Cloud Chaos: Key Terms & Gotchas in Software, SaaS and Cloud Computing Agreements

Brian Busse
Arlo Technologies, Inc.

Charley Haley
Cooley

April 21, 2023

Agenda

- High-Level Overview
- Commercial Terms
- Data Security
- Data Usage Rights
- IP and Technology

High-Level Overview

- Cub Reporter's Creed: What, Who, How, Where, When?
  - What is the product use case (and is it (or what it accesses) critical)?
  - Who is the counter-party (and what is my leverage)?
  - How is the cloud product being integrated into my business (technically and contractually, e.g., flow-down terms)?
  - Where is the data flowing into the product coming from, and where is it being stored?
  - When do I get (and lose) access to the product (and what happens then)?

High-Level Overview (continued)

- Huge range of use cases and contract types (MSA, terms of service, P.O.s); general structure is remote access to cloud-based technologies on a subscription basis
- Usually include limited representations, but include detailed SLA with service credits
- IP transfers fairly rare (if definitions are correct); IP discussions focus on scope of data licenses
- Ever-greater data privacy and data security focus
- Exhibits are technical, and often as important than body of cloud agreement
- Industry-specific technical requirements may be required (to account for PHI, PII)
- Consider the specifics of your use case (or your sale) before launching the negotiation
- This presentation will reference a generic SaaS agreement (provided separately as Attachment 1)

Commercial Terms

- Is integration required? Is acceptance testing needed? What if acceptance never occurs?
- When do we “go live”, and when does the subscription (and payment obligation) begin?
- Do I need termination assistance? How do I get my data back?
- Termination for convenience
- What representations, if any, should provider give?
  - Industry-specific? ISO? No debarrment?
  - Sample definition that was wrapped into representation; compliance with –
  - *“**Good Industry Practice**” means, in respect of any activity, performing that activity effectively, reliably and professionally in good faith, in line with recognized applicable industry standards and in a prompt and timely manner using the degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from a skilled, experienced and market leading operator engaged in the provision of services similar to the Services. Includes without limitation compliance with Security Industry Practice;*

Commercial Terms (continued)

- Service Quality and Disruption
  - Is platform a key part of customer business? Is this a sole-source vendor?
    - What is the lead time to replace the platform?
  - SLA generally includes -
    - Availability; Response and Restore covenants; Service Credits
  - Business Continuity Plan
  - Escrow Agreement
    - Could the customer really benefit from this?
    - “Red flag” issue for vendor

Commercial Terms (continued)

- Should the customer policies – and other contractual obligations - apply to vendor's cloud platform?
  - InfoSec
  - Procurement terms
  - Code of Conduct
  - Flow-downs
- Each party needs to review and understand
  - all Exhibits, Schedules, embedded or referenced
  - Including hyperlinks
  - What if they change?

Commercial Terms (continued)

- Negotiating the cloud agreement
  - For either party, can be a long process – suggest an “internal term sheet” summarizing (x) value of the deal, and (y) what each party will NOT do, MUST have, etc.
  - Try to frame as operational process as much as legal one
    - e.g., security and data teams of both parties to coordinate on data flows/security
  - Does each party understand what the other sits from a compliance perspective?
    - When we say “compliance with Applicable Law”, applicable to whom?
    - e.g., do we need a BAA? e.g., the customer is a regulated financial institution, but we do not know anything about Gramm Leach Bliley?
  - Limitations of Liability and carve-outs, e.g. infringement risk, data loss
  - Understand precedence (fight the battles you need to fight)

Data Security

- Consider whether the security covenants should be specific or generic, and what is fair.
  - Specific would be, e.g., a covenant to –
    - *"establish, maintain, and ensure that Supplier remains in good standing with, Supplier's ISO/IEC 27001:2013 certification (or any successor) and the appropriate control objectives defined in ISO 27002 (or any successor), as well as any certifications and attestations required under the Customer Policies and Procedures, in relation to the Services and fulfilment of Supplier's obligations under this Agreement.*
  - Generic would be, e.g., a covenant to comply with -
    - *"**Security Industry Practice**" means, recognized, then-current applicable security industry standards, including those practices described in the International Organization for Standardization (ISO/IEC) ISO/IEC ISO27001, ISO/IEC 27002:2013, the National Institute of Standards and Technology (NIST) NIST 800-44, the Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications, and the Center for Internet Security (CIS) Standards (or any successor);*
  - Middle of road is have liability accrue if objective standard is not met. Some customers want a representation that use of platform "*does not cause loss or corruption of, or damage to, the uploaded Customer Data*".

Data Security (continued)

- Data Exhibit
  - If provided by customer, will need to be reviewed line-by-line by vendor IT team, and an addendum may be needed to provide carve-outs
- Parties to determine whether any specific privacy statutes apply
  - Is a BAA or DPA required?
- Data Protection and Security – Final Thoughts
  - Standards should be objective, not subjective; use ongoing compliance to improve model
  - Different treatment for types of data (PII, PHI)
  - Is a breach of data security covenants equivalent to breach of confidentiality covenants?

Data Usage Rights

- Vendor usually wants to own “usage data”, customer wants to own data outputs from its use of the platform. In some cases customer data rights can be broadly stated, e.g. -
  - *“**Customer Data**” means all data, documents or records of whatever nature (including personal data) and in whatever form relating to the business of Customer including details of customers, employees or otherwise, whether subsisting before or after the date of this Agreement and whether created or processed as part of, or in connection with, the Services or provided by Customer to the Supplier in connection with this Agreement;”*
- Data Licenses.
  - Vendor sometimes wants a license to improve/train products and services, and to create aggregate data sets.
  - Customers in turn want narrow license, e.g.,
    - *“Customer hereby grants to the Supplier and the Subcontractors a non-transferable, non-exclusive, royalty-free licence to use, modify, adapt and enhance Customer Data for the Term solely for the purpose of performing their obligations under this Agreement, subject to and in accordance with the terms of this Agreement. “*
  - Privacy statutes, in particular CCPA, require additional express consents, and/or treat the vendor differently, if the data usage is anything beyond the narrow license above.

IP and Technology

- In some cases customers request extremely broad definitions that arguably create broad IP transfers, e.g.,
  - *""**Materials**" means anything (including any item, work product, data, record, documentation, hardware or software (in object code and source code format)) used in or for the performance of the Supplier's obligations under this Agreement or provided to, or used in, the receipt of the Services by XXX. References to this term shall include any modification, adaption, enhancement or derivation of such materials and all Intellectual Property Rights in such materials;"*
- Aside from such definitions, there are usually limited (intentional) IP transfers from use of multi-tenant platforms. Threshold question is whether the go-live requires configuration, or actual customization.
- Licenses
  - Outbound from Vendor – Not technically needed for basic "use" right, sometimes needed if vendor retains reports and other outputs
  - Inbound to Vendor – data and content license as described above; feedback; grant-back to work product and other customizations

Thank you

Cooley

Presenters

Brian Busse
General Counsel, Arlo Technologies, Inc.

Charley Haley
Partner, Cooley LLP