Understand Your Cyberthreats:
Key Considerations in Your Company's Cybersecurity

Ezra D. Church| Doneld G. Shelkey | Emily R. Lowe

Overview

Why Should I Care?

Key Legal Requirements

Implementing Privacy and Security in Deals

Why should I care?

- If your company cannot collect and deploy data consistent with data privacy laws, there may be flaws in the business model and prevent your success
- Failure of a company to meet basic data privacy and security standards can result in crippling liability
- Failure of a company to meet basic data privacy and security standards can be a major impediment to financing / acquisition

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 (CCPA)

- Passed into law on March 28, 2019; effective Jan. 1, 2020
- Inspired by the EU GDPR
- California is a traditional leader in US privacy law
- Comprehensive privacy law intended to protect personal information of California residents
- "Personal Information" is defined broadly as any information "that identifies, relates to, describes, is reasonable capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
- 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 in combination; (3) or derives 50% or more of its annual revenue from selling consumers' personal information.

CCPA—Key Requirements

- Notice about what personal information the business collects, purpose, and sharing.
- Right to know categories and specific information collected
- Right to request deletion
- Right to opt out of "sale" of personal information
- Other obligations, include:
  - Contracts with service providers
  - Training employees how to respond to rights requests
- Enforcement
  - AG can seek $2,500 per violation / $7,500 for intentional violations
  - Class actions for data breaches of $100-750 per consumer per incident

What's Next? California Privacy Rights Act (CPRA)

- CPRA "CCPA 2.0" Ballot Initiative, Passed, Nov. 3 (effective, Jan. 2023)
  - Opt-out for sensitive data (racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sex life or sexual orientation, and genetic or biometric data)
  - Right to correction
  - Retention requirements
  - New California Privacy Protection Agency
- Enforcement?
- Other states?

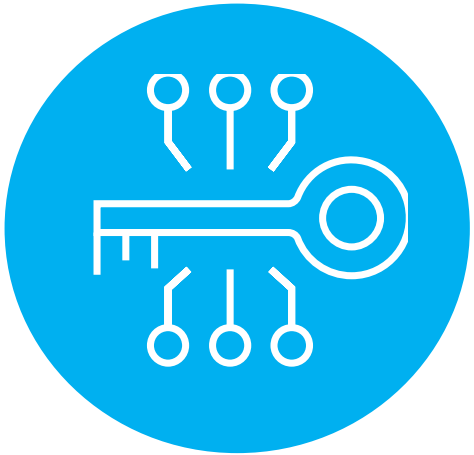
What's next? VA Consumer Data Protection Act (CDPA)

- Virginia CDPA (effective Jan. 2023):
  - Virginia becomes the second state to enact comprehensive consumer privacy laws
  - Similar to CCPA in many respects
  - Requires affirmative consent for processing "sensitive data."

    (racial or ethnic origin, genetic or biometric data, kids data, and precise geolocation)
  - Expanded opt-out to include not just sale, but also use of personal data for targeted ads and profiling
  - Enforced only by the attorney general

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?

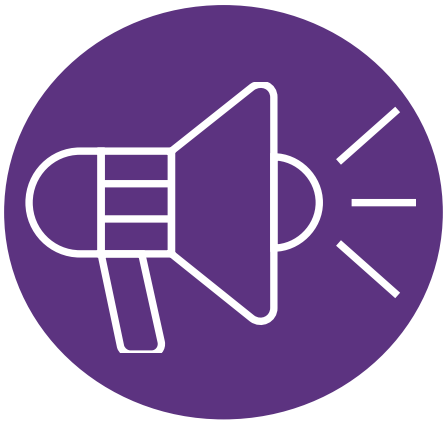


3. Data Security Requirements

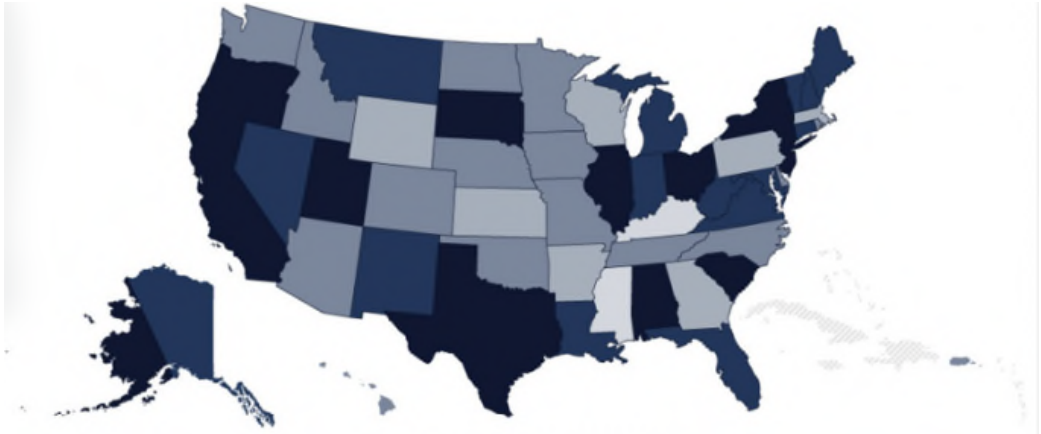
- US Sector-specific laws may apply
- GDPR requirement for technical and organisational measures to protect personal data
- Contracts may require certain security standards – NB EU/UK data processing agreements must include security obligations
- MA Security Regulations
  - Have a written information 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



State Data Breach Notification Laws – All 50+



Stricter laws ← → Less strict laws

5	Alabama	5	Texas	4	Michigan	3	Colorado	3	North Dakota	2	Kansas
5	California	5	Utah	4	Montana	3	Delaware	3	Oklahoma	2	Massachusetts
5	Illinois	4-5	Alaska	4	Nevada	3	Hawaii	3	Rhode Island	2	Pennsylvania
5	New Jersey	4	Connecticut	4	New Hampshire	3	Idaho	3	Tennessee	2	Wisconsin
5	New York	4	Florida	4	New Mexico	3	Iowa	3	Washington	2	Wyoming
5	Ohio	4	Indiana	4	Vermont	3	Minnesota	3	Guam	2	Washington, D.C.
5	Oregon	4	Louisiana	4	Virginia	3	Missouri	3	Puerto Rico	2	U.S. Virgin Islands
5	South Carolina	4	Maine	4	West Virginia	3	Nebraska	2	Arkansas	1	Kentucky
5	South Dakota	4	Maryland	3	Arizona	3	North Carolina	2	Georgia	1	Mississippi

Source: Digital Guardian, 2018

Data Breach – How Much?

> Average total cost of a data breach:

$3.92 million

> Average cost per lost or stolen record:

$150

> Likelihood of a recurring material breach over the next two years:

29.6%

> Average total one-year cost increase:

1.5%

> One-year increase in cost per lost or stolen record:

1.3%

> Average cost savings with an Incident Response team:

$16 per record

Why so much? Categories of costs:

- Detection and escalation (forensics)
- Notification (letters, publicity)
- Lost business (downtime, customers)
- Aftermath (redress, litigation)

Source: Ponemon Cost of Data Breach Survey, 2019

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.

What's going to be on the Due Diligence List?

- Personally Identifiable information (PII)
- Applicable Regulations
- Internal Audit of compliance with Regulations
- Collection of payment information
- US vs. Global
- History of Security Incidents

What's going to be on the Due Diligence List?

- Certifications & Cyber Insurance
- Business Continuity and Disaster Recovery
- Remote Access
- Policies and Procedures
- Employee Training
- HIPAA

Personally Identifiable Information (PII)

- Have a handle on and be ready to disclose:
  - categories of PII collected
  - the methods of collection
  - who PII is collected from
- Do third parties provide or have access to PII?
  - If so, why and how is it handled?
- Transferability

Regulations & Compliance

- Is the Company subject to any of the following regulations with respect to privacy and data security?
  - Federal Trade Commission Act (FTC Act)
  - Fair Credit Reporting Act (FCRA)
  - Telephone Consumer Protection Act (TCPA)
  - Illinois' Biometric Information Privacy Act (BIPA)
  - California Consumer Privacy Act (CCPA)
  - General Data Protection Regulation (GDPR)

Regulations & Compliance

- Is the Company in material compliance with applicable laws and regulations?
  - Are there any outstanding or ongoing compliance initiatives?
- Does the Company do gap assessments (or something similar) with respect to compliance with applicable laws and regulations?

Payment Processing/Collection of Credit Card Information

- If the Company collects credit card information, will need to confirm compliance with PCI DSS and provide evidence of compliance.

US vs. Global Collection or Storage of Information

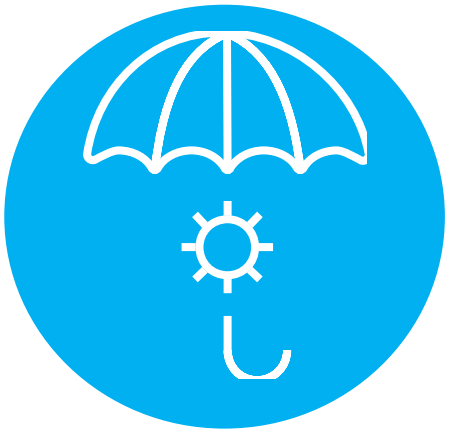
- Does the Company collect, store or use information from individuals outside of the United States or transfers information across international borders?
  - which countries are involved;
  - steps the Company takes to comply with international privacy laws and regulations
  - Where are the Company's servers located?

Security Incidents

- Any privacy or data security incidents (during the prior x year period)?
  - Details
  - Documented Resolution
  - Steps taken to prevent similar incidents.
- Has the Company conducted any reports, evaluations, assessments (including self-assessments), etc. with respect to any privacy or cybersecurity tests or audits (including vulnerability scans or penetration tests), whether conducted internally or by a third-party?
  - Status of any remediation

Certifications and Insurance

- Does the Company have any related certifications (such as SOC 1, SOC 2, ISO).
- Confirm whether the Company has cyber insurance and if amounts are adequate.



Business Continuity and Disaster Recovery

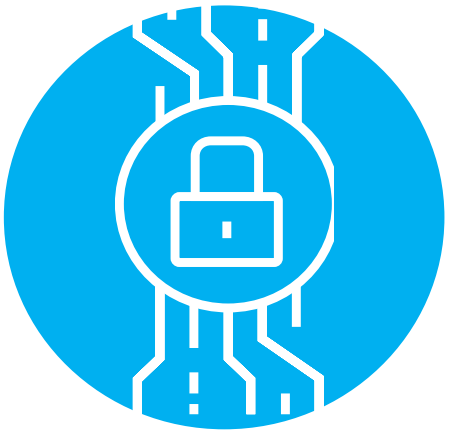
- Does the Company have a business continuity and disaster recovery plan?

Remote Access

- Do employees or contractors of Company use remote access technologies to access PII or other secure information and data?
- Does the company have any remote access policies, including policies such as requirements for multifactor authentication for all remote access to sensitive data and systems.

Policies and Procedures

- Has the Company implemented policies and procedures to protect data (e.g., physical/logical segmentation, user access controls, encryption, separation of duties, third party or internal technologies)?



Training

- Does the Company provide any information security training to employees and/or contractors?

HIPAA?

- Is the Company subject to HIPAA?

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 and/or demonstrate a strategy, particularly on breaches, class actions, and government investigations.
  - Keep / develop logs of any data security breaches, remediation efforts, and steps to prevent breaches 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?

Ezra D. Church

Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

Ezra D. Church focuses his practice on class action lawsuits and complex commercial and product-related litigation, with particular emphasis on the unique issues facing retail, ecommerce, and other consumer-facing companies. Ezra also focuses on privacy and data security matters, and regularly advises and represents clients in connection with these issues. He is co-chair of Morgan Lewis's Class Action Working Group.

Ezra has extensive experience handling complex and unusual class action litigation, and has handled all aspects of such cases from inception through trial and appeal. His work in this area includes defeat of class certification in a rare copyright class action against one of the world's leading publishers, successful opposition of class certification in an unusual defendant class action against many large financial institutions, and a successful defense verdict in a consumer class action trial against an international retailer, including affirmance on appeal. He is an active member of the Firm's Class Action Working Group and regularly writes and speaks on class action issues. He is a contributor to the Firm's chapter on class action litigation in the leading treatise Business and Commercial Litigation in Federal Courts and co-author of a chapter in A Practitioner's Guide to Class Actions, among others.

Doneld G. Shelkey

Boston
+1.617.341.7599
doneld.shelkey@morganlewis.com

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.

Emily R. Lowe

Pittsburgh
+1.412.560.7438
emily.lowe@morganlewis.com

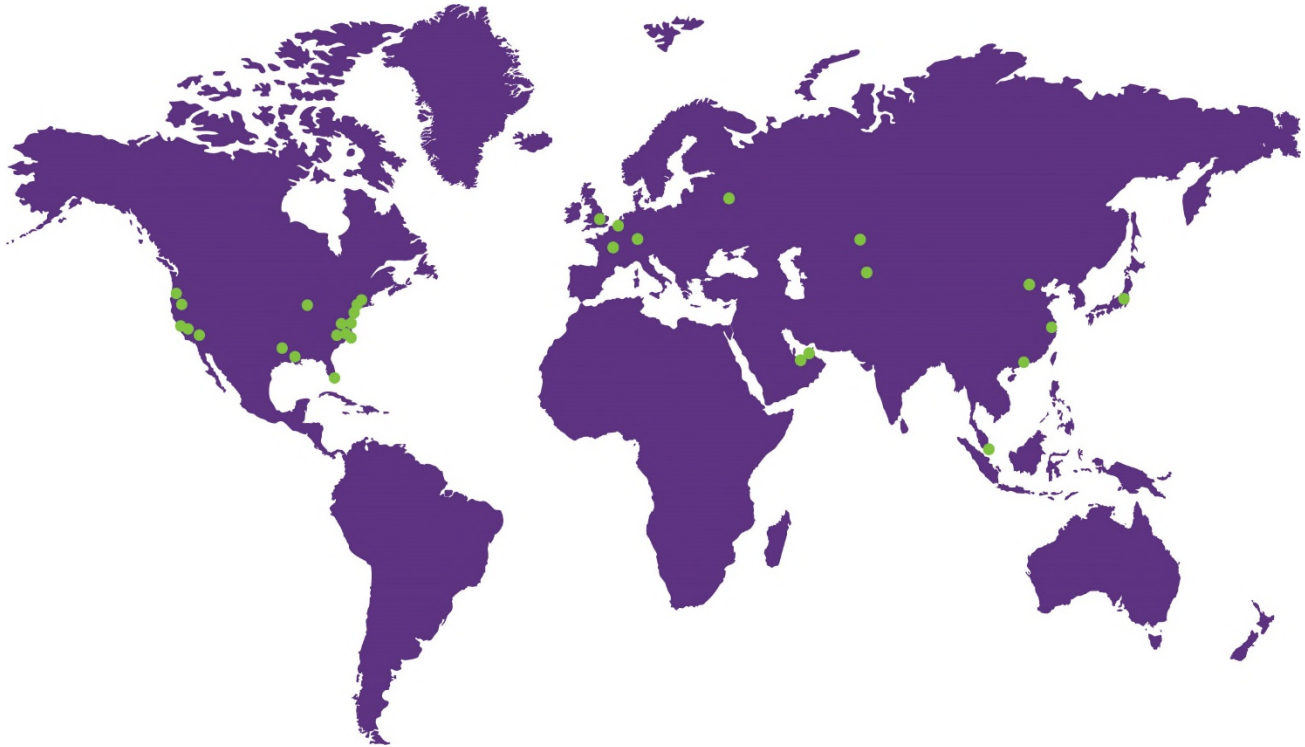
Emily R. Lowe represents clients in commercial transactions, with a focus on the acquisition, use, protection, development, and commercialization of technology and biotechnology. Emily helps domestic and international companies commercialize their products through various commercial vehicles, including manufacturing and supply agreements and distribution strategies, and development and licensing agreements.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*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. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU