Morgan Lewis

M&A ACADEMY

Privacy and Data Security Issues in M&A Transactions

Ezra Church, Kristin Hadgis, Don Shelkey and Todd Liao

February 1, 2022

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 (with local laws)
- **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 / Jurisdiction Specific US Privacy Laws

Money	Health	Kids	California
• 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	• California Consumer Privacy Act

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

California Consumer Privacy Act

- First law of its kind in the US and more likely to follow
- Effective January 1, 2020
- Applies to a **business** which: (1) has annual gross revenues in excess of $25 million; (2) annually buys, receives, sells or shares personal information of 50,000 or more consumers, households, or devices, alone or incomgination; (3) **or** dervies 50% or more of its annual revenue from selling consumers' personal information.
- Requires privacy notices be provided at the time personal information is collected
- Gives consumers rights, including:
  - Right to know specific pieces of personal information collected about the consumer in the preceding 12 months
  - Right to delete personal information
  - Right to opt out of sale of personal information
  - Right to a website privacy policy that describes how to exercise these privacy rights
- Requires certain language in contracts with "service providers"

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?

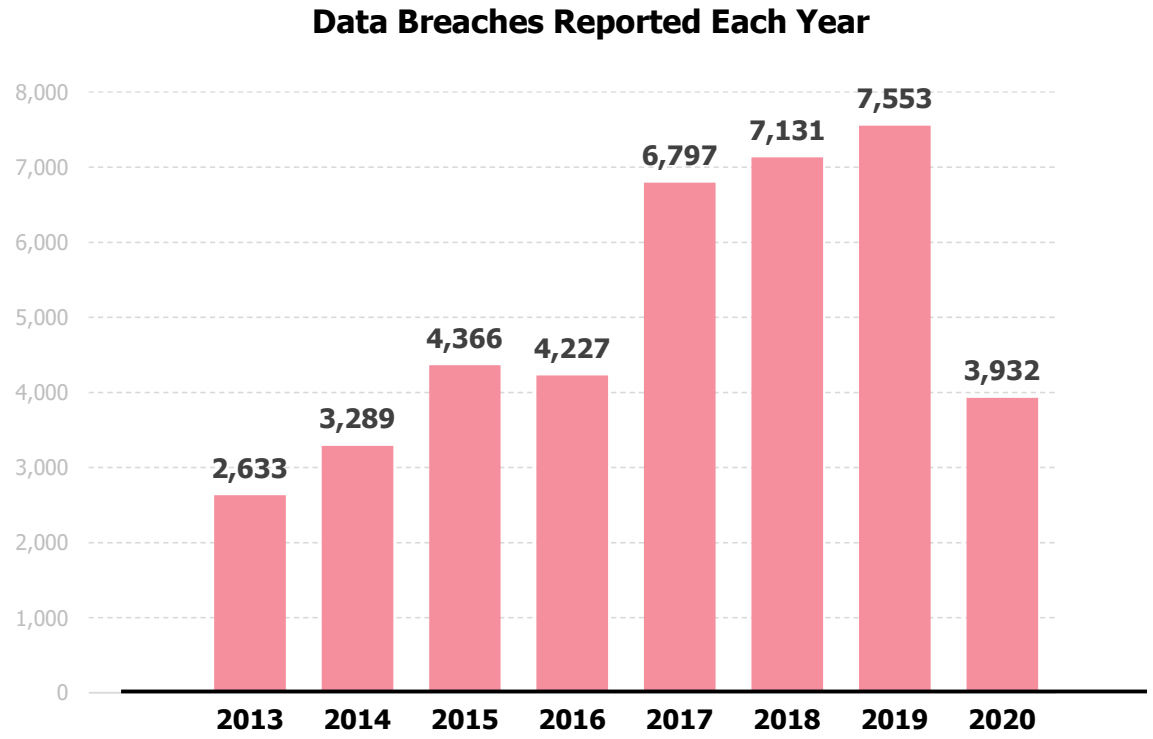
3. Data Security Requirements

- 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/UK 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 / Privacy Policies / Notices - China

- **Chinese Personal Information Protection Law (PIPL)**
  - The PIPL applies to data processing activities within China
  - The PIPL also applies to data processing activities outside China when:
    - the purpose is to provide products or services to individuals located in China
    - analyzing or assessing the behaviors of individuals located in China
  - Dawn raids, penalties, and civil remedies for breaching PIPL
  - Notice to data subjects if personal information will be transferred to the buyer in the M&A
  - Fines are significant: up to 5% of annual revenue or 50 million RMB (approx. $7.9 million USD)
- **Privacy policy provided by controllers:**
  - The identity and contact details of the data controller
  - The purpose of the processing and the categories of personal data
  - Any recipient or categories of recipients of the personal data
  - 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, the right of portability

Cross-Border Data Transfers - China

- **Transfers out of China**
  - Separate consent of data subjects is required.
  - Data localization and government-led security assessment requirements for certain companies and personal information.
  - Security self-assessment requirement for all companies under the recent draft regulation.
  - Standard contractual clauses similar to the EU model will be published by the authorities soon.
- **Triggering Criteria for Mandatory government-led Security Assessment (under draft regulation)**

Key Factors	Triggering Criteria
Based on the "**special identity**" of the data controller	CIIO
	Operators who possess personal information of over a million users
Based on the "**sensitiveness and scale**" of the data to be transferred abroad	The data to be transferred includes "important data"
	Cross-border transfer of personal information of over 100,000 individuals or sensitive personal information of over 10,000 individuals
Other factors	Other situations to be determined by the CAC

Breach Notification and PIPIA - China

- **Breach Notification**
  - Without "undue delay", controller to notify supervisory authority of data breach
  - Without "undue delay", controller to notify affected individuals unless controller adopts measures that are able to effectively avoid harm to affected individuals
- **PIPIA:** Controller should conduct a personal information protection impact assessment (PIPIA) before the following data processing activities:
  - Processing sensitive personal information
  - Using personal information to conduct automated decision-making
  - Entrusting third parties to process personal information, providing personal information to third parties, or publishing personal information
  - Providing personal information abroad
  - Other personal information processing activities that will impose a major influence on individuals

CLE

- If you registered noting that you need CLE, the code is **PLACEHOLDER**. Please save this number; you will need this to receive a Certificate of Attendance. You will be contacted within 30-60 days by our CLE administrative team.
- We will process your credits for other states where this program has been approved.
- Questions? Please email Sarah Trousdale at sarah.trousdale@@morganlewis.com

6. International Privacy Rules / Cross Border Data Transfers

- **EU/UK GDPR**
- The GDPR applies to processors and controllers having an EU/UK-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/UK territory where the processing of personal data regarding EU/UK data subjects relates to:
  - the offering of goods or services (regardless of payment)
  - the monitoring of data subjects' behavior within the EU/UK
- Dawn raids, injunctions, penalties for breaching GDPR
- Fines are significant: the higher of 4% of global revenue or €20 million/£17.5 million for breaches (likely to be long-standing and significant breaches at the maximum end of potential penalties).
- **Transfers out of EU/UK**
  - UK likely to gain adequacy determination (i.e. no restriction on EU-UK data flow).
  - Standard contractual clause agreements: good, but need risk assessments and consider additional safeguards and suspension of data flow rights if risks are too high.
  - Binding Corporate Rules: good for international transfers but they take time to have approved. One European entity retains liability.
  - Consent of Data Subjects: really only works at an individual level; consent must be freely given/fully informed and can be revoked at will; not good for database or large-scale transfers. Can be good if just a few European customers.
  - Necessary for Contract Performance or litigation purposes: limited to "necessary" transfers e.g. address for shipping or a legal dispute (may need to review data before transfer so only necessary data is transferred).
- **APEC Countries; Russia**
  - Data localization in Russia, China
  - Data processing and sharing restrictions in many countries e.g. China, Australia, Singapore, Dubai, Bahrain, Japan, Brazil

Privacy Policies/Notices—EU/UK

- 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/UK

- 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 (any kind of breach)
- Phased information can be provided to supervisory authority as the investigation progresses

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/UK 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)
  - The Seller is likely to be a processor so an EU/UK data processing agreement may be needed (can be included in the TSA)
  - 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

Kristin M. Hadgis
Philadelphia, PA
T +1.215.963.5563
F +1.215.963.5001

Kristin counsels and defends retail and other consumer-facing companies in matters relating to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, retail operations, loyalty and gift card programs, and commercial disputes. Kristin also handles data security incident response crisis management, including any resulting litigation or government investigations.

Biography

Todd Liao
Shanghai
T +86.21.8022.8799
F +86.21.8022.8599

Todd works with clients on a wide range of financial transactions and legal issues involving China. He frequently works with multinational corporations on cross-border mergers and acquisitions, foreign direct investment and investment financing, disposal of Sino-foreign joint ventures and assets, and the structuring of complex commercial transactions. Todd also handles intellectual property (IP) work, specifically assisting clients with managing their trademark portfolios. He is admitted in New York only.

In addition, Todd counsels on matters related to the US Foreign Corrupt Practices Act (FCPA) practice in China and throughout the Asia-Pacific region. He advises multinational corporations regarding compliance with the FCPA and other regulatory compliance matters including policies and practices, gifts, travel and entertainment policies and violations, third-party due diligence issues, managing and conducting investigations of alleged FCPA violations, whistleblower investigations, and employee disciplinary actions. He also conducts FCPA training in multiple languages.

Biography

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

Doneld 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.

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.