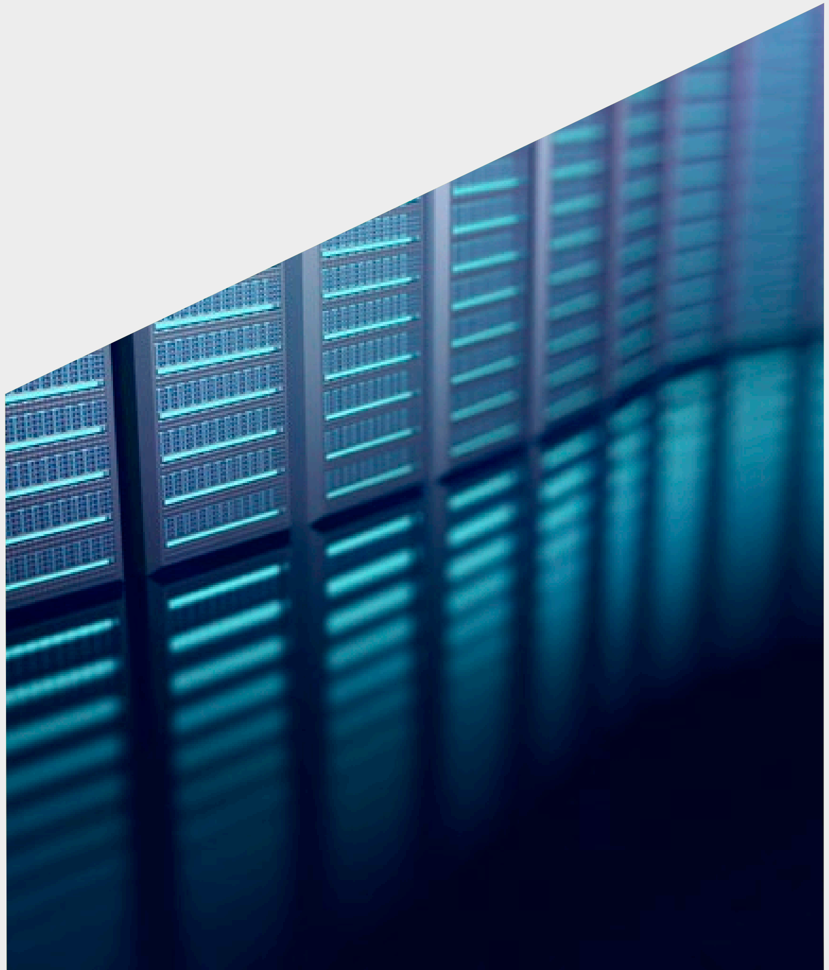
McDermott
Will & Emery

PRIVACY AND CYBERSECURITY CONTRACTING:

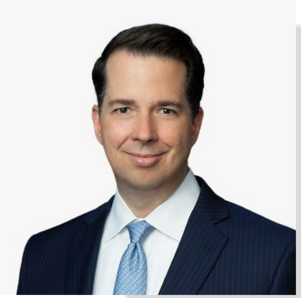
What’s the “Deal”?

June 29, 2022

mwe.com



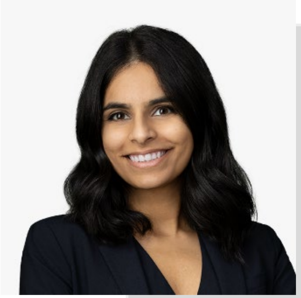
SPEAKERS



TODD MCCLELLAND

Partner,
Atlanta

tmcclelland@mwe.com



SABA BAJWA

Associate,
Los Angeles

sbajwa@mwe.com

BRIAN LONG

Associate,
Dallas

brlong@mwe.com

AUSTIN MOONEY

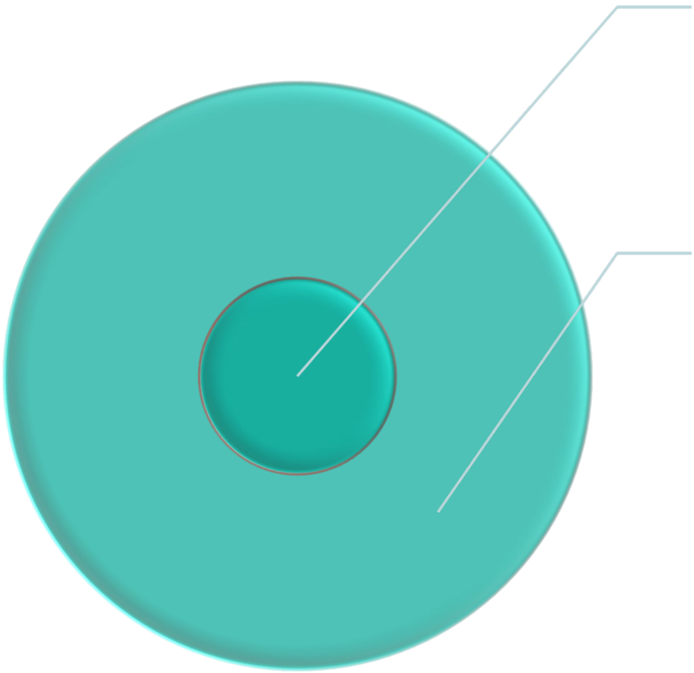
Associate,
Washington, DC

amooney@mwe.com

AGENDA

- B2B Contracting Trends and Considerations
- Privacy Contracting: Sources of Law
  - Controllers vs Processors
  - International Privacy: DPAs and SCCs
  - US State Laws
- DPA Template Creation and Points of Contention
- Common Cybersecurity Contract Terms
  - Liability, Indemnity, and Reps and Warranties
  - Prescriptive security requirements

TREND #1 – CONSIDER ALL COMMERCIAL CONTRACTS, NOT JUST LARGE TECHNOLOGY AND OUTSOURCING ARRANGEMENTS



Technology and Outsourcing

All commercial contracts

- NDA
- M&A
- Manufacturing
- Facilities
- Staff Augmentation
- Government contracts

TREND #2 – THE STANDARD IS NO LONGER THE STANDARD

This is the industry standard

Once size fits all

All other customers agree to this

This is the way it’s done

This is what all our vendors must agree to

These are our standard security requirements

TREND #3 – RISK AND COMPLIANCE-BASED CONTRACT REVIEW

- Must balance the influence of deal value
- May need to think globally
- How does the contract fit into the company's enterprise risk management approach?
- Insurance
- Who "owns" the contract internally
- Consider: Your "compliance" may include compliance with other contracts
  - Contracts on one side (*e.g.*, where you are the vendor) may dictate contract terms on the other side (*e.g.*, where you are the customer)

TREND #4 – PRIVACY AND CYBER RISK GOES BOTH WAYS

- The customer may not be the only party with privacy and cyber risk or compliance obligations
  - Consumer lawsuits against outsourcing vendors
  - Breach notification laws

TREND #5 – CONTRACTS OFTEN INCLUDE MORE PRIVACY AND CYBERSECURITY SPECIFICITY

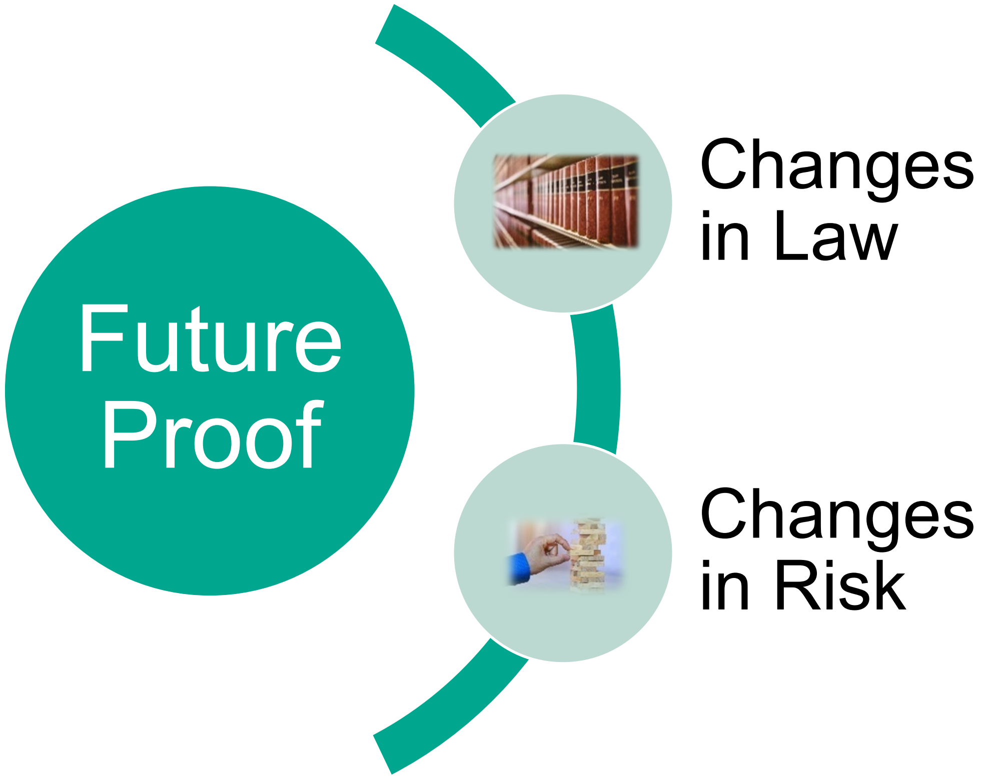
Old:

- Confidentiality and “reasonable” security

New:

- DPA with detailed privacy requirements
- Detailed list of security controls and requirements
- Audit rights / Third party assessments and certifications
- Specific attention in the LoL
- Indemnification
- Breach notification
- Reps and Warranties
- Etc.

TREND #6 – FUTURE PROOF THE CONTRACT



Future Proof

Changes in Law

Changes in Risk

TREND #7 – STRESS TEST THE CONTRACT. WHAT WOULD HAPPEN IF…

This vendor/customer has a data breach?

This vendor's vendor has a data breach?

My vendor's services become unavailable due to a cyber attack?

Our employee had their credentials to our vendor's cloud stolen?

We receive a DSAR request for data hosted by the vendor?

We (as a vendor) have a breach and our customer's consumers bring a class action against us?

My vendor has a breach and they notify my customers, employees or a regulator, without my input or approval?

A cyber attack against my vendor/customer is launched by a foreign government…force majeure?

There is a material change in law that requires changes to my contract?

My customer causes my company to be subject to laws we are not familiar with or able to comply with?

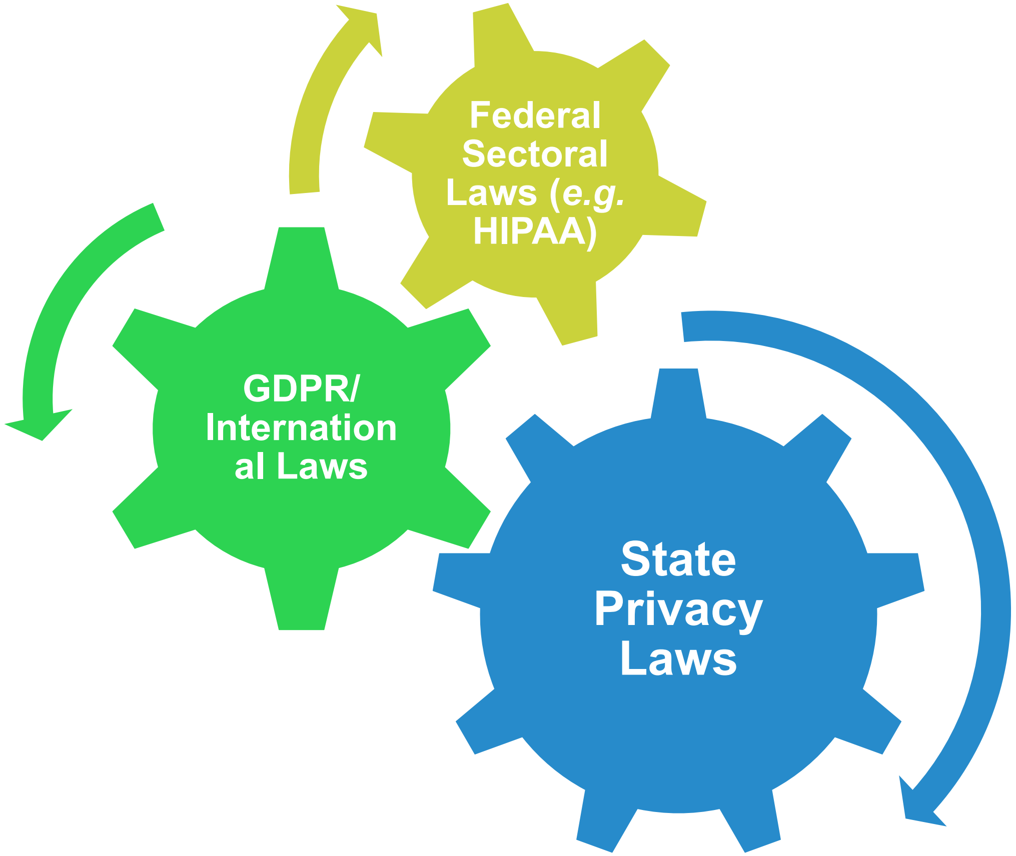
My customer/vendor won't cooperate as they investigate their data breach?

My vendor insists upon being able to anonymize and sell my data?

PART 1

Privacy Contracting – Requirements & Negotiations

PRIMARY SOURCES OF CONTRACTING REQUIREMENTS – PRIVACY



Federal Sectoral Laws (*e.g.* HIPAA)

GDPR/ International Laws

State Privacy Laws

INTERNATIONAL PRIVACY – GDPR

- European Union/EEA privacy law
  - Replaced the Data Protection Directive in 2018 – similar contracting terms
- Wide jurisdictional scope, high fines
- Two types of GDPR contracting requirements:
  - Article 28 Data Processing Addenda (DPAs)
  - Standard Contractual Clauses (SCCs)

CONTROLLERS VS. PROCESSORS

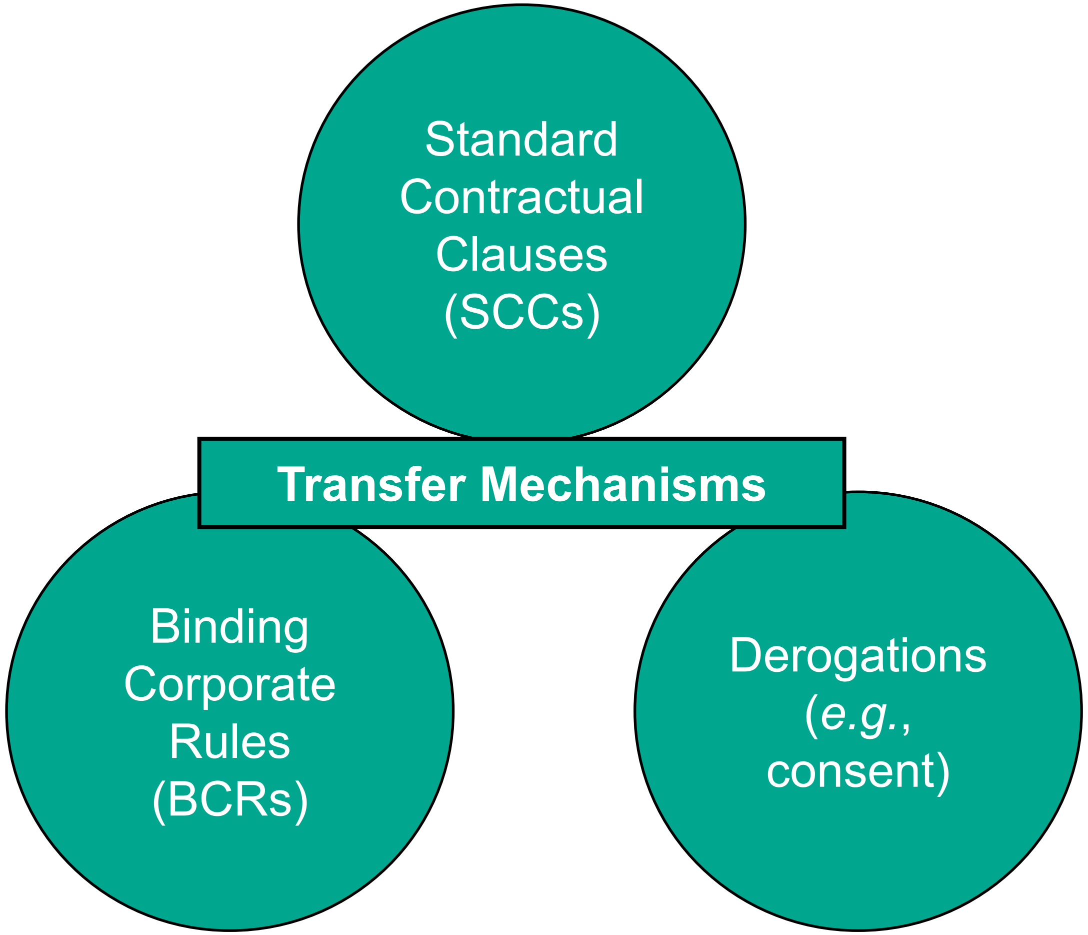
- Controllers: “Determine the purposes and means” of data processing
- Processors: process “on behalf of” controllers
- Processor examples: SaaS providers, consultants/advisors, payment processors
  - Edge cases: Staffing agencies? Facilities service providers?
- Independent Controller Contracting?
  - Not required, but recommended for risk mitigation/data transfers

GDPR ARTICLE 28 DATA PROCESSING ADDENDA

- Implement appropriate technical and organization safeguards
- Processing instructions
- Confidentiality
- Assist controller in achieving compliance with GDPR obligations
- Requirements for deletion and return of personal data
- Audits/inspections
- Subprocessors
  - Authorization
  - Flow down of contract terms
- Processing Annex

CROSS BORDER DATA TRANSFERS

- GDPR restricts transfers out of EEA
  - Need “adequacy decision” or “transfer mechanism”
- Schrems II case – invalidated U.S. Privacy Shield (conditional adequacy decision
  - Privacy Shield replacement pending
  - For now, SCCs are the primary mechanism for most companies
- UK SCCs – New & Old



Transfer Mechanisms

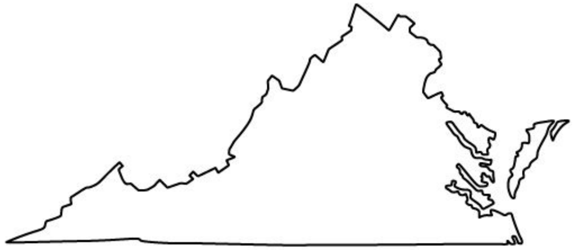
Standard Contractual Clauses (SCCs)

Binding Corporate Rules (BCRs)

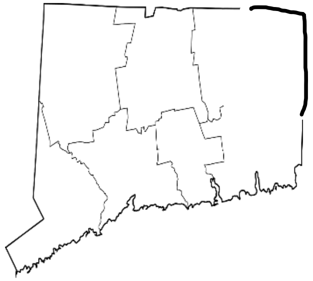
Derogations (*e.g.*, consent)

US STATE LAWS

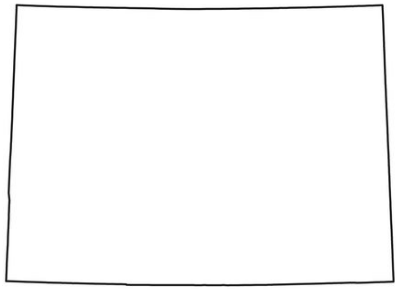
California CCPA
January 1, 2020
CPRA
Amendments
January 1, 2023



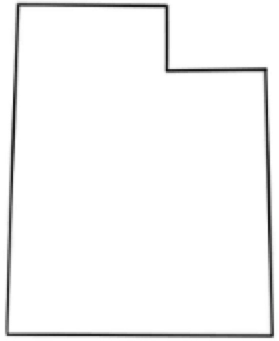
Virginia CDPA
January 1, 2023



Connecticut CPA
January 1, 2023



Colorado CPA
July 1, 2023



Utah CPA
December 1, 2023

CALIFORNIA "SERVICE PROVIDER" CONTRACTS

- **CCPA**
  - "business" vs. "service provider" vs. "**third party**"
  - Contracts include restrictions on:
    - Data "sales"
    - Secondary uses/unrelated commercial purposes
    - Processing data "outside of the business relationship" with customer/business
  - Require "certification" of understanding the contract

- **CPRA** (Effective Jan. 1, 2023)
  - "business" vs. "service provider" vs. "**contractor**"
  - New contract terms (in addition to previous service provider terms):
    - Specified purposes
    - Compliance with law
    - Pass on requirements
    - Audit/Accountability rights
    - Notice of noncompliance and right of remediation
  - **Big Q:** are service provider contracts even required?
  - Contracts are clearly required for data partners: recipients of data "sales" or "shares"

OTHER STATES FOLLOW SUIT

- 2021: VA enacts the Consumer Data Protection Act (CDPA), Colorado enacts Colorado Privacy Act (CPA)
- 2022: Utah and Connecticut
  - All four laws contain contracting requirements similar to GDPR
    - Confidentiality requirement
    - Pass-on terms with notice of new subprocessors
    - Implement reasonable security
    - Processing instructions, anticipated data types and duration of processing
    - Deletion and return of data
    - Audit/accountability

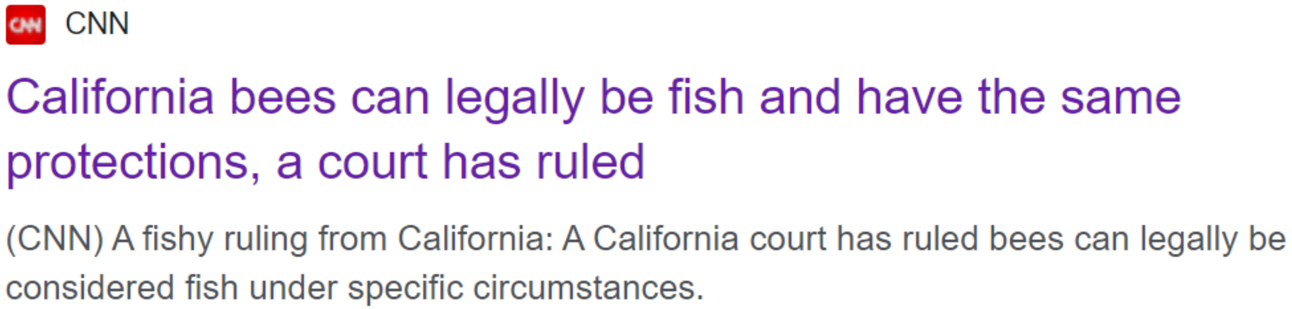
DPA TEMPLATE CREATION

- Managing many jurisdictions: multiple templates or “One Size Fits All?”
  - Depends – customer or vendor?
- Combine privacy with cyber addenda?
- Scope of covered data
- Different templates for different vendors?
- Winning the “Battle of the Forms”
  - Have a playbook ready if not
- Counterparty says “take it or leave it” – find the one or two most important things, work them into whatever document is negotiable

KEY NEGOTIATION POINTS

- Audit rights
- Indemnity, Liability, and Termination
- Open-ended policies/instructions
  - Illusory contract doctrine
- Definitions – watch out for bees!

- Government data requests - commitments to challenge & warrant canaries (Schrems II)
- Subprocessing restrictions/data localization
  - Pass-through terms – verbatim?
- Secondary internal use/improvement
- Compliance with law provisions



CNN

California bees can legally be fish and have the same protections, a court has ruled

(CNN) A fishy ruling from California: A California court has ruled bees can legally be considered fish under specific circumstances.

PART 2

Cybersecurity Contracting Considerations

TYPICAL CONTRACT TERMS WITH CYBER ISSUES

- Limitation on Liability
- Indemnification
- Reps and Warranties
- Compliance with Laws
- Confidentiality
- Breach Notification
- Force Majeure
- Service Levels
- Security Requirements
- Additional Terms to Consider

LIMITATIONS ON LIABILITY (CUSTOMER POSITION)

- Terms:
  - Limitation of consequential and like damages acceptable, subject to certain exclusions.
  - Ordinary damages cap may be acceptable (if reasonably sized and determined), subject to certain exclusions
  - Damages exceptions for (i) breaches of confidentiality; (ii) indemnification obligations; (iii) gross negligence and willful or intentional misconduct; (iv) breaches of cybersecurity, privacy, or data protection obligations, including "notification related costs;" and (v) violation of law

- Rationale:
  - Damages for breaches of confidentiality are typically consequential in nature. Absent this exception, a waiver of consequential damages would leave the customer with no remedy
  - The vendor should have some skin in the game
  - The customer has no way of telling if the vendor is meeting its security commitment
  - The vendor is liable for a data breach only if it has breached the contract. The vendor needs to carefully consider its privacy and security commitment and confirm it is complying with the contract
  - The customer would not enter into this contract if the vendor is not living up to its privacy and cyber commitments

LIMITATIONS ON LIABILITY (VENDOR POSITION)

- Terms:
  - Includes standard limitation on consequential, indirect and other damages
  - Includes a cap on direct damages, possibly based on fees paid for the service/product giving rise to the claim or some amount paid by the customer over a period of time
  - No exclusions from either limitation

- Rationale:
  - Too much exposure could jeopardize the company
  - Cyber and privacy present potentially impossible to quantify risks
  - Incidents may be fault of the customer, especially under a shared security approach. Also, credential stuffing and other attacks may be the customer's fault
  - Vendors may not know what data is being provided to them by their customers
  - The service "is what it is" and the pricing is based on the customer accepting the risk based on the security posture of the vendor's technology and environment
  - The vendor is not insuring against this risk. The customer can procure insurance if it wants additional protection
  - Vendors are unsure of their security posture

LIMITATION ON LIABILITY (NEGOTIATED)

- Solutions:
  - May need to get creative. This is an evolving issue. No such thing here as "standard"
  - Increasingly difficult to get a vendor to take unlimited liability for a data breach, without any fault by the vendor
  - Often see a secondary "super cap" for cyber-related claims
  - Exclusions for breaches of confidentiality will exclude data breaches caused by a malicious third party
  - Often see customer access to vendor cyber liability insurance policies. Loss payee?
  - Before relying on a gross negligence exclusion, know the state law that applies and how it is defined

- Other Thoughts:
  - Breach risk frequently goes both ways – the customer's breach may impact the vendor
  - Increased importance of up-front due diligence and periodic audits
  - Build trust through third party assessments and certifications – give the customer a defensible position.
    - Third party security certifications, assessments, pen test reports, vulnerability scans, risk assessments, etc.
  - Customers may need to better police what data gets sent to vendors
  - Some customer risk may be offset through insurance
  - Consider other rights (*e.g.,* termination) upon a vendor's data breach
  - May need to walk away – including for existing contracts

INDEMNIFICATION

Customer

- Indemnified for any claim or losses arising from data breach, privacy incident, or noncompliance with law or contract

Vendor

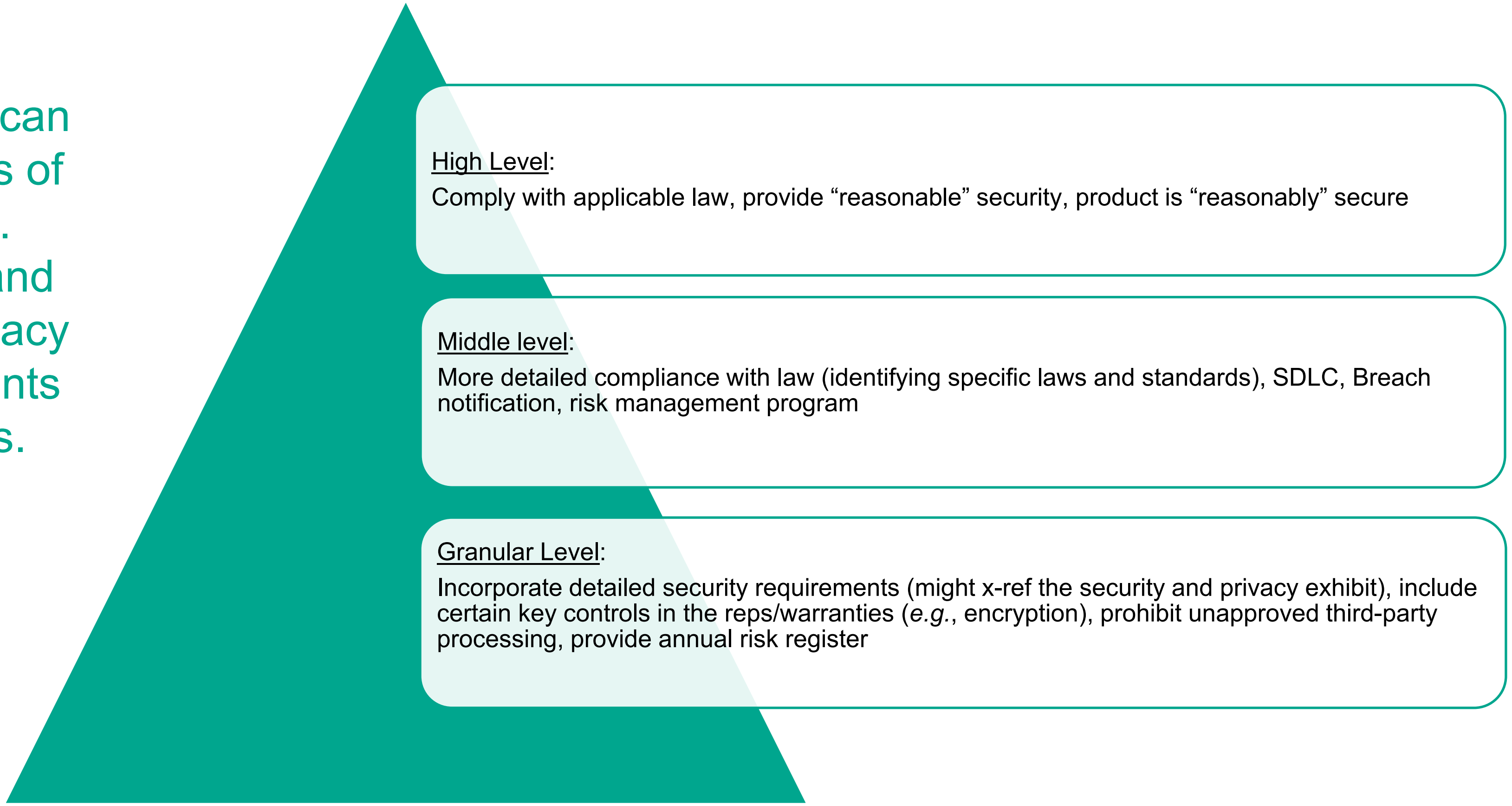
- Limit to third party claims
- Capped
- Clarify that disclosed and permitted data uses are not privacy violations (customer's issue)
- Cover only data breaches that result from a breach of the agreement
- Does not cover any violation of law

Resolution

- Typically limited to third party claims
- Often capped at super cap – tied to discussion of limitation of liability

REPS AND WARRANTIES (CUSTOMER POSITION)

Reps and warranties can be at varying degrees of abstraction / detail. Consider remedies and impact of making privacy and cyber commitments reps and warranties.



High Level:

Comply with applicable law, provide “reasonable” security, product is “reasonably” secure

Middle level:

More detailed compliance with law (identifying specific laws and standards), SDLC, Breach notification, risk management program

Granular Level:

Incorporate detailed security requirements (might x-ref the security and privacy exhibit), include certain key controls in the reps/warranties (*e.g.*, encryption), prohibit unapproved third-party processing, provide annual risk register

REPS AND WARRANTIES (VENDOR POSITION)

- First position: prefer to avoid making reps or warranties regarding privacy or cybersecurity
- If a rep or warranty is necessary, we want to be very precise on exactly what we are committing to. Specify the service, product or environment that is in scope. Everything else is disclaimed
- Structure as warranties only, and not representations
- Varying approaches on cyber:
  - Some vendors will make a general reasonableness rep/warranty
  - Others will rep/warrant only as to their specific security documentation
- Vendors often “water down” the language with terms such as “designed to,” “substantially,” and similar language
- Be careful to carve out any shared or customer responsibilities
- If applicable, consider making the provisions mutual
- Make sure you don’t tie yourself to what could become dated security requirements

REPS AND WARRANTIES (VENDOR POSITION)

- Disclaimer:
  - Basics: OTHER THAN AS PROVIDED IN THIS AGREEMENT, NO EXPRESS WARRANTIES AND NO IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE PROVIDED HEREUNDER
  - Can’t guarantee:
    - Security is sufficient to prevent a data breach
    - Product will not be attacked or compromised
    - Data will not be lost or compromised (at rest or in transit)
  - Not responsible for incidents caused by or attributable to the customer
  - Except as warranted, systems, operations, products, etc. are AS IS

REPS AND WARRANTIES (NEGOTIATED)

- Very unsettled contract provisions. Unlike limitations on liability, there is no true common approach
- Vendors are often not as focused on reps and warranties, and typically are more focused on limitations on liability

SECURITY REQUIREMENTS

Customer

- May require detailed cyber requirements. Detailed requirements can lead to good cybersecurity discussions
- Consider aligning with an industry standard
- Incorporate other standards as appropriate (*e.g.*, OWASP)
- Customer security requirements might pull in applicable legal requirements and standards

Vendor

- Prefer to go with vendor security terms to standardize and ensure the wording is appropriate
- Customer requirements must be carefully reviewed. This is just as much a “legal” document as a “business” document
- Confirm the separation of duties between vendor and customer. Security requirements might pull in services the vendor doesn’t perform or that belong to the customer
- Watch for extra legal provisions (*e.g.*, indemnification)
- Consider whether customer requirements box you in to practices and controls you want the flexibility to change

THANK YOU / QUESTIONS?