KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
DALLAS-FORT WORTH

Annual In-House Symposium

Data in the Cloud: Maintaining Appropriate Contractual Controls in SaaS, IaaS, and PaaS

April 6, 2023

Speakers

Sonia Baldia

Partner
Kilpatrick Townsend

Sonia Baldia brings business and technology savvy to her global practice, which encompasses U.S. and international commercial, transactional, and IP expertise. Sonia advises clients on a wide array of sourcing, technology, and other commercial transactions as well as cloud and digital transformation matters. She is consistently recognized by *Chambers USA*, *Legal 500*, *Best Lawyers*, and other leading publications for her technology, IT and outsourcing expertise.

Jeffrey Connell

Senior Associate
Kilpatrick Townsend

Jeff Connell focuses his practice on data privacy, information technology, business outsourcing agreements, systems integration, software as a service (SaaS) transactions, technology licensing, and other technology and commercial transactions. His pro bono service has been recognized by the *Georgia Bar Journal*, which named him a Pro Bono All-Star, and he was recently recognized by *Best Lawyers, Ones to Watch.*

Agenda

- Overview of the Cloud
- Top Concerns Regarding Data in the Cloud
  - Data Ownership
  - Controls on Data Access/Use
  - Data Location
  - Data Security, Oversight, and Safeguards
  - Indemnities and Liability
  - Data and Vendor Bankruptcy

We will not cover data privacy legal compliance topics in this presentation

KILPATRICK TOWNSEND

Cloud Overview + Top Concerns

ACC Association of Corporate Counsel
DALLAS-FORT WORTH

Cloud Computing vs. Traditional Software Licensing

In a traditional software licensing engagement, the software is installed **on-premise** in the customer's environment.

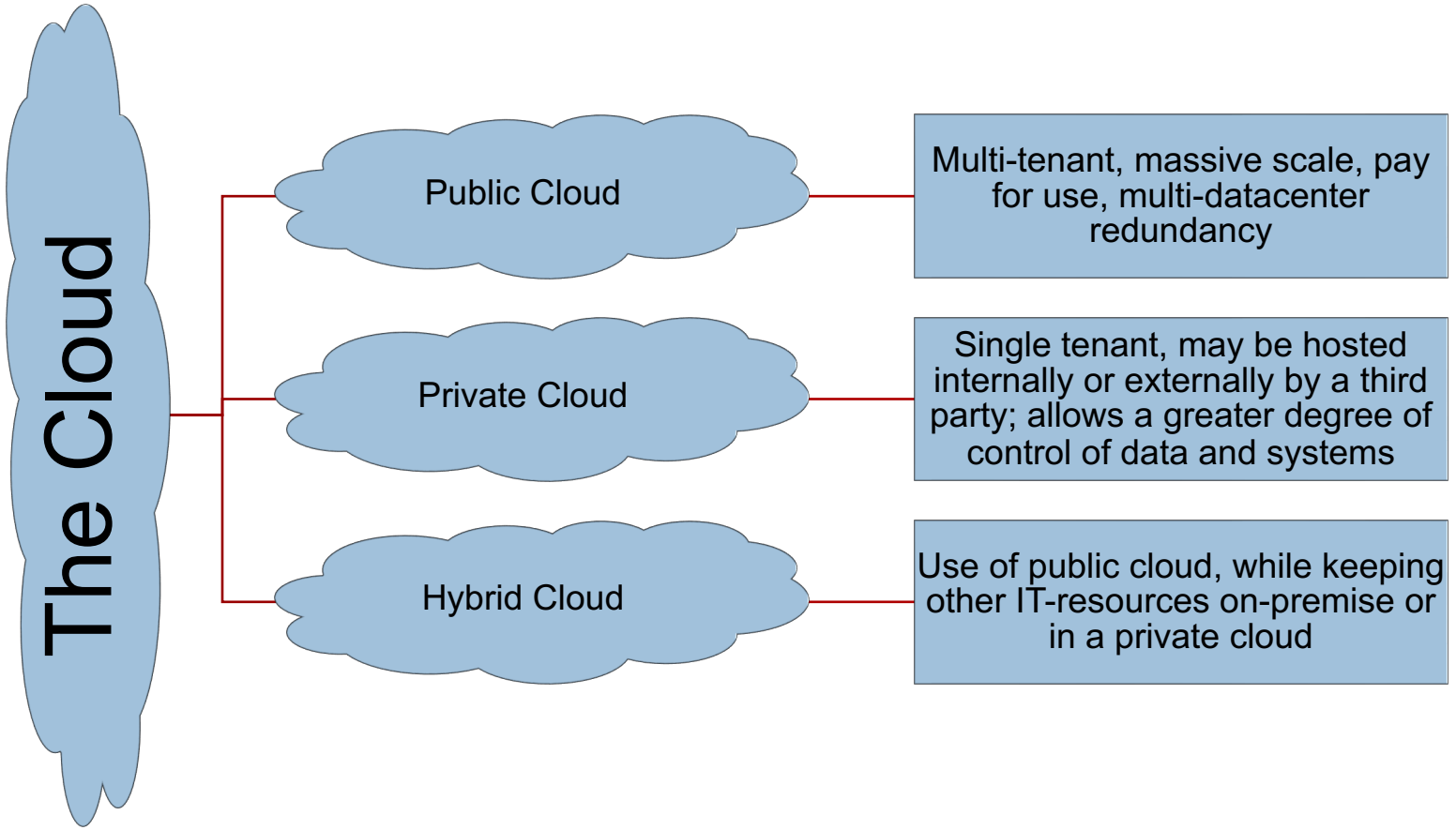
The customer can have the software configured to meet its particular business needs and retains control over its data.

In a cloud computing environment, the software and the customer's data are **hosted by the vendor**, in a private environment, public environment, or hybrid environment.

The software configuration is much more homogeneous across all customers in a "one to many" model.

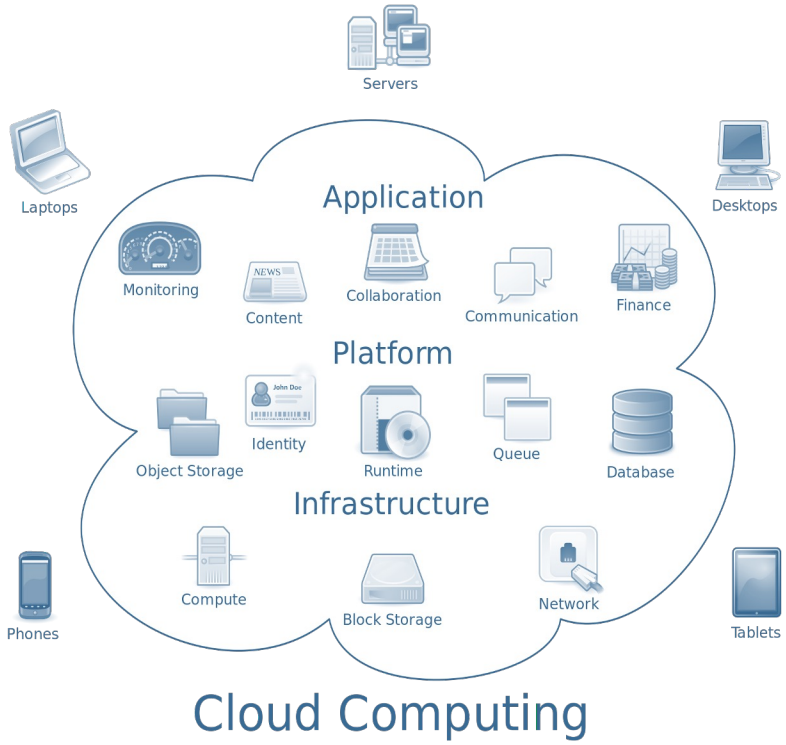
Customer's top priorities shift from customer specific configuration and acceptance to service availability and data security. However, like a traditional software licensing agreement, provisions such as insurance, indemnity, intellectual property, limitations of liability, and warranties remain important.

A Brief Overview of the Cloud



Cloud Delivery Models

SaaS: Software as a Service	PaaS: Platform as a Service	IaaS: Infrastructure as a Service
Consumer uses provider's applications running on provider's cloud infrastructure	Consumer can create custom applications using programming tools supported by the provider and deploy them onto the provider's cloud infrastructure.	Consumer can provision computing resources within provider's infrastructure upon which they can deploy and run arbitrary software, including OS and applications. Allows for dynamic scaling.

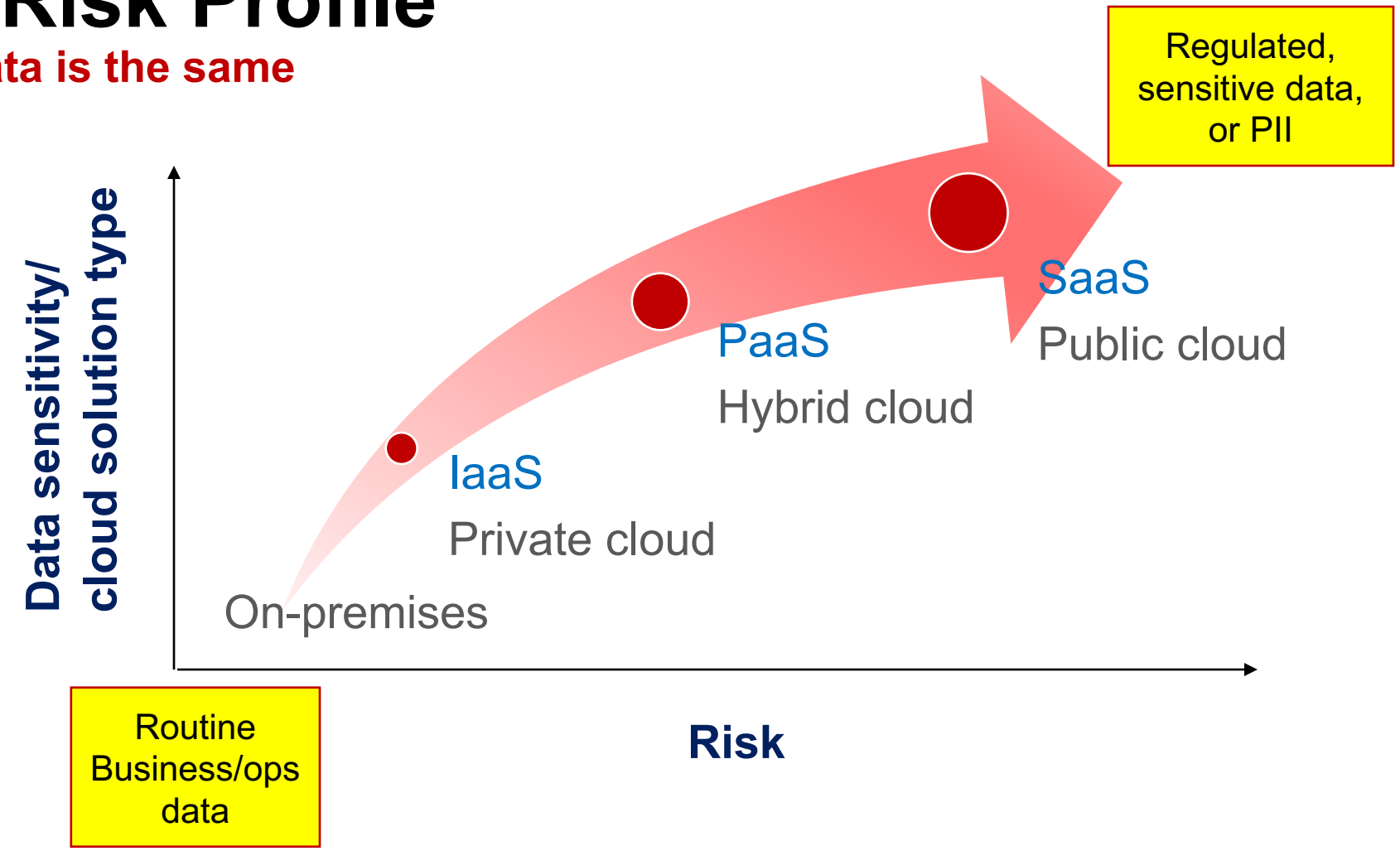


Top Concerns Regarding Data in the Cloud

1. What type of data is uploaded or generated in the cloud?
2. Who owns the data?
3. Is data secure in the cloud?
4. Who can access and use the data?
5. Where will my sensitive or regulated data be stored? Where are the vendor's servers located?
6. Will it be transferred to or accessed from outside the US?
7. Is the Vendor solution compliant with applicable laws and regulations?
8. How to mitigate risk and liability for data breach or non-compliance?
9. What happens to my data if Vendor goes bankrupt?

Data Risk Profile

Not all data is the same

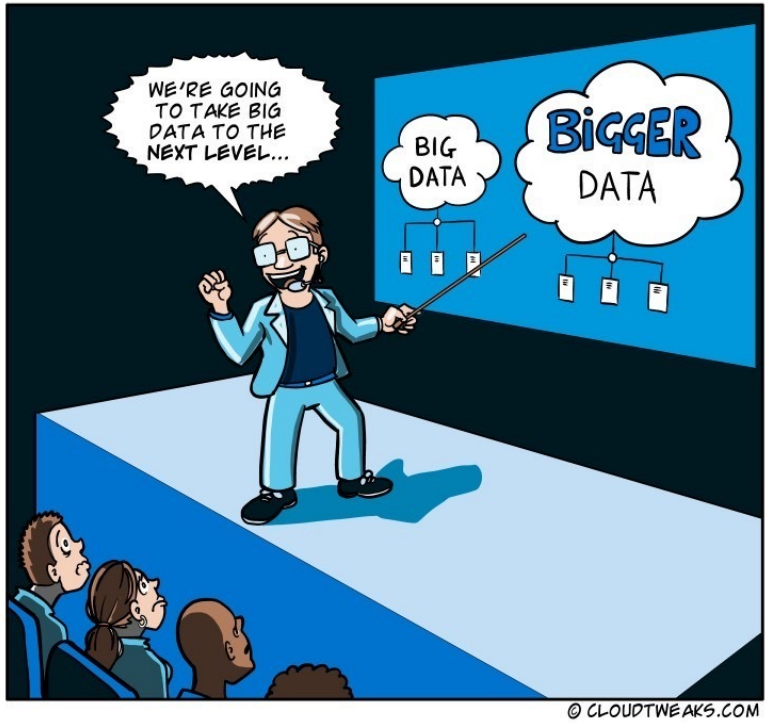


Data Ownership

Data Ownership

Data Ownership

- What is Customer Data and how should it be defined?
- Who retains ownership of the data that is processed, stored, transmitted, and/or created in the cloud solution?
- Does Vendor want to reserve the right to use Customer's data for improving the cloud solution?



Customer Data – Types of Data

Customer Inputs

- Data of Customer and its users submitted or made available to Vendor

Outputs Identifiable to Customer

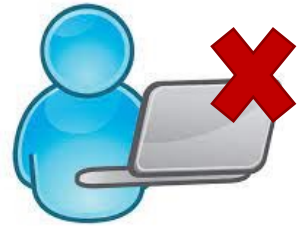
- Original data that has been subject to a modification, enrichment, or other derivation, but from which the original data may be traced
- E.g., certain analytics, insights and reports

Outputs Not Identifiable to Customer

- Aggregated or anonymized data sets where original data is not identifiable
- Data regarding Vendor's network or performance of the solution

Confidential Information

- Extends beyond just "Customer Data" in the solution
- May include confidential business strategy and customer lists; scope should be clearly defined



Data Ownership

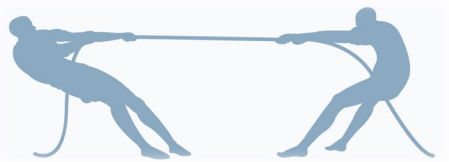
Customer Perspective

From a Customer's perspective, a definition of Customer Data that is too narrow may not capture other data that is derived from the use of the cloud solution but that contains sensitive and critical information.

Vendor Perspective

A Vendor, however, may find it operationally difficult to provide a broad definition of Customer Data. Moreover, a Vendor often relies on data generated in the cloud for its own internal business purposes. Vendors will also want rights to aggregated data (discussed later).

Customer Data



Customer - Own more than just input; own any data generated by use of solution (output).

Vendor - Whatever Customer puts in, Customer owns.

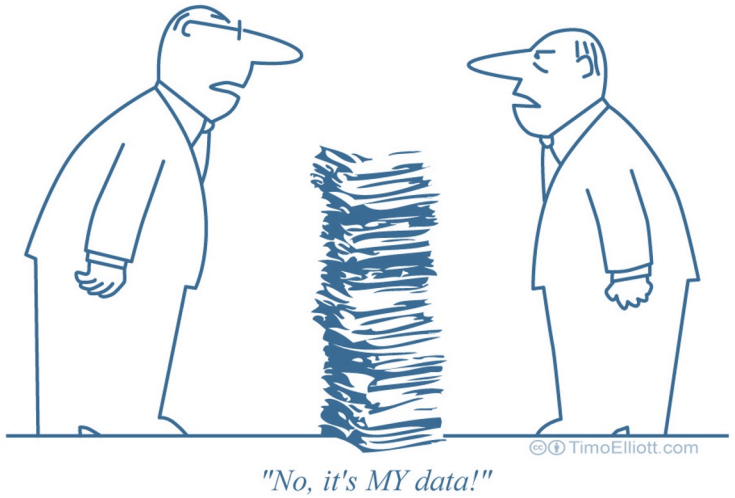
Customer Data Definition

"means all data and/or information provided or submitted by or on behalf of Customer, all data and/or information stored, recorded, processed, created, derived or generated by Vendor as a result of and/or as part of the Service, regardless of whether considered Confidential Information"

"means any data that Customer or its Authorized Users enter into the Service"

Data Ownership ~ Data Control

- Clearly define the types of in-scope data
- Consider different data definitions so that liability/obligation attaches proportionately based on data sensitivity
- Specify the parties' respective ownership rights for each type of data
- If PII is involved, consider the standard of care required for any "highly sensitive" personal data
- Consider Vendor's ownership and use of aggregated data
- Clearly delineate scope of use rights



"No, it's MY data!"

Controls on Data Access/Use

Data Use Rights

- Explicitly identify boundaries on how Vendor can access and use the data.
- Provide for remedies in the event the scope of use is exceeded.
- Approval rights for Vendor affiliates/subcontractors and flow down protections
- Expressly identify use restrictions
- Data Processing Agreement if PII or regulated data is involved
- Access / return / destruction of data

Access and Destruction of Data

- Ensure unfettered access to all data owned.
- Require Vendor to return or destroy any data in its possession at any time promptly upon Customer's request and upon termination for any reason.
- Data may be retained by Vendor in limited circumstances only.
- Length of data retention and protection of retained data

Aggregated Data

- Anonymization, or de-identification, refers to a process that removes information capable of identifying the original owner of the data from collected data.
- Underlying data sets that comprise aggregated data (i.e., personal information, usage metrics).
- Many Vendors have built products and offer solutions to Customers on the assumption that they will have the ability to monetize certain data.
- Giving away rights to aggregated / anonymized data may create certain risks for Customers, particularly with respect to sensitive or industry-specific data.
- In recent years, Vendors are pushing hard to include aggregated data provisions giving ownership / broad license rights to the provider with respect to aggregated / anonymized data.
  - "Baked into the cost."
- CAUTION: Can the data truly be aggregated? Anonymized?
- Any use of aggregated data should ensure that the data can truly be anonymized.

Data Location

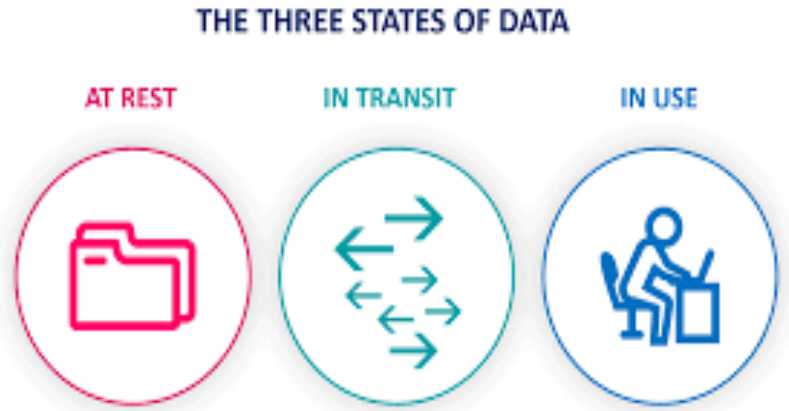
Why does Data Location matter?

- Where is “the cloud”?

- Operational implications
  - Disruption due to natural disaster
  - Data security vulnerability
  - Offshore access by Vendor affiliates/subcontractors
  - Geolocational complexity from implementing multi-vendor platforms

Legal implications

- Cross-border flow of regulated or sensitive data may trigger inadvertent compliance and disclosure obligations:
    - Data sovereignty
    - Data residency
    - Data localization
- Data transfer restrictions may apply (e.g., GDPR)
- Export control/OFAC considerations



Mitigate location risk

1. Understand Vendor cloud solution (including security measures and policies) relative to three states of data
2. Require onshore data residency for regulated or sensitive data
3. Monitor, limit or restrict offshore access by Vendor affiliates/subs
4. Any changes to location must be subject to robust change control process
5. Vendor to promptly notify prior to compelled disclosure to government entity with jurisdiction over data
6. Vendor to comply with all applicable laws and regulations relative to its solution, services and data processing (e.g., GLBA, HIPPA, CCPA, GDPR, Export Control, OFAC)
7. Conduct periodic audits to ensure compliance and impose heavy penalty for breach

Sample Clauses

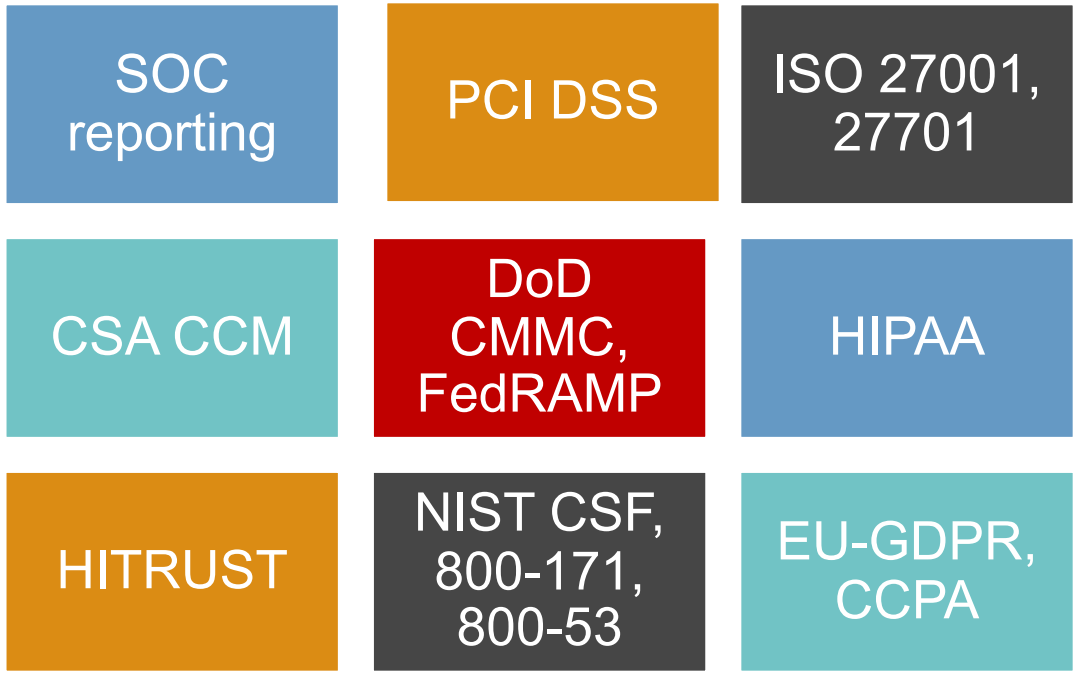
- Supplier shall provide the Solution and Services, including any processing of Customer Data, from the hosting facility set forth in the Order Document (the "Hosting Site"). Supplier will maintain and enforce at the Hosting Site safety and physical security procedures that are at least (i) equal to industry standards for such types of service locations, and (ii) as rigorous as those procedures in effect at the Hosting Site as of the Effective Date. In no event shall Supplier transfer any Customer Data to any location outside the United States. Supplier shall not and shall not permit any Supplier Personnel to perform the Services from a location outside of the United States, except as expressly agreed by Customer in writing. Supplier shall remain fully liable and responsible for the performance of all Services performed by non-U.S. operations hereunder.
- Supplier shall provide the Solution and Services in compliance with all applicable Laws. Use of the Solution and Services, including processing of Customer Data, as intended shall not cause Customer and its Authorized Users to be in violation of any applicable Laws. Supplier shall promptly identify and notify Customer of any changes in applicable Laws that relate to Supplier's performance, and/or Customer's receipt or use, of the Solution and Services.
- Supplier shall comply with all U.S. or other export control Laws (the "Control Laws") applicable to any Solution, Deliverables or technology provided or disclosed in connection with any Services, including any restrictions on the exposure or release of technical data, software source code or other information ("Information") to any unauthorized Supplier Personnel. Each Party shall implement and maintain appropriate technology control programs and procedures compliant with the Control Laws to prevent the unauthorized exposure or release of such Information. In addition, Control Laws prohibit certain transactions with certain countries ("Restricted Countries") or with persons and entities designated on government restricted parties' lists ("Restricted Parties"). Supplier agrees that it shall not export, re-export, transfer, or release any Customer Information to Restricted Countries or nationals thereof, or to Restricted Parties.

Data Security, Oversight and Safeguards

Vendor Security Diligence

1. What technical measures will Vendor implement to safeguard Customer Data?
2. Will Vendor conduct background checks on staff who get data access?
3. How will data security incidents be handled?
4. What audit rights will Customer have?
5. Will Vendor provide annual SOC 1/2 or ISO 27001 data security audits?
6. Does Vendor solution comply with applicable data security laws applicable to regulated data (GDPR, HIPPA, GLBA, State security laws, others)?
7. Will vendor use sub-processors?
8. Engage with Infosec team upfront to conduct Vendor security and risk assessment

Industry Certifications and Audit Controls



- Customers frequently require compliance with certain industry standards.
- Ensure that the scope of the applicable standards aligns with the use case (business, processes, functions)
- Annual certifications vs. audit rights
- Audit Frequency
- Period that may be audited
- Auditors

Contractual Checklist

- Outline permitted and prohibited uses
- Robust confidentiality provisions – data as “confidential information”
- Limit Vendor’s ability to subcontract without consent and, if approved, require flow downs
- Obligate Vendor to implement robust data security protocols
- Data breach notification and response plan
- Data backups
- Data migration and transition
- Return / destruction of data

Customer Perspective

A Customer wants to ensure Vendor safeguards for security and confidentiality of Customer Data are critical in any cloud contract. Vendor should deliver details regarding, and agree to reasonable provisions addressing, its competency and its policies and procedures related to protection against security vulnerabilities, data backups, the use of Customer Data, and data conversion.

Vendor Perspective

A Vendor should be responsible solely for their actions. In other words, it is important to exclude any third-party actions over which Vendor has no control, such as a malicious hacker. A Vendor will agree to reasonable controls commensurate with the data it agrees to handle. Moreover, it is necessary to cap liability at an amount that reflects a Vendor's risk to reward.

Data Breaches

Customer - A Vendor should have strict liability for data breaches.

Vendor - A Vendor shouldn't be used an insurance policy against any data breach.

Data Security

Common Landing Spot

- Robust security programs are the first line of defense.
- Security incident notification without undue delay
- To the extent a Vendor employee absconds with data, that's covered under "intentional torts." But a Vendor's responsibilities are primarily contained within maintaining its security program.

Practice Pointers

- Be aware of Customer specific obligations that may be used to limit/reduce Vendor liability (i.e., encryption).
- Have a breach response in place.
- Limit data access locations (U.S. vs foreign).

Sample Clause

- Audit Rights. During the Term and for a period of two (2) years thereafter, Customer shall have the right, at its expense, either directly or through an independent accounting firm, to audit Supplier's (a) books and records for the purpose of verifying all amounts payable to or charged by Supplier, (b) performance of the Services and satisfaction of the Service Levels, and (c) compliance with this Agreement and applicable Laws (an "Audit"). Audits shall take place during Supplier's normal business hours and shall be conducted in a manner that does not unreasonably interfere with Supplier's normal business operations. If any Audit conducted pursuant to this Section xx uncovers any overcharge by Supplier or any failure by Supplier to comply with this Agreement or applicable Laws, Supplier shall promptly refund to Customer the amount of such overcharge and correct such non-compliance with this Agreement or applicable Laws.

Sample Clause

- Self-Testing and SOC 2 Type II Report. Once per calendar year, Supplier shall engage, at its cost and expense, a nationally recognized accounting firm to conduct a SOC 2 Type II audit report ("Security Audit"). Each Security Audit shall cover, at a minimum, all security policies and procedures and controls of Supplier and Supplier Agents, including system security, administrative security, and physical security. Supplier shall provide Customer with a copy of the Security Audit promptly upon receipt by Supplier. If (a) the Security Audit in its final and issued version contains a qualified opinion relating to security matters including risks to Supplier's and Supplier Agents' solution, networks or physical facilities which could result in the unauthorized destruction, loss, alteration of or access to Customer Data, or the Services being provided to Customer being adversely affected, or (b) there are any deficiencies, weaknesses, concerns or recommendations arising out of any Security Audit, then (i) Supplier shall promptly meet with Customer to discuss the audit report, and (ii) Supplier shall, at its own expense, promptly correct the deficiencies and/or weaknesses giving rise to the qualified opinion, and (iii) Supplier shall, at its own expense, promptly address all other deficiencies, weaknesses, concerns, and recommendations arising out of the Security Audit. If Supplier fails to take the remedial actions set forth in the foregoing clauses (i), (ii), and (iii) within one day, three days, or ten days (respectively) after the date Customer raises security concerns, Customer may elect to immediately terminate this Agreement, in whole or part, without regard to any cure period by providing written notice to Supplier.


KILPATRICK
TOWNSEND

Indemnity


ACC
Association of
Corporate Counsel
DALLAS-FORT WORTH

Indemnity for data-related violations

- Scope/Triggers

1. Vendor's failure to comply with data security obligations
2. Violation of applicable laws, including privacy laws
3. Customer supplied data
4. Gross negligence or willful misconduct
5. Breach of confidentiality obligations
6. Claims by Vendor's third parties/data/tools
7. IP infringement

- Third party vs. first party claims
- Unlimited vs. super cap
- Who controls defense?
- Enabling Clause

Indemnity Enabling Clause

“Defend and pay”	The duty to defend and pay only requires the indemnitor to pay for defense costs and any resulting judgments awarded to a third party or settlements.
Full indemnity (i.e., “defend, indemnify, and hold harmless”)	Generally, a full indemnity is intended to broadly make the indemnitee whole; covers more damages than payment of judgments or settlements.

Customer Perspective

1. Customer seeks an enabling clause that includes a **full indemnity** (i.e., “defend, indemnify, and hold harmless”).
2. Customer will want to ensure that it is able to recover for **first party damages** in addition to third party damages.
3. Customer will include a **series of indemnity events**, including for confidentiality, privacy, non-infringement, personal injury and property damage, violation of law, and gross negligence.

Vendor Perspective

1. A Vendor seeks to limit indemnity obligations to “**defend and pay**” so that the Vendor is only responsible for amounts finally awarded by a court with the obligation only triggered by third party claims.
2. A Vendor seeks to limit its indemnity obligations to a **narrow list of trigger events**, such non-infringement and will include exclusions.

Indemnities

Common Landing Spot

- Indemnities are typically limited to **3rd party claims**, although full indemnity vs. defend and pay is still somewhat of a toss-up.
- Depending on Vendor's risk tolerance, Vendor may offer **IP-infringement** at a minimum, but other triggers may include:
  - **Gross negligence or willful misconduct**
  - breach of **confidentiality** and **data security obligations**, if tied to a SuperCap (*more on this later*)
  - **Violation of applicable laws** (may be tied to a SuperCap)

Practice Pointers

- Even though an indemnity may be triggered by 3rd party claims, a **broad definition of "Losses"** can include first party damages.
- Substantial super cap for indemnity if Vendor push back on uncapped indemnity
- Watch out for **exclusions to certain indemnities** that could undo protection (such as integration with 3rd party systems or Customer's provision of "unclean" data).

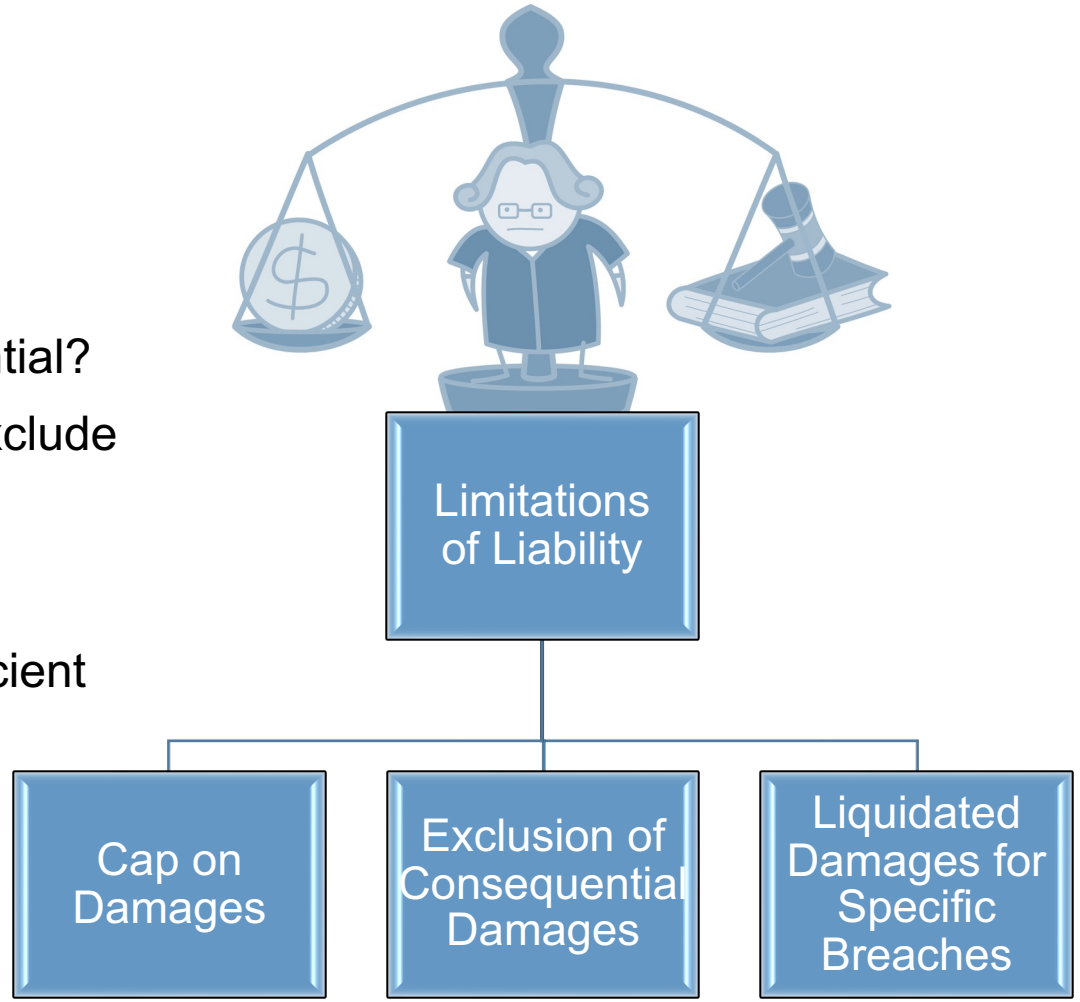

KILPATRICK
TOWNSEND

Liability


ACC
Association of
Corporate Counsel
DALLAS-FORT WORTH

Limitation of Liability

- Types of Damages
  - Direct vs Consequential
- Consequential Damages Waiver
  - Are potential damages more likely direct or consequential?
  - Does prohibiting consequential damages effectively exclude ability to recover meaningful damages?
- Cap on liability
  - Aggregate Cap vs. Per Order / SOW vs. Fees for Deficient Services
  - Super Cap for certain exclusions



Unlimited Liability or Super Cap?

- Exclusions/carve-outs based on cause of damage
  - Breach of confidentiality
  - Breach of data security obligations – could be super cap
  - Indemnity for data security breach – could be super cap
  - Violation of privacy laws – could be super cap
  - Gross negligence and willful misconduct
- Consider defining acknowledged direct damages to include data breach notification, investigation and remediation costs

Customer Perspective

A Customer wants to maximize potential for recovery of damages and, therefore, include **all amounts paid or payable** into the calculation – whether or not under the same order/SOW – **and a dollar amount floor**.

Exclusions should be applied to **both** the **damages cap** and the **consequential damages waiver**.

Vendor Perspective

A Vendor will attempt to limit the overall damages cap as much as possible, often times through **services-specific caps**.

Vendors want to limit exclusions from the limitations of liability – the "*not an insurance provider*" argument exclusions.

Vendors may start with limited exclusions (such for IP infringement indemnity and bad acts (fraud/gross negligence), but will attempt to only carve out from the damages cap.

Exclusions

Customer - Capture the losses that may happen from an economic perspective

Vendor - Consequential damages should be excluded

Damages Cap

Customer - Aggregate fees paid or payable; Dollar amount floor

Vendor - Limited to amount of fees paid for the services under a particular order OR fees for the deficient services; No dollar amount floor

Limitation of Liability

Common Landing Spot

- Damages caps are often set at 12-18 months fees.
- Full exclusions from limitations of liability are negotiable and vary by Vendor tolerance.
- Super Caps for certain breaches such as data security are now market and vary drastically in amounts (i.e., a set amount, or 2x or 3x the general cap).

Practice Pointers

- Do carve-outs apply to both the damages cap and the consequential waiver?
- What are “direct damages”? Consider including a definition for acknowledged direct damages.
- Is it clear that amounts paid under a carve-out or super cap do not erode the general damages cap?

Sample Clauses

- Damages Cap. Each party's liability for all claims arising out of or relating to this Agreement, whether in contract, tort or otherwise, will not exceed an amount equal to the greater of: (a) the Fees payable by Customer to Supplier during the twenty four (24) month period immediately preceding the date of the event or occurrence giving rights to the applicable action or claim (or if twenty four (24) months have not elapsed since the Effective Date, twenty four (24) times the average monthly Fees payable by Customer) and (b) [$XXXXXXXXX] .

- Each party's liability to the other for all claims arising out of or relating to this Agreement, whether in contract, tort or otherwise, will not exceed the fees paid by Subscriber to the Service Provider under the relevant order form or Statement of Work for the twelve (12) months immediately preceding the first event that gave rise to the liability.

Sample Clause

- Exclusions. Notwithstanding anything to the contrary contained herein, the limitations on amounts and types of damages set forth in Section xx and Section xx shall not apply to:
  - (a) accrued but unpaid credits and amounts due and payable to Customer by Supplier under this Agreement (including SLA Credits);
  - (b) indemnification obligations of Supplier hereunder;
  - (c) Losses resulting from a breach by Supplier of Section xx (Laws and Regulations);
  - (d) Losses resulting from a breach by Supplier of its obligations to obtain, maintain or comply with Section xx (Consents and Governmental Approvals);
  - (e) Losses resulting from a breach by Supplier or Supplier Agents of Section xx (Confidentially Information and Data Security);
  - (f) Losses resulting from a breach by Supplier of Section xx (Disaster Recovery);
  - (g) Losses resulting from a breach by Supplier of Section xx (Termination Assistance) or Section xx (Abandonment);
  - (h) Losses resulting from personal injury or property damage caused by the acts or omissions of Supplier and Supplier Agents; and
  - (i) Losses resulting from fraud, gross negligence or willful misconduct by Supplier or Supplier Agents (or, for clarity, its agents, subcontractors and representatives).

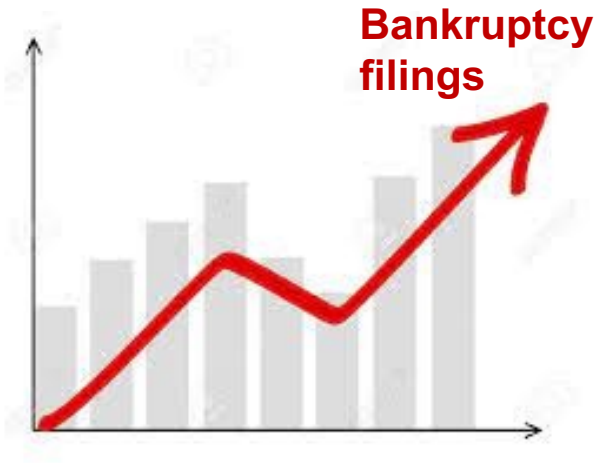
KILPATRICK TOWNSEND

Data and Vendor Bankruptcy

ACC Association of Corporate Counsel
DALLAS-FORT WORTH

Where is my data?

- You may not be able to get your data back if the cloud provider files for bankruptcy or shuts down business
- Risk mitigation:
  1. Upfront Vendor due diligence is critical
  2. Consider hosting most critical data on-premises or replicate critical data elsewhere
  3. Clearly articulate your ownership of all data
  4. Provider to acknowledge that such data will not be considered part of its bankruptcy estate
  5. Provider to notify you immediately of any determination to file for bankruptcy and return data
  6. Require right to immediate access to your data upon bankruptcy filing
  7. Periodic financial reporting by provider



Questions?

Sonia Baldia

Partner
Kilpatrick Townsend

+1 202.508.5840

sbaldia@kilpatricktownsend.com

Jeffrey Connell

Senior Associate
Kilpatrick Townsend

+1 404.541.6822

Jeff.Connell@kilpatricktownsend.com

Locations

Counsel to innovative companies and brands around the world

We help leaders create, expand, and protect the value of their companies and most prized assets by bringing an equal balance of business acumen, technical skill, and creative thinking to the opportunities and challenges they face.

Anchorage
Atlanta
Augusta
Beijing
Charlotte
Chicago
Dallas
Denver
Houston
Los Angeles
New York
Phoenix
Raleigh
San Diego
San Francisco
Seattle
Shanghai
Silicon Valley
Stockholm
Tokyo
Walnut Creek
Washington DC
Winston-Salem