Morgan Lewis

M&A ACADEMY

Privacy and Data Security Issues in M&A Transactions

Ezra Church, Don Shelkey, and Lee Harding

February 18, 2020

Overview

- Introduction
- Why should I care?
- Five Key Legal Requirements
  - Sector-Specific laws
  - Privacy Policies
  - Data Security Requirements
  - Breach Notification Laws
  - International Privacy Rules / Cross-Border Restrictions
- Implementing Privacy and Security in Deals
  - Diligence
  - Reps and Warranties
  - TSAs

Why should I care?

- If a target company cannot collect and deploy data consistent with data privacy laws, there may be flaws in the premise for the deal or the business model itself
- Failure of target company to meet its data privacy and security obligations can be a major risk for acquiring company
- Transfer and sharing of data in connection with diligence and after the transaction may in itself violate data privacy laws

Good News / Bad News

- **Good News** – there is no all-encompassing data privacy or cybersecurity statute in the U.S.; the GDPR applies across Europe
- **Bad News** – there is no all encompassing data privacy cybersecurity statute in the U.S.; the GDPR applies across Europe:

Attorney General Enforcement
FTC Act
FCRA
CAN-SPAM
COPPA
Breach Notification Laws
Data Disposal Laws
FERPA
Gramm-Leach-Bliley
MA Data Security Regulations
Red Flags Rule
FACTA
EU "safe harbor" rules
Consumer Class Actions
PCI and DSS Credit Card Rules
Document Retention Requirements
HIPAA

CA Online Privacy Act
CA Consumer Privacy Act
Stored Communications Act / ECPA
Do Not Call Lists
Telephone Consumer Protection Act
Video Privacy Protection Act
Wire Tapping liability
Invasion of Privacy Torts
Computer Fraud and Abuse Act
Communications Decency Act
Spyware Laws
RFID Statutes
FDCPA
Driver's Privacy Act
Social Security Number Laws
Others State Laws

1. Sector Specific US Privacy Laws

Money	Health	Kids
• Gramm-Leach-Bliley Act • Fair Credit Reporting Act (FCRA) • State Laws	• Health Insurance Portability & Accountability Act (HIPAA)	• Family Educational Rights & Privacy Act (FERPA) • Children's Online Privacy Protection Act (COPPA) • State Laws

- Consumer Marketing! Telephone Consumer Protection Act (TCPA), CAN-SPAM, and Do Not Call regulations

2. Privacy Policies—US

- FTC and State Laws (e.g., CA, NV & DE)
- Self-imposed regulation
- Basic principles
  - Notice
  - Access and Control
- Must notify regarding material, retroactive changes
- Language to look for:
  - "Transfer of assets" language
  - Restrictions on sharing/sale of personal information
  - Promises about security
- Look at the language for all entities involved over time; website and mobile
- Other public statements about privacy and security?

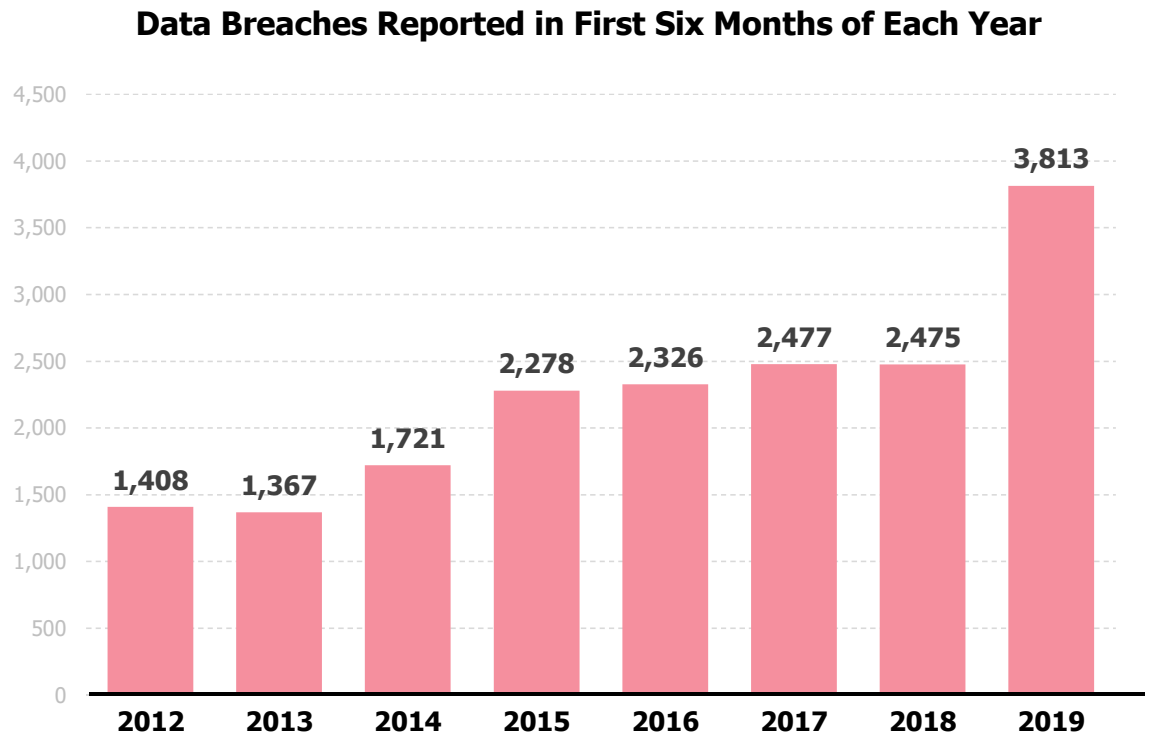
3. Data Security Requirements

- US Sector-specific laws may apply
- GDPR requirement for technical and organisational measures to protect personal data
- Contracts may require certain security standards – NB EU data processing agreements must include security obligations
- MA Security Regulations
  - Have a written information security plan
  - Additional administrative discipline
  - Social security numbers
  - Encryption
  - Training

4. Breach Notification—US

- 50 States and D.C.
- Based on the individual's residence
- Triggering elements vary
- Encryption / lack of use exception – sometimes
- Timing of notice– "as soon as practicable," but need information to notify
- Vendor management

Data Breaches on the Rise



- Source: Risk Based Security, Inc., August 2019

5. International Privacy Rules / Cross Border Data Transfers

- **EU GDPR**
- The GDPR applies to processors and controllers having an EU-based establishment where personal data are processed in the context of the activities of this establishment
- The GDPR also applies to controllers and processors based outside the EU territory where the processing of personal data regarding EU data subjects relates to:
  - the offering of goods or services (regardless of payment)
  - the monitoring of data subjects' behavior within the EU
- Dawn raids, injunctions, penalties for breaching GDPR
- Fines are significant: the higher of 4% of global revenue or 20 million Euros for breaches (likely to be long-standing and significant breaches at the maximum end of potential penalties).
- **Transfers out of EU**
  - Privacy Shield
  - Model clause agreements: good, but must have right language and foreign counterparty who retains liability; NB Brexit and UK likely to be a third-country unless deal is agreed by 29 March (or Brexit postponed)
  - Binding Corporate Rules: hard to implement at multi-national level; can be good for isolated transfers. One European entity retains liability.
  - Consent of Data Subjects: really only works at an individual level; can be revoked at will; not good for database or large-scale transfers. Can be good if just a few European employees or customers.
  - Necessary for Contract Performance: very limited to "necessary"; e.g. address for shipping.
- **APEC Countries; Russia**
  - Data localization in Russia, China
  - Data processing and sharing restrictions

Privacy Policies/Notices—EU

- GDPR includes mandatory transparency obligations
- Privacy policy or notice provided by controllers (only):
  - the identity and contact details of the data controller and where applicable, the data controller's representative) and the data protection officer
  - the purpose of the processing and the legal basis for the processing
  - the legitimate interests of the controller or third party, where applicable
  - the categories of personal data
  - any recipient or categories of recipients of the personal data
  - the details of transfers to third country (e.g. US) and method of transfer such as model clauses or other data transfer agreements
  - the retention period
  - the data subject's rights relating to the processing such as the right of access and rectification
  - the right to withdraw consent at any time, where relevant
  - the right to lodge a complaint with a supervisory authority
  - the source of the personal data and whether it came from publicly accessible source
  - whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
  - the existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences

Breach Notification—EU

- Without "undue delay" (and within 72 hours), controller to notify supervisory authority of data breach unless it is unlikely to result in a risk to individuals' privacy
- Without "undue delay", controller to notify affected individuals if data breach is likely to result in a high risk to individuals' privacy
- Processor to notify controller without "undue delay" upon becoming aware of data breach
- Phases of information can be provided to supervisory authority

M&A - Reps and Warranties

- Privacy and Security related reps and warranties are most often included in the "Intellectual Property" section.
- Common Privacy related reps:
  - Compliance. Seller is in material compliance with all applicable Laws, as well as its own rules, policies and procedures, relating to privacy, data protection, and the collection, use, storage and disposal of personal information collected, used, or held for use by Sellers in the conduct of the Business.
  - No breaches. There has been no unauthorized access to or acquisition of personal information processed by the Seller or on Seller's behalf.
  - Claims. No claim, action or proceeding has been asserted in writing or, to the Knowledge of Seller, threatened in connection with the operation of the Business alleging a violation of any Person's rights of publicity or privacy or personal information or data rights.
  - Security. Seller has taken reasonable measures, including, any measures required by any applicable Laws, to ensure that personal information used in the conduct of the Business is protected against unauthorized access, use, modification, or other misuse.
  - Transaction compliance. The transaction itself, including execution of the related documents will not violate privacy laws or any contract or other commitment of Seller.
  - Known vulnerabilities. For technology / software heavy deals, there are no vulnerabilities in the NIST NVD.

M&A - Privacy related Diligence (Buy Side)

- Scope and effort driven by risk profile.
- Review privacy policies and contracts.
- Review compliance with industry, data, and jurisdiction-specific rules (Money, Health, Kids, Consumer Marketing, EU data).
  - Consider discussion with privacy officer / privacy counsel.
- Review security-related documents for red flags.
- Review any data braches carefully, incl. response planning and team, vulnerability scans, audits; ask hard questions.
- Rep and warranty insurers will focus on privacy and security , particularly EU and credit card data.

M&A - Privacy related Diligence (Sell Side)

- Address it head on and project confidence, particularly in regulated industries or retail, uploading privacy policies to the data room and describing data collection and transfer issues.
- Identify potential problem areas and develop a strategy, particularly on breaches, class actions, and government investigations.
  - Keep / develop logs of any data security breaches, remediation efforts, and steps to prevent in the future.

M&A - TSAs

- Transition Services Agreements; common in M&A transactions.
  - Not done with privacy just because a deal is signed / closed.
  - Often involve some of the most sensitive data that the company (employee data, customer data).
  - Involve a member of the privacy team early when discussing the TSA.
  - Could require an information security audit from Buyer (which is somewhat counter intuitive)
  - Think of them as an outsourcing or hosting deal…the issues are the same!


QUESTIONS?

Biography

Ezra D. Church
Philadelphia, PA
T +1.215.963.5710
F +1.215.963.5001

Ezra focuses his practice on privacy and data security matters, and regularly advises and represents clients in connection with these issues, including representation of companies faced with class actions, government investigations, and he has advised hundreds of companies in connection with data breaches and privacy and cybersecurity compliance issues such as data transfer, privacy policies and notice, information security policies, and online and mobile data collection. He has earned designation as a Certified Information Privacy Professional (CIPP) with the International Association of Privacy Professionals. He is co-chair of Morgan Lewis's Class Action Working Group.

Biography

Doneld G. Shelkey
Philadelphia, PA
T +1.617.341.7599
F +1.617.341.7701

Doneld G. Shelkey represents clients in global outsourcing, commercial contracts, and licensing matters, with a particular focus on the e-commerce and electronics entertainment industries. Doneld assists in the negotiation of commercial transactions for domestic and international manufacturers, technology innovators, and retailers, and counsels clients in the e-commerce and electronics entertainment industries on consumer licensing and virtual property matters.

Biography

Lee Harding
London, U.K.
T +44.20.3201.5639
F +44.20.3201.5001

Lee Harding has a broad and versatile practice that goes beyond the provision of traditional legal services. Lee's practice is focused on the myriad legal implications arising out of a rapidly changing workplace: flexible working, five generations in the workplace, giving workers a voice, and the crossover between employment and the regulatory environment, to name but a few. The nontraditional legal services that Lee offers require a proactive approach to managing workplace issues before they escalate. He engages with a wide range of stakeholders to deliver sophisticated and actionable solutions that resonate across the entire business.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.