Association of Corporate Counsel
NATIONAL CAPITAL REGION

ACC NCR FALL CONFERENCE

Advanced Topics for In-House Attorneys

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

KILPATRICK TOWNSEND

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

cvent

Advanced Topics for In-House Attorneys

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

Presented September 14, 2022

Speakers

Sonia Baldia

Partner
Kilpatrick Townsend

Edwin Szeto

VP & Deputy GC
Cvent, Inc.

Jeffrey Connell

Associate
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. She has been recognized by *Chambers USA*, *Legal 500*, and other leading publications for her technology and outsourcing expertise, including deals involving India. She is a frequent speaker and writer on global sourcing, digital transformation, IP, and technology topics.

Ed Szeto has over twenty years of technology contracts experience. As Vice President & Deputy General Counsel for Cvent, Inc., a leading SaaS provider of technology and services to the events and meetings industries, Ed leads the commercial legal team and is responsible for all contractual matters with Cvent customers and vendors. Prior to joining Cvent, Ed spent ten years with MICROS Systems, Inc., a provider of technology products to the hospitality and retail industries, until its acquisition by Oracle.

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
- Data Location
- Data Security, Oversight, and Safeguards
- Data Controls
- Liability / Risk Management

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.

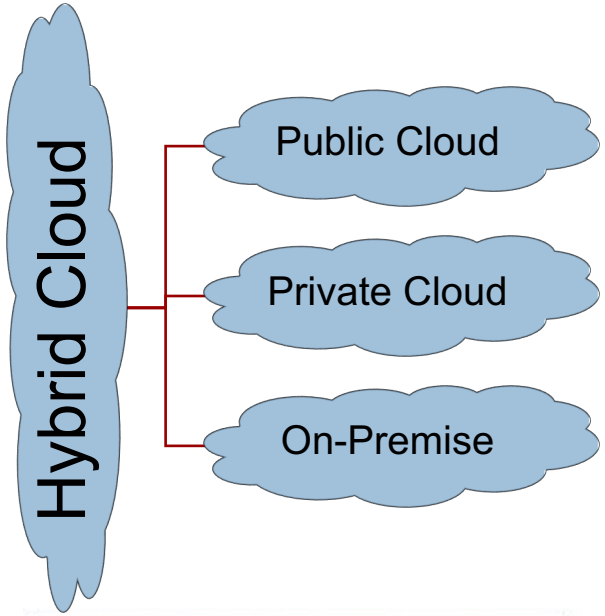
In a cloud computing environment, the software and the customer's data are **hosted by the vendor**, in a private environment, public environment, or hybrid environment.

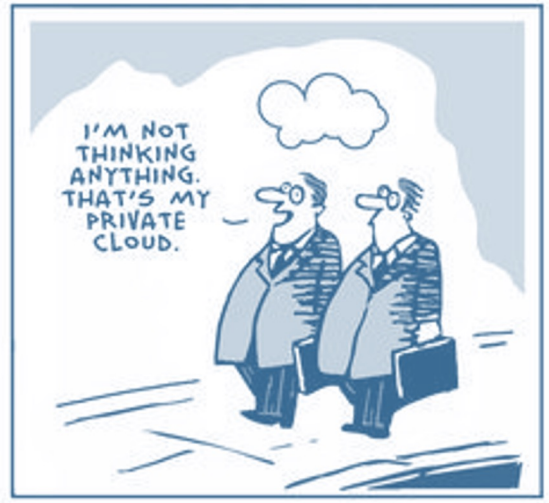
The software configuration is much more homogeneous across all customers in a "one to many" model.

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

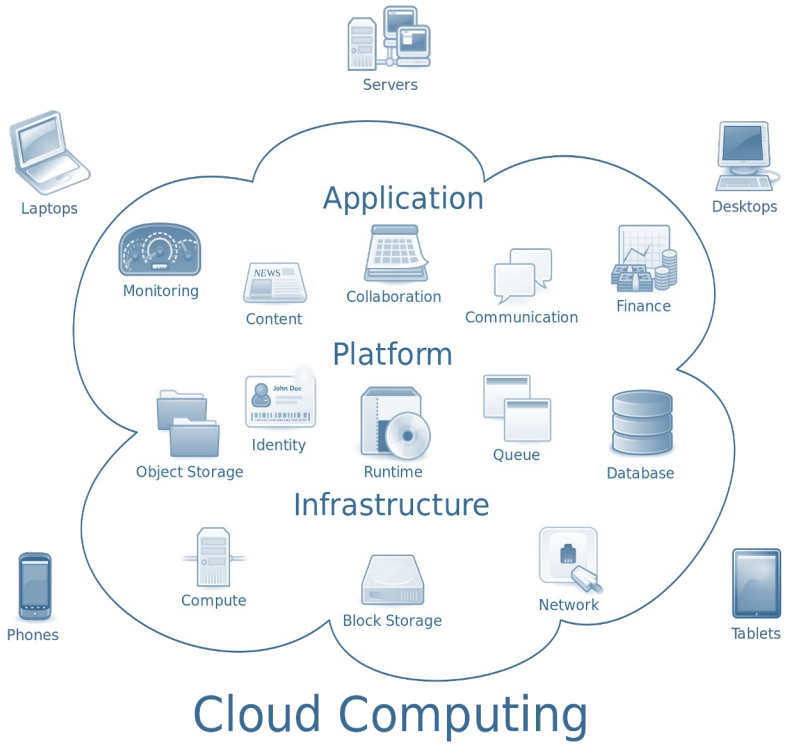
- Public Cloud
  - Multi-tenant, massive scale, pay for use, multi-datacenter redundancy
- Private Cloud
  - Single tenant, may be hosted internally or externally by a third party; allows a greater degree of control of data and systems
- Hybrid Cloud
  - Use of public cloud, while keeping other IT-resources on-premise or in a private 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.
Google Docs, Google Gmail, Salesforce CRM, Facebook, Groupon, Oracle	AWS, Microsoft Azure, Spring Source, Google Cloud	AWS, Google Cloud, RackSpace, IBM, VMware



Top Concerns Relating to Data in the Cloud

Data Ownership	Different elements of data; who retains ownership and may use it freely; aggregated data
Data Location	Data localization; onshore / offshore locations; regulated data; data transfer restrictions; DPAs
Data Security / Oversight / Safeguards	Security audits; certifications, SOC reports; data breach notification and remediation; security/privacy compliance; vendor due diligence; data privacy and security risk assessments
Data Controls	(Access/disclosure/use) – who has access to data; usage right; aggregated data; subcontractors or subprocessors; consents; data return; destruction; data retention; DPAs
Liability / Risk Mitigation	Representations, Warranties, Indemnity, Limitation of Liability, Insurance, Termination

Data Ownership

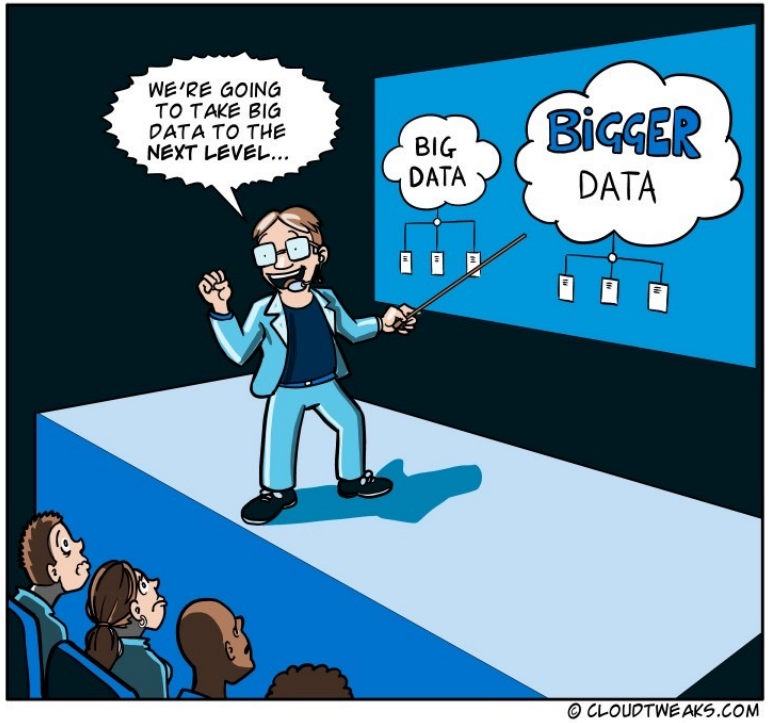
cvent

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

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 with the cloud solution?
- Does Vendor want to reserve the right to use Customer's data for purposes of operating and improving the cloud solution?



Customer Data – Types of Data

Customer Input

- Data of customer and its users submitted or made available to the vendor

Derived Data Identifiable to Customer

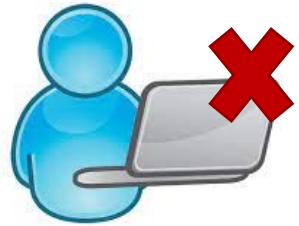
- Original data that has been subject to a modification, enhancement, or other derivation, but from which the original data may be traced
- E.g., certain analytics, insights and reports

Derived Data Not Identifiable to Customer

- Aggregated or anonymized data sets where the original data is not identifiable
- Data regarding the 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

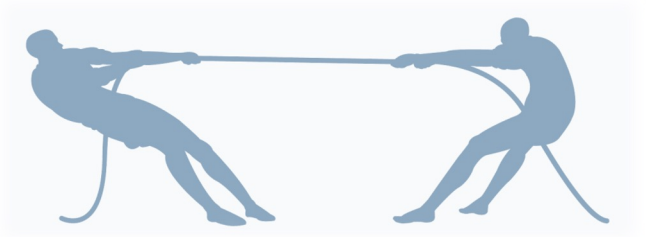


Aggregated Data

- 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 service providers have built products and offer solutions to customers on the assumption that they will have the ability to monetize certain data.
- Caution: data can often be re-identified.

Customer Perspective

Data Ownership



From 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.

Customer Data

Own more than just input; own any data generated by use and output.

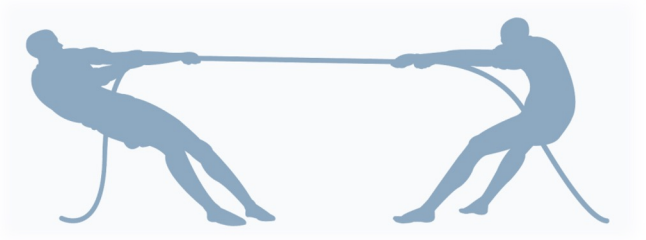
Customer Data Definition

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

"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"

Vendor Perspective

Data Ownership



A Vendor, however, may find it operationally difficult to provide a broad definition of Customer Data. Moreover, a Vendor often relies on data generated within the cloud solution for its own internal business purposes.

Customer Data

Whatever Customer puts in, Customer owns.

Aggregated Data

Include aggregated data provisions giving ownership/broad license rights to Vendor with respect to aggregated/anonymized data.

✓ "Baked into the cost"

Data Ownership – Practice Pointers

- Clearly define the types of in-scope data.
- Consider whether the data identifies Customer, can be used to identify Customer, or if it is capable of being re-identified.
- Specify the parties' respective ownership rights for each type of data.

KILPATRICK TOWNSEND

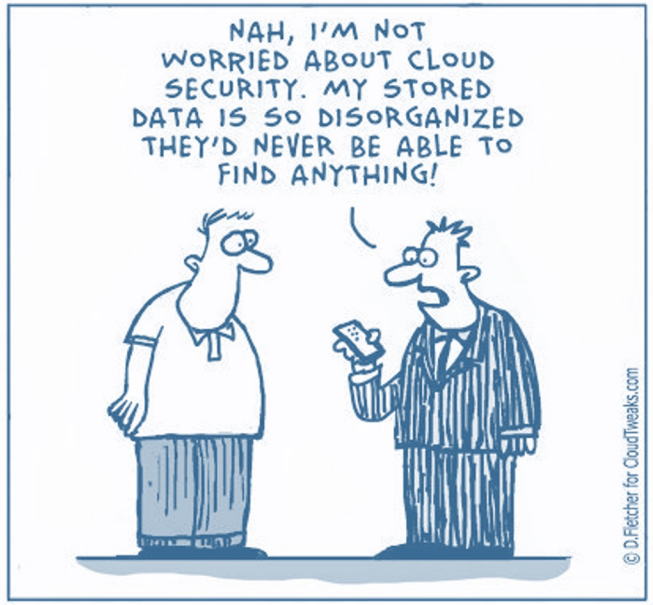
cvent

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Data Location

Compliance

- Always ensure compliance with applicable law (i.e., HIPPA, GLBA).
- Determine if customer policies, vendor policies, or both are appropriate.



Data Location Issues

- Data transfer (EU and similar jurisdictions)
- Location of users accessing data
- Movement and storage of data
- Location of subcontractors accessing data
- Use of multiple platforms
- Data breach
- Data destruction
- Ability to impose security and privacy requirements
- Compliance with privacy laws
- Lack of transparency and control

Sample Clauses

- Supplier shall perform its obligations under this Agreement, provide the Solution in compliance with applicable Laws, and conform the Solution to comply with changes in applicable Laws. Use of the Solution 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 the performance, receipt or use of the Solution. Supplier shall be responsible for any fines and penalties arising from any noncompliance with any applicable Laws relating to the performance, receipt or use of the Solution.
- Supplier shall make the Solution available 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.
- Supplier shall develop and maintain a process to restrict access in its shared services locations to the Confidential Information of Customer and the Customer Data so that employees of Supplier or Supplier Agents providing services to the other customers of Supplier do not have access to the Confidential Information of Customer or the Customer Data, and to ensure that the Customer Data and the Systems on which Customer Data is processed or stored are at all times physically and logically separated from data and systems used for such third parties. Supplier shall not and shall not permit any Supplier Agent to perform the Services from a location outside of the United States.

Data Compliance

Market Landing Spot

- Robust security programs are the first line of defense.
- To the extent an employee absconds with data, that's covered. But a Provider'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.
- Consider data locations (U.S. vs foreign).

KILPATRICK TOWNSEND

cvent

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Data Security, Oversight, and Safeguards

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
- Protection against security vulnerabilities
- Data backups
- Data migration and transition
- Return / destruction of data

Vendor Diligence

1. What technical procedures will vendor implement to safeguard Customer Data?
2. Will vendor conduct background checks on staff who get data access?
3. What audit rights will customer have? Will vendor provide annual SOC 2 or ISO 27001 data security audits?
4. Will vendor implement written data breach procedures?
5. Does vendor solution comply with privacy laws, CCPA, CPRA, GDPR, others?
6. Does vendor solution involve data transfer to/from the EU and use of SCC's?
7. Conduct vendor security and risk assessment

Contractual Controls

SOC reporting	PCI DSS	ISO 27001, 27701
CSA CCM	DoD CMMC, FedRAMP	HIPAA
HITRUST	NIST CSF, 800-171, 800-53	EU-GDPR, CCPA

- 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

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.

Customer Perspective

Data Security

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.

Data Breaches

A Provider should have strict liability for data breaches.

Vendor Perspective

Data Security

A Provider should be responsible solely for their actions. In other words, it is important to exclude any third-party actions over which the vendor has no control, such as a malicious hacker. A Provider 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 Provider's risk to reward.

Data Breaches

A Provider 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 Provider'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).

KILPATRICK TOWNSEND

cvent

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Data Controls

Personal Information

- To avoid unnecessary security risks, the customer generally wants to limit the service provider's ability to disclose personal information to third parties without the customer's prior written consent.
- However, the service provider may seek or require flexibility to disclose personal information to certain third parties, such as its subcontractors or agents, without first seeking the customer's permission.

"Highly-Sensitive Personal Information" means an (i) individual's government-issued identification number (including social security number, driver's license number or state-issued identified number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; or (iii) biometric or health data.

"Personal Information" means information provided to Service Provider by or at the direction of Customer, or to which access was provided to Service Provider by or at the direction of Customer, in the course of Service Provider's performance under this Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual.

Confidential Information

- Require the receiving party to make an affirmative commitment to keep all such information confidential and to not disclose it to any other third parties.
- Specify circumstances where the receiving may make disclosures.
- Maintain confidentiality using the same degree of care used to protect its own information (i.e., data and software source code), but not less than a reasonable degree of care.

Usage Rights

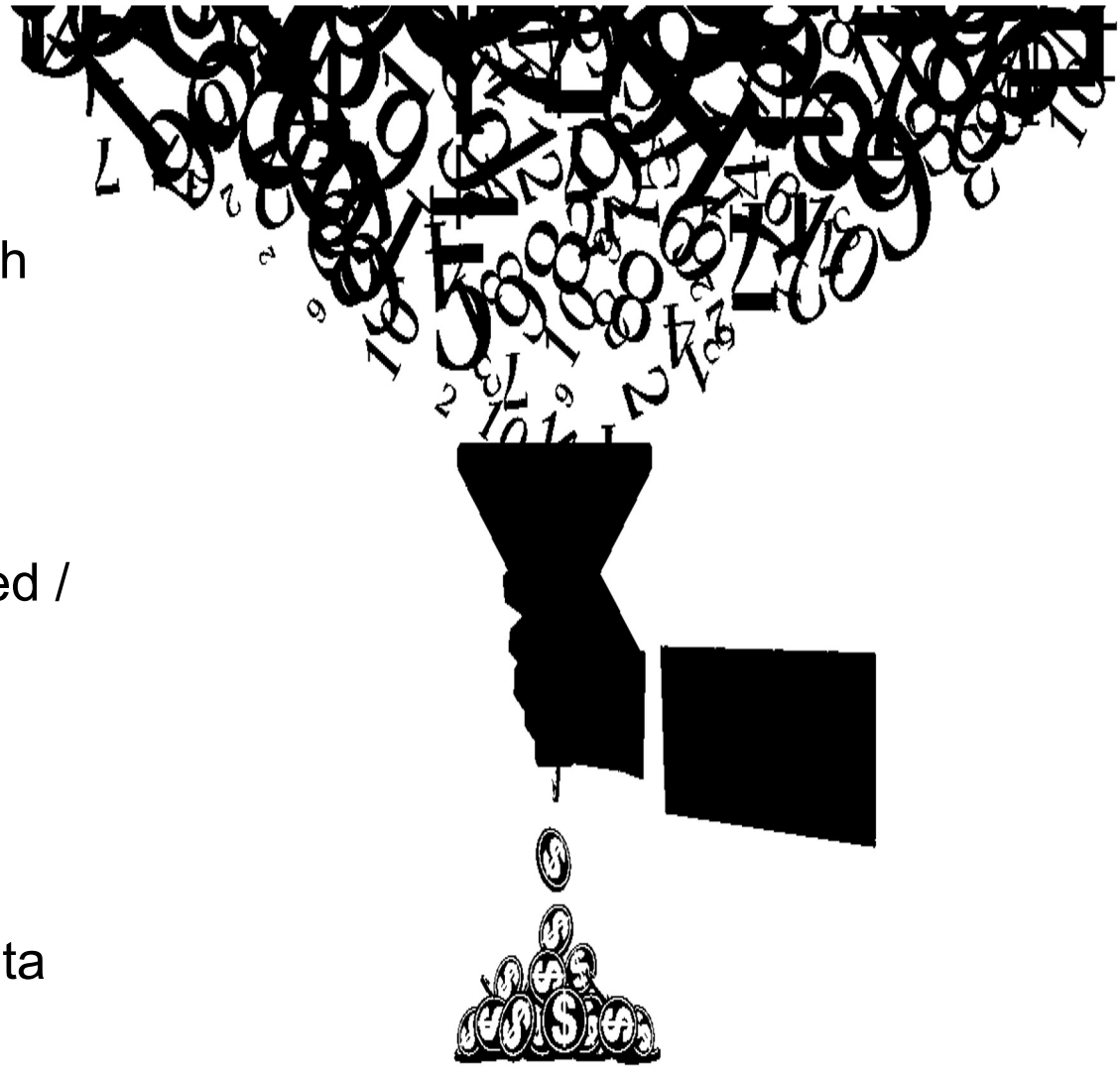
- Explicitly identify boundaries on how the other party can use the data.
- Define the type of access and use while also providing remedies in the event the scope of use is exceeded.
- Data Processing Agreement
- Identify specific exclusions of conditions, situations, and circumstances.
- Access / return / destruction of own data.

Access and Destruction of Data

- Ensure unfettered access to all data owned.
- Require the vendor to return or destroy any personal information in its possession at any time promptly upon the customer's request and upon termination for any reason.
- Information may be retained by the vendor in limited circumstances.

Aggregated 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, providers 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.”
- Can the data truly be aggregated? Anonymized?
- Any use of aggregated data should ensure that the data can truly be anonymized.



KILPATRICK TOWNSEND

cvent

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Liability / Risk Mitigation

Representations

- Vendor representations
  - Rights and licenses
  - Malicious code
  - Open source (permitted use)
  - Data security
- Customer representations
  - Rights to data
  - Required consents
  - Compliance with law

Sample Clause

- Supplier represents, warrants and covenants that:
  - the Services will be performed accurately, on time and in a professional manner by personnel with the education, experience, training and qualifications required to perform the tasks to which they are assigned.
  - it has all necessary intellectual property rights to the Solution and the Services and to grant the rights and licenses contemplated by this Agreement; and the Solution and the Software, Related Documentation and Services that comprise the Solution do not infringe upon any patent, copyright, or other proprietary or intellectual property right of any third party or misappropriate any trade secret or proprietary right of any third party.
  - no Malicious Code shall be coded or introduced into the Solution or the information technology environment of Customer by Supplier or as a result of a breach by Supplier of its obligations under this Agreement.
  - it shall obtain, maintain and comply with all Consents and Governmental Approvals required in connection with the provision, receipt and use of the Solution.
  - it has not used or distributed and does not use or distribute any Open Source Software in any manner that requires or has required (A) the Company to permit reverse engineering of any software code or other technology owned by the Company or (B) any software code or other technology owned by the Company to be (1) disclosed or distributed in source code form, (2) licensed for the purpose of making derivative works or (3) redistributed at no charge.

Indemnities

- Vendor's breach of data security obligations
- Vendor's violation of applicable laws
- 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.

- Trigger: Third party claims vs. direct claims
- Uncapped vs. super cap

Customer Perspective

Indemnities

A Customer seeks an enabling clause that includes a **full indemnity** (i.e., “defend, indemnify, and hold harmless”).

Moreover, a Customer will want to ensure that it is able to recover for **first party damages** in addition to third party damages.

Finally, a 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.

Scope

Broad indemnity to cover any and all damages, losses and liabilities

Triggered by a direct indemnity claim

At a minimum, covers both first party and third party damages

Vendor Perspective

Indemnities

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.

A Vendor seeks to limit its indemnity obligations to a **narrow list of occurrences**, such non-infringement and will include exclusions.

Scope

Limited indemnity to defend and pay

Indemnities

Common Landing Spot

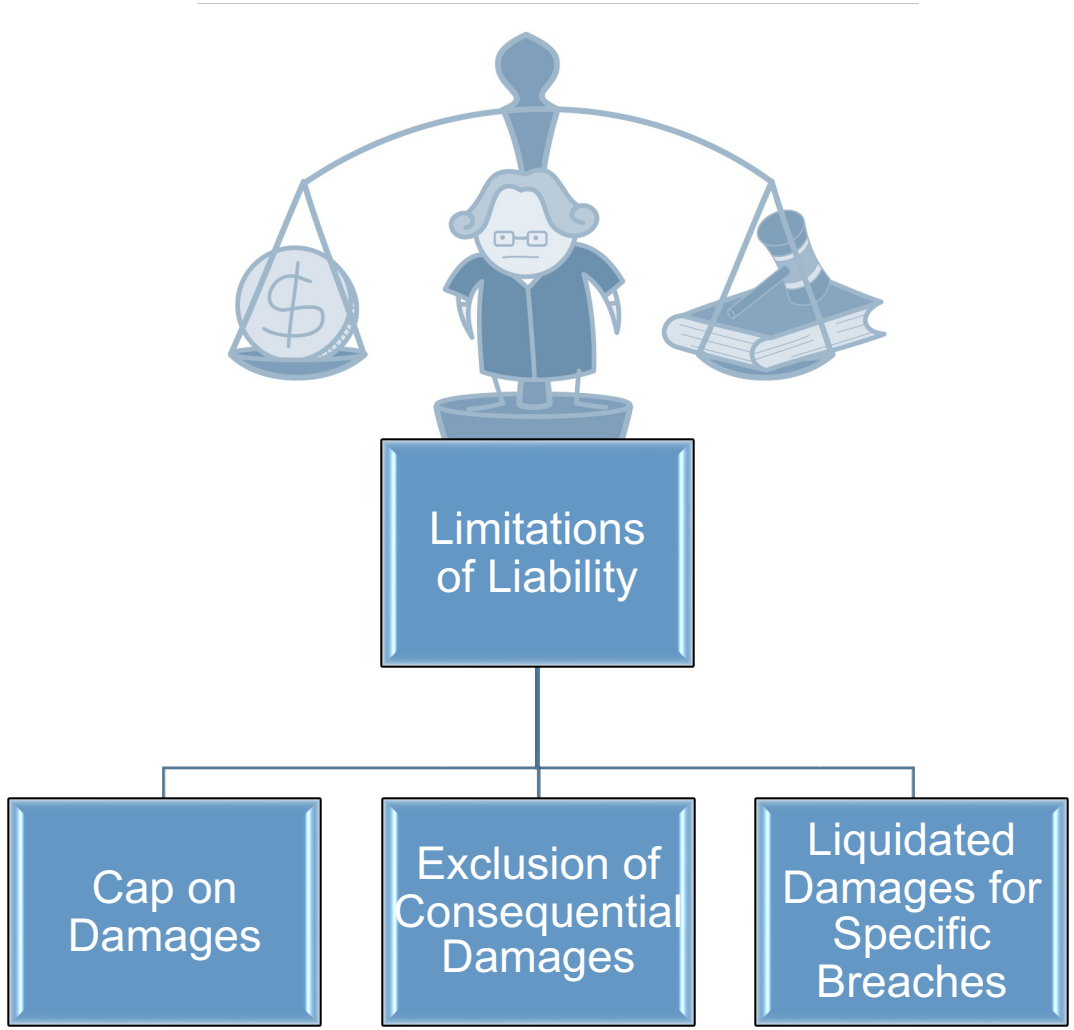
- Indemnities are typically limited a **3rd party claims trigger**, although full indemnity vs. defend and pay is still somewhat of a toss-up.
- Depending on the Vendor's risk tolerance, Vendors offer **IP-infringement** at a minimum, but others may include:
  - **personal injury** if its damage to tangible property or bodily damage (would not be strictly acts, likely tied to negligence or higher standard)
  - breach of **confidentiality** and **data security**, if tied to a SuperCap (*more on this later*)
  - breach of legal compliance (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 IP infringement indemnity that could undo protection (such as integration with 3rd party systems or customer's provision of "unclean" data).

Limitation of Liability

- Damages Cap
  - Aggregate Cap vs. Per Order / SOW vs. Fees for Deficient Services
- Consequential Damages Waiver
  - Are potential damages more likely direct or consequential?
  - Does prohibiting consequentials effectively exclude ability to recover meaningful damages?
- Exclusions from Limitations
  - Full exclusions from the damages cap (i.e., unlimited liability) vs. super caps



Customer Perspective

Limitation of Liability

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**.

Exclusions

Include exclusions that capture the losses that may happen from an economic perspective

- **Such as: breach of confidentiality, data security, indemnification, violations of applicable law, personal injury, property damage, intellectual property infringement, fraud, gross negligence, willful misconduct.**

Damages Cap

Aggregate fees paid or payable

Dollar amount floor

Vendor Perspective

Limitation of Liability

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 as for IP infringement indemnity and bad acts (fraud/gross negligence), but will attempt to only carve out from the damages cap.

Exclusions

Consequential damages should be excluded

Damages Cap

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 prior 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 Clause

- Damages Cap. Each party's liability for all claims arising out of 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 (24) times the average monthly Fees payable by Customer) and (b) [$5,000,000] .

- Each party's liability to the other for all claims arising out of this Agreement, where 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 six 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).

Questions?

Sonia Baldia

Partner
Kilpatrick Townsend

+1 202.508.5840

sbaldia@kilpatricktownsend.com

Edwin Y. Szeto

Vice President & Deputy General Counsel
Cvent, Inc.

+1 571.765.5699

ESzeto@cvent.com

Jeffrey Connell

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
Dallas
Denver
Houston
Los Angeles
New York
Raleigh
San Diego
San Francisco
Seattle
Shanghai
Silicon Valley
Stockholm
Tokyo
Walnut Creek
Washington DC
Winston-Salem