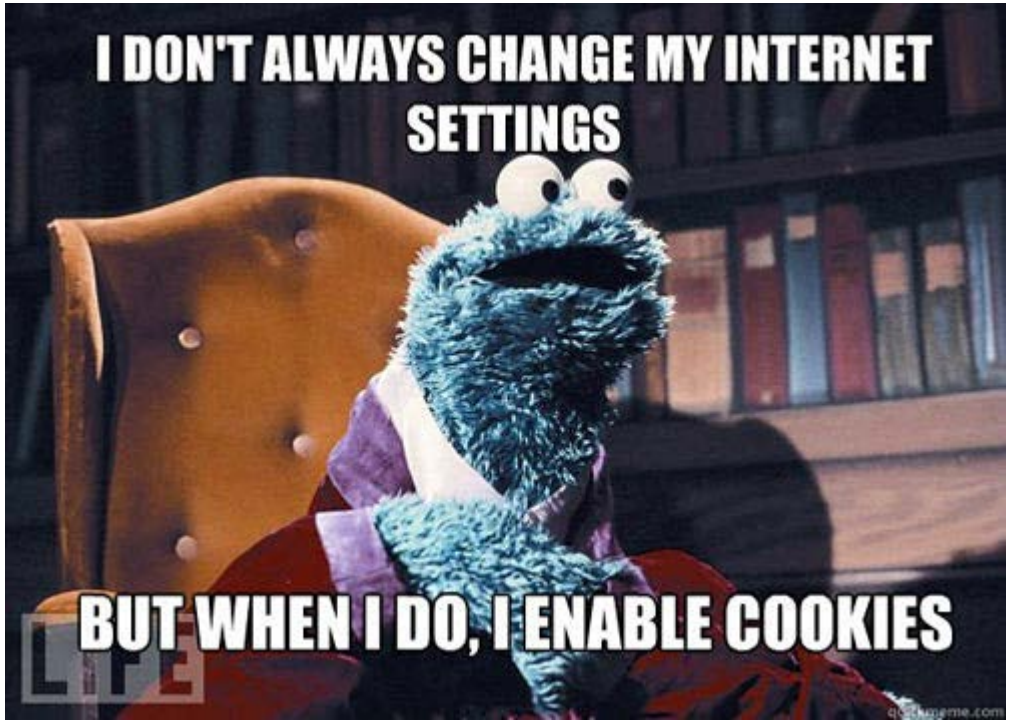
- <u>Can the data be transferred like any other asset?</u>
  - What were the target's representations made regarding transfer?
  - Note regulations that may limit transfer or disclosure of information. Can data be transferred without consent?

Integration Planning Issues: Use Limitations

- <u>Many US privacy laws and regulations are focused on contacting consumers for marketing purposes</u>
  - Consent to contact via one channel may not be transferred to other channels
  - Repurposing data previously collected from consumers requires care

Integration Planning Issues: Tracking Technologies

- <u>Online solutions or mobile applications that track consumers or customers generally require disclosures</u>



- After an acquisition, these disclosures may require adjustment
  - If the changes are material and apply to previously collected data, opt-in consent to updated disclosures may need to be required
  - Implementing new disclosures may require that tracking activities be suspended or limited until remediation is complete

Integration Planning Issues: Merging Customer Records

- <u>Combining customer records following an acquisition may raise issues if the promises made to customers at the time of collection were not adequate</u>
  - Regulators may raise questions about combinations of customer accounts
  - Regulators may also believe that customers could be surprised about changes in account settings, and raise complaints

"Before I write my name on the board, I'll need to know how you're planning to use that data."

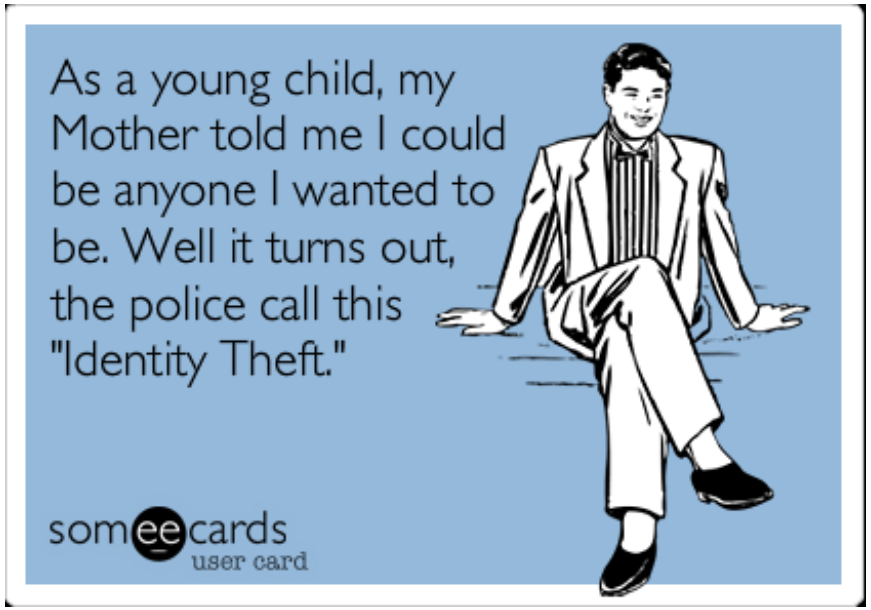
Deal Impacting Issues: Data Security, Breaches and Security Incidents

Deal Impacting Issues: Data Security Program

- Target's Data Security Program
  - Does the target have appropriate electronic, technical and physical security measures to protect personal information and sensitive personal information relating to customers, clients, employees and other workers, worldwide, and provide all related company policies?
  - FTC has published "Start with Security: A Guide for Business" describing ten key steps that a business should take to address privacy and data security
    - Does the target have any known security vulnerabilities? How is the target the addressing them?
    - Have there been any actual or alleged data security breaches or unauthorized access or acquisition of personal information or sensitive personal information?

Deal Impacting Issues: Breach Notification and Cyber Insurance

- Did the target fail to notify or disclose following the breach / incident?
  - Undisclosed security incidents should be assessed to determine whether:
    - Disclosure is legally required; and
    - Would disclosure of the incident affect the target's value?
      - What information was accessed?
      - How was the information used?
  - Data breaches are not just legal nightmares, but they can also be PR and reputational nightmares



- Check to make sure the target is carrying adequate cybersecurity/data breach insurance

Deal Impacting Issues: Ongoing Regulatory Inquiries

- <u>Understand any on-going regulatory inquiries and their potential impact on the target</u>

- Regulatory settlements can:
  - require that data be destroyed, reducing the value of customer databases or agreements
  - include monetary penalties,
  - long-term third-party audit obligations, and
  - implementation of an internal privacy program
- Beginning in May 2018, EU authorities may impose fines up to 4% of global annual revenue under the General Data Protection Regulation

Integration Planning Issues: Evaluating Privacy Program Maturity

- **Consider using a "Privacy Program Maturity Model"** to assess target's business units and identify priorities – one common model was developed by American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA)
- A simplified maturity model might look like this:

Ad Hoc	Repeatable	Defined	Managed	Optimized
• Practices are informal and unwritten • Employee training is unstructured or rare • No clear responsibility for privacy or security	• Some policies exist, but may not be complete or may not cover all topics • Employees receive periodic guidance • Privacy and security identified as a management responsibility	• Key policies exist addressing major privacy and security issues • Employees are trained on policies • Someone has been identified as responsible for privacy and security	• Policies have been implemented • Employees receive regular training and guidance • Privacy and security issues are actively monitored by employees with relevant expertise	• Policies are monitored and enforced • Employee training is regularly updated/modified • Upper management supports privacy and security functions

Integration Planning Issues: Understanding the Target's Existing Program and Obligations

- <u>Understand what laws and regulations apply to the target's ongoing data use and collection practices</u>
  - FTC can bring a cause of action against the acquirer for activities of the target pre-close based on successor liability
  - If issues identified during due diligence are going to be addressed post-close, be sure to address them quickly!

Integration Planning Issues: Policies and Procedures Required by Statute or Regulation

- <u>Failure to have appropriate policies and procedures in place to safeguard sensitive information may be an unfair trade practice</u>
  - Depending on the industry and the jurisdiction, statutes may require adopting specific policies and procedures
    - **COPPA** applies to websites and apps directed to kids under or that knowingly collect information from them
    - Sector-specific laws include **HIPAA** (health care), **GLBA** (financial institutions)
    - Jurisdiction-specific laws apply in states like **California**, **Massachusetts**, and **Nevada**
    - Jurisdiction and sector-specific laws in New York (financial institutions), **Texas** (health care)

Integration Planning Issues: EU General Data Protection Regulation Preparedness

- <u>The EU General Data Protection Regulation (GDPR) is a comprehensive law on privacy and the processing of personal data</u>
  - Will take effect in May 2018
  - Key changes include:
    - accommodation of data subject rights,
    - maintenance of records,
    - appointment of persons to supervise compliance, and
    - consultation with regulators before engaging in some activities
  - Large fines for non-compliance

- <u>Is the target ready for the GDPR? If not, will the target be ready by May 2018</u>?

Integration Planning Issues: EU General Data Protection Regulation Preparedness

- <u>The EU's comprehensive approach is increasingly the baseline for new data protection laws in other countries</u>
  - Scope of information protected is *much* broader than information protected in the United States:
    - 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
  - <u>What does this mean</u>?
    - Most data about individual people could meet this definition
    - Be careful with "anonymous" data

Integration Planning Issues: Vendor Management

- <u>Almost all companies use third-party vendors to manage personal data about employees, customers, and consumers</u>
  - These vendors' practices can be a source of privacy and data security risks
  - Companies should:
    - do due diligence on companies before making them vendors,
    - use appropriate contractual controls, and
    - monitor vendors for compliance with contracts
  - If vendor relationships are being transitioned during the deal:
    - Review contractual protections
    - Implement assessment or monitoring

Integration Planning Issues: International Data Transfers or Storage

- <u>Almost all companies transfer or store data outside of the United States</u>
  - Transfers may be to affiliates, vendors, data centers, cloud service providers
  - Subject to the laws of the jurisdiction where the servers are located
- <u>Understand which laws apply to the target's data and ensure the target has a plan for compliance</u>
  - Acceptable mechanisms for transferring data from the EU include Privacy Shield, Standard Contractual Clauses, and BCRs
    - Remember that many EU countries also require registration of data processing activities, and registration may need to updated post-closing
  - Data localization laws limit or restrict transfer of data out of a jurisdiction (e.g., Russia's Federal Law No. 242-FZ and China's Cybersecurity Law)

Language on Privacy and Data Security in Acquisition Agreements: Representations & Warranties; Covenants

- *Defining "personal information" or "personal data"*
  - ***Buyer*** - Consider a broad definition that includes unique device identifiers, IP addresses, and other information that could be linked to a person
    - Include information covered by the EU's GDPR
  - ***Seller*** – Make sure the definition is consistent with your practices and reaches only the information you treat as personal information / data

- Policies and Procedures
  - If the target has a written information security policy (WISP), target should represent that it has complied with and will comply with the WISP
  - If the target does not have a WISP, the target should covenant to use reasonable best efforts to establish an information security program and comply with it during the period prior to closing

Language on Privacy and Data Security in Acquisition Agreements: Representations & Warranties; Covenants

- <u>Compliance</u>
  - With all laws, including applicable laws related to privacy, data security, and the processing of personal information
  - With target's own policies, representations to consumers & employees, contracts, and applicable industry standards
  - With notices, consents, and other information provided to data subjects regarding the processing of personal information

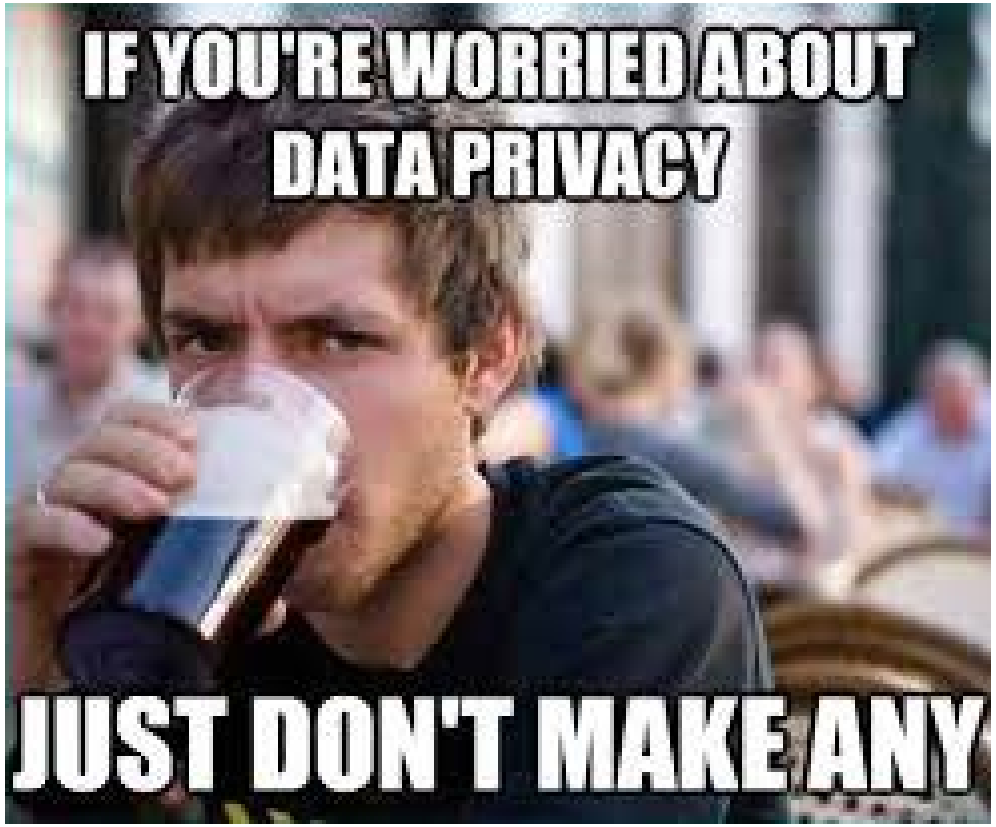
Language on Privacy and Data Security in Acquisition Agreements: Representations & Warranties; Covenants

- Data Utility
  - Target collected data consistent with relevant laws, provided required notices, and obtained consents that permit the use of the data in the context of target's current business operations and (if possible) the buyer's intended use of the data
  - No other restrictions on use of the data
- Data Incidents
  - No data security incidents, complaints, unaddressed notices of security vulnerabilities or investigations by regulatory authorities
  - Service providers, vendors, and contractors responsible for data handling have not experienced any incidents related to the data that is the subject of the contract

Language on Privacy and Data Security in Acquisition Agreements: Conditionality and Indemnification

- Buyers with leverage can sometimes include Privacy and Data Security reps as part of the package of Intellectual Property Reps, which often come with enhanced indemnity and closing condition protections
- Regardless of the caps and limitations on coverage, ensure that the indemnification package is adequate to cover identified compliance issues (coupled with pre-closing covenants to help bring the target into compliance by or shortly after)
  - For known data breaches or regulatory inquiries, consider carving these out of the general escrow and creating a special escrow with a sufficient duration and fewer limitations on recovery
  - Data breach costs are usually related to the volume of records breached, not the economic value of the records
- Additionally, for known breaches or inquiries, consider appropriate covenants and closing conditions relating to their resolution or progress

Thank you!



Appendix – Sample Privacy and Data Security Due Diligence Checklist

Privacy

1. Provide copies of all current and prior versions of internal and external privacy policies and notices, including website and app policies and notices, relating to the collection, use, sale, lease or transfer (including cross border transfer) of personal information and sensitive personal information of customers or clients.
2. Provide copies of all current and prior versions of internal and external notices, privacy policies, training materials and manuals relating to the collection, use, sale, lease or transfer (including cross border transfer) of personal information and sensitive personal information relating to employees, contractors, and temporary workers.
3. “Personal information means any information that can be used to identify an individual.
4. “Sensitive personal information” includes Social Security Numbers, government identification numbers, credit or debit card numbers, financial account information, precise geolocation information relating to an individual, video viewing behavior relating to an individual, driver’s license number, and information relating to an individual’s health, race, ethnicity, religious or philosophical beliefs, trade union membership, political beliefs, sexual orientation, and criminal background.

Appendix – Sample Privacy and Data Security Due Diligence Checklist

Privacy (Continued)

5. List all jurisdictions where the company have employees or offices or equipment, and all filings with and approvals received from any data protection authority or regulator relating to personal information and sensitive personal information of any customers, service providers, third parties, or employees.
6. List all jurisdictions from which the company collects personal information or sensitive personal information from individuals.
7. State whether the company de-identifies personal information or sensitive personal information. If so, state the circumstances in which is does so and the means by which it does so.
8. State whether the company uses encryption for personal information or sensitive personal information in transit or at rest. If so, state the circumstances when it does so.

Appendix – Sample Privacy and Data Security Due Diligence Checklist

Privacy (Continued)

9. List all types of personal and sensitive personal information collected, processed, and shared with any third party. If shared, provide copies of all contracts regarding such sharing.
10. Provide all agreements with customers, service providers and other third parties relating to the collection, provision, use, sale, lease or transfer (including cross-border transfer) of personal information or sensitive personal information.
11. Explain how the company gets compliant consents for various forms of direct marketing and other communications, and how such consents are tracked and managed (i.e., for e-mail marketing, direct mail marketing, telemarketing, delivery of marketing and non-marketing text messages, fax advertising, delivery of marketing and non-marketing prerecorded messages, use of an autodialer to place marketing and non-marketing calls to cell phones, and any other methods of communicating).

Appendix – Sample Privacy and Data Security Due Diligence Checklist

Privacy (Continued)

12. State whether the company uses sensitive information in its direct marketing.
13. Describe all uses of tracking mechanisms, including cookies, beacons/tags, Javascript, local storage, browser fingerprinting, or similar means used to track individuals online for purposes of online advertising, personalization, or content delivery. Provide a list of, and contracts with, all vendors and service providers used for those or similar purposes.
14. Provide copies of any certifications or related documents in connection with the Privacy Shield program in connection with the transfer and protection of "personal information" from the European Union or Switzerland to the U.S.

Appendix – Sample Privacy and Data Security Due Diligence Checklist

Data Security

1. Describe all electronic, technical and physical security measures to protect personal information and sensitive personal information relating to customers, clients, employees and other workers, worldwide, and provide all related company policies.
2. Provide all external audit and similar reports, including reports of any penetration testing and vulnerability assessments, relating to data security.
3. Provide all certifications relating to data security (e.g., SAS70, ISO 27001, and any PCI-DSS ROC).
4. Provide copies of the company's plans for addressing actual or suspected security incidents.

Appendix – Sample Privacy and Data Security Due Diligence Checklist

Data Security (Continued)

5. Describe any known security vulnerabilities and how the company is addressing them.
6. Describe all actual or alleged data security breaches or unauthorized access or acquisition of personal information or sensitive personal information.
7. Describe any data security breaches or unauthorized access or acquisition of personal information for which notice was provided to individuals or to any regulator or public authority, as well as copies of all such notices.
8. Describe any company program to intake reports of actual or suspected security vulnerabilities, and copies of policies on how the company addresses such reports.

Appendix – Sample Privacy and Data Security Due Diligence Checklist

Data Security (Continued)

9. Describe and provide any complaints, notices of suspicious activities (including potential data security vulnerabilities), regulatory inquiries, consent decrees, citations, fines, administrative actions or litigation regarding privacy or data security.
10. If applicable, provide an explanation of measures taken to comply with the Payment Card Industry (PCI) Standard. The PCI Standard requires card payment processors to have in place certain measures to protect cardholder data. In particular, the processors should build and maintain a secure network; encrypt transmission of cardholder data across open, public networks; use and update anti-virus software; develop and maintain secure systems and applications; implement strong access control measures; restrict access to cardholder data on a business need-to-know basis; assign a unique ID to each person with computer access; restrict physical access to cardholder data; regularly monitor and test networks; track and monitor all access to network resources and cardholder data; regularly test security systems and processes; and maintain an information security policy.