11.17.2016

ABA IP Litigation Roundtable Committee Hot Topics in IP Law: "How to Identify and Contract with a Cloud Services Provider that you can Truly Trust"

Prepared By: Dennis Garcia, Assistant General Counsel, Microsoft Corporation, dennisga@microsoft.com

https://www.linkedin.com/in/dennisgarciamicrosoft.

I. As a "Level-Set", Provide a Non-Technical Overview of Cloud Computing/Cloud Computing "101" that is Suitable for Lawyers as Many Lawyers are Not Technical and Do Not Understand the Basics of Cloud Computing.

a. Nowadays the Cloud is Ubiquitous in our Personal Lives.

i. The Cloud Powers Web-Enabled Hosted Email that All of Us Have Been Using Since the Late 1990s.

ii. Much of the Data Generated by our Smartphones are Stored in the Cloud.

iii. The Cloud Powers Social Media (e.g., Facebook, LinkedIn, Twitter).

b. There is No Singular Definition of Cloud Computing:

i. Formal Definition: The National Institute of Standards & Technology ("NIST") Definition:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

ii. Informal Definition: The Cloud is "a fancy way of saying stuff's not on your computer" via Quinn Norton, "Byte Rights," Maximum PC, September 2010, at 12.

c. The Cloud = "Off-Premises" Computing (Versus the Traditional "On-Premises" Computing Model) Delivered Via a Cloud Provider's Data Centers.

d. The Three (3) Major Types of Cloud Computing:
   i. Software as a Service ("SaaS") – an example is Microsoft Office 365.
   ii. Infrastructure as a Service ("IaaS") – an example is Amazon Web Services.
   iii. Platform as a Service (PaaS) – an example is Microsoft Azure.

e. Potential Benefits of Cloud Computing:
   i. Cost Savings.
   ii. Scalability.
   iii. Improved Productivity.
   iv. Enables You to Focus on Your Core Business.
   v. Enhanced Security if You Work with a Trusted Cloud Provider.

f. Potential Disadvantages of Cloud Computing:
   i. Losing Control of Your Data Can Mean Less Security.
   ii. Cloud Provider is a Bigger Target for Hackers.
   iii. Hidden Costs When Working with a Cloud Provider.
   iv. Data Migration Can be Costly & Time Consuming.
   v. Being "Locked-In" to a Cloud Provider.

II. Why Is It Important to Select a Trustworthy Cloud Provider?

a. We Continue to Learn About High Profile Data Loss Incidents Affecting Many Organizations Across All Industries.

b. Cybercriminals are Increasingly Becoming More Sophisticated.

c. Security versus Privacy Debate: The Need of Government to Have Access to Data to Protect Us from a National Security Perspective Versus the Need to Protect the Privacy Interests of People & Organizations.

d. There is No Cloud Computing Law Per Se: Instead There's a Patchwork of Evolving Data Privacy/Data Protection Laws that Varies from Country to Country.

e. As the Cloud Computing Industry Continues to Grow there are So Many Cloud Providers to Choose From Nowadays. Those Providers Range from Traditional IT Providers to Providers "Born in the Cloud" to Small Providers that have Limited Capital to Providers from Other Industries who Now Offer Cloud Services (e.g., Telephony Companies).

III. **<u>Phase 1</u>**: Conduct Thoughtful Due Diligence & Evaluation on a Potential Cloud Services Provider.

a. This is a Highly Critical Phase.

b. Assemble Your Team of Professionals to Guide You Through this Phase.

   i. You Do Not Need an "Army" of Professionals.

   ii. Instead Focus on a "Core Four (4)" Approach of Enlisting the Support of these Key Stakeholders:

      1. Legal Counsel.
      2. Privacy Professional from Your Chief Privacy Officer ("CPO") Team.
      3. Security Professional from Your Chief Security Officer ("CSO") Team.
      4. Professional from Your Risk Management/Compliance Team.

c. Begin Your Due Diligence/Evaluation Process.

   i. Consider Developing and Issuing Request for Information ("RFI") or Request for Proposal ("RFPs") Documents to Potential Cloud Providers.

   ii. As an Alternative Develop a Detailed Security Questionnaire for Cloud Providers to Answer.

d. Regardless of Whatever Process You Use Consider Developing a Common Due Diligence/Evaluation Framework Based on These Four (4) Guiding Principles:

   i. Security: A Cloud Provider Should Be Committed to the Protection of Your Data When Using its Cloud Services.

      1. Clearly Understand the Technical, Operational & Physical Measures that a Cloud Provider Undertakes to Protect Your Data in its Cloud Services.
      2. Understand What Encryption Methodologies a Cloud Provider Uses to Protect Your Data in its Cloud.
      3. Does a Cloud Provider Have Assets that Enable It to Identify & Fight Cybercriminals? If so, does it Incorporate Those Learnings Back into Both its Cloud Solutions and Data Centers to Make Them More Secure? (e.g., Microsoft's Digital Crimes Unit team): http://news.microsoft.com/presskits/dcu/#sm.00007jj5da13xiewnvc3tp8cxf7zj

   ii. Privacy & Control: A Cloud Provider Needs to Maintain Privacy and Your Control of Your Data When Using its Cloud Services.

      1. Make Sure that a Cloud Provider Agrees to Specific Data Processing/Protection Terms as Part of its Cloud Contract.
      2. Those Terms Should Contain the EU Model Clauses that have been Validated by an Influential EU Regulator like the Article 29 Working Party. Please see this example:

http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/#sm.00007jj5da13xiewnvc3tp8cxf7zj

3. Review a Cloud Provider’s History with Worldwide Privacy Regulators and Gravitate Towards Cloud Providers that have a Strong and Positive “Track Record” with those Regulators.
4. Gravitate Towards those Cloud Providers who Offer More Data Control Options to You in the Form of Both Data On-Premises and Off-Premises (Cloud Computing) Solutions.
5. Ensure that a Cloud Provider’s Contract is Clear that You Retain Ownership to Your Data and that a Cloud Provider Can Only Use Your Data to Provide its Cloud Services and Not for Advertising or Similar Commercial Purposes.
6. Clearly Understand from a Cloud Provider what Happens when Law Enforcement Seeks Access to Your Data.
7. Determine Whether a Cloud Provider has been willing to Resist Law Enforcement Access to Your Data Via Litigation. See examples here: https://digitalconstitution.com/
8. Determine Whether a Cloud Provider is Actively Seeking to Modernize US Privacy Laws (e.g., the Electronic Communications Privacy Act (“ECPA”) to be More Consistent with 21st Century Cloud Computing Technology.

iii. Compliance: Understand Whether a Cloud Provider Helps Enable You to Meet Your Compliance Needs when Using its Cloud Services.
    1. EU-U.S. Privacy Shield Compliance.
    2. EU Model Clauses Compliance.
    3. Health Insurance Portability and Accountability Act ("HIPAA") Compliance Via a Business Associate Agreement ("BAA").
    4. International Organization of Standardization ("ISO") 27001 Compliance.
    5. ISO 27018 Code of Practice Compliance.
    6. ISO 19086 Family of Standards that Establishes a Framework for Cloud Service Level Agreements ("SLAs"). http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67545

       https://www.microsoft.com/en-us/trustcenter/Compliance/ISO-IEC-19086-1

    7. Statements on Standards for Attestation Engagements ("SSAE") 16 Service Organization Control ("SOC") 1 Type II Compliance.
    8. SSAE 16 SOC 2 Type II Compliance.
    9. Key US Public Sector Compliance Standards: (a) FEDRamp, (b) Family Educational Rights and Privacy Act ("FERPA"), and (c) Criminal Justice Information Services ("CJIS").

iv. Transparency: Work with a Cloud Provider who is Crystal Clear and Truly Transparent Regarding its Cloud Business Practices.

        1. Depicting and Periodically Updating Cloud Business Practices Via Websites (e.g., Microsoft Trust Centers) https://www.microsoft.com/en-us/trustcenter
        2. Periodic Issuance of Law Enforcement Transparency Reports (or Similar Reports).
        3. Specificity Regarding the Location of “Data at Rest” with a Cloud Provider.
        4. Transparency Regarding the Identity of Third Party Subcontractors.
        5. Clear Cloud Contract Provisions.
        6. No Unilateral Cloud Contract Changes During Subscription of Cloud Services.
        7. Easy Access to Third Party Audit Reports.
        8. Ask a Cloud Provider if it is Willing to Offer a Tour of its Data Center Environment.

IV. **Phase 2**: Establish a “Smart” Contract with a Cloud Services Provider.

- a. Cloud Services are Not Custom Information Technology Services.
- b. It is Commercially Reasonable to Leverage/Work From a Cloud Provider’s Standard Cloud Contract Terms Versus a Customer’s Standard Form.
- c. Many Cloud Providers are Reluctant to make Material Cloud Contract Changes Regarding its Operation of Cloud Services.
- d. Make Sure Your Contract with a Cloud Provider Contains these “Top 10” Terms at a Minimum:
    - i. Clarity on Data Ownership & Usage.
    - ii. Data Processing/Protection Agreement.
    - iii. Meaningful SLAs.

iv. Third Party Access to Data.
v. Limitation of Liability.
vi. Security Incident Notification.
vii. Independent Verification.
viii. Responsibility for Subcontractors.
ix. Terms of Use/Service Changes.
x. Compliance with Applicable Laws.

e. Here are Samples of Contract Terms from Leading Cloud Providers:

i. Microsoft: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

ii. Amazon Web Services:

https://aws.amazon.com/agreement/

iii. Google:

https://admin.google.com/terms/apps/2/2/en/premier_terms.html

V. **<u>Phase 3</u>**: Actively Manage & Monitor Your Cloud Contract

a. Don't Just Put Your Cloud Contract in a Drawer and Forget About It!

b. Assign a Professional In-House to Actively Manage Your Contracts with Cloud Providers.

c. Keep Your Cloud Provider Honest to its Cloud Contract Obligations (e.g., SLAs).

d. Monitor Data Privacy/Protection Changes in the Law and Seek Appropriate Cloud Contract Amendments as the Law Evolves.

e. As the Cloud Provider Marketplace Continues to Become More Concentrated Via Mergers & Acquisitions Make Sure

You Understand Your Rights and Obligations When Cloud Providers are Subject to a Change in Control Event.