DOND 2017

DEAL OR NO DEAL:
EPISODE VII – THE LAST CONTRACT

Session 8: 5:00-6:00

Presented by Davis Polk

Title:

Cloud Computing Transactions: Risks, Rewards and Mitigation Techniques

Speakers:

Michelle Ontiveros Gross - Counsel, Davis Polk
Steve Salmon - Partner, Davis Polk
Arthi Chakravarthy - VP, Commercial Legal Affairs, TiVo

Michelle Ontiveros Gross

COUNSEL

+1 650 752 2073
michelle.gross@davispolk.com

Ms. Gross is counsel in Davis Polk's Corporate Department, practicing in the Intellectual Property and Technology Group in Northern California. Her practice includes a wide range of intellectual property-related matters, including strategic alliances, joint ventures, and licensing, as well as intellectual property strategy and commercialization, copyright, patent and trademark matters and integration of business units and product lines in connection with mergers and acquisitions. She also advises clients on data privacy and security matters, including with respect to cybersecurity, technology and data initiatives, development of privacy and data security policies and product development.

Ms. Gross also has significant experience advising clients on large-scale, complex business process and information technology outsourcing transactions (across a broad range of business processes such as finance and accounting, information technology, application development and maintenance, human resources, claims processing, logistics, co-location, and facilities management).

BAR ADMISSIONS

- State of California
- State of New York

EDUCATION

- B.S., Stanford University, 2001
- J.D., Columbia Law School, 2004

WORK HIGHLIGHTS

REPRESENTATIVE EXPERIENCE

- Citigroup in connection with various technology transactions related to its divestiture of OneMain
- FormFactor on its acquisition of Cascade Microtech
- Equinix in numerous acquisitions including its acquisition of Verizon's data center business
- Ingram Micro in its sale to Tianjin Tianhai, a subsidiary of China's HNA Group
- SMART Modular in connection with numerous licensing and technology collaboration transactions
- Roper Technologies in connection with various acquisitions of technology companies
- 1-Page in its acquisition of Marianas Labs
- A semiconductor company on privacy and data security compliance issues
- Affymetrix on its contested $1.3 billion sale to Thermo Fisher Scientific
- Tencent Holdings Limited in its investment in Grail
- Numerous corporations with structuring outsourcing arrangements in compliance with federal, state, and other laws and best practices
- Corporations and financial institutions on cybersecurity policies, procedures and training, as well as cyber breach prevention and mitigation measures
- An educational technology company on privacy and data security compliance issues and negotiation of privacy compliance agreements with public entities
- A Singaporean investment company on intellectual property and privacy and cybersecurity advice in connection with its investment in a software technology provider
- Initial Public Offerings by Adamas Pharmaceuticals, Aeglea Biotherapeutics, Coherus, Conformis, Coupa, Etsy, GoDaddy, iRhythm, Loxo Oncology, Nevro, Pure Storage

RECOGNITION

Legal 500 U.S. –Technology:

- Transactions
- Outsourcing
- Data Protection and Privacy

Super Lawyers – "Rising Star":

- Northern California: Intellectual Property
- New York: Intellectual Property

PROFESSIONAL HISTORY

Davis Polk since 2014

Stephen Salmon

PARTNER

+1 650 752 2063
stephen.salmon@davispolk.com

Mr. Salmon is a partner in Davis Polk's Corporate Department, practicing in Northern California. He has extensive experience in both mergers and acquisitions transactions and a variety of capital markets offerings for clients across many industries.

WORK HIGHLIGHTS

MERGERS AND ACQUISITIONS REPRESENTATIONS

World Kitchen on its acquisition by GP Investments Acquisition Corp.

Ingram Micro in its pending sale to Tianjin Tianhai, a subsidiary of China's HNA Group

Dialog Semiconductor in its attempted acquisition of Atmel

Dialog Semiconductor on its acquisition of iWatt

J.P. Morgan on the acquisition of Dell by Michael Dell and Silver Lake Partners

Reliance Steel on its acquisition of Metals USA

Mirion Technologies and affiliated funds of American Capital on the acquisition of Mirion by Charterhouse Capital Partners

Blue Coat Systems on its acquisition by an investor group led by Thoma Bravo

Vector Capital on its acquisition of Gerber Scientific and concurrent disposition of assets

Oracle on multiple public and private acquisitions and dispositions, including the acquisitions of Art Technology Group, Phase Forward, GoldenGate, Hyperion, Stellent and Metasolv

Citigroup on multiple loan portfolio dispositions

NYSE Euronext on its acquisition of APX, and APX's subsequent merger with BlueNext

W Capital on multiple primary and secondary investments in technology companies

CAPITAL MARKETS REPRESENTATIONS

The underwriters on the initial public offerings of Aimmune Therapeutics, Virgin America, Coherus BioSciences, Violin Memory, UCP and Internet Brands

Cadence, Reliance Steel and Leidos on their investment-grade notes offerings

Convertible notes offerings by Citrix, Accuray, Invensense, Beckman Coulter and others

GENERAL CORPORATE ADVISORY WORK

Public reporting, securities compliance and corporate governance advice for companies like Dialog Semiconductor, Leidos, Roper, Blue Coat Systems and Mirion Technologies

RECOGNITION

Mr. Salmon is recognized as a leader in the legal industry:

Super Lawyers – "Rising Star," 2012-2016

Daily Journal – "Top 40 Under 40," 2016

OF NOTE

Speaker at PLI's "Venture Capital 2016: Nuts and Bolts" seminar

PROFESSIONAL HISTORY

Partner, 2015-present

Associate, 2006-2015

BAR ADMISSIONS

State of California

EDUCATION

B.A., Philosophy, Yale University, 2000

cum laude

J.D., Stanford Law School, 2006

SPEAKER BIOS: SESSION 8

Arthi Chakravarthy
VP Commercial Legal Affairs
TiVo

Arthi is currently Vice President, Commercial Legal Affairs at TiVo. Previously she was General Counsel at DNA2.0 (d/b/A Atum) where she managed all legal issues for the company. Before that, she was at Broadcom Corporation managing commercial transactions for a $2.5B division where she helped pioneer a $100MM LOB. Prior to Broadcom, she was at Wilson Sonsini. She graduated from Stanford University with a degree in Human Biology, and her Juris Doctor from Stanford Law School.

Agenda

- Cloud Computing Diligence Issues
- Negotiating Key Cloud Contract Terms
- Mitigation Cloud Computing Risk: Cybersecurity Insurance
- General Data Protection Regulation

Cloud Computing Diligence Issues

Due Diligence Issues

Information Assets

- Type of data being processed
- Location
- Materiality
- Applicable Laws
  - Health Insurance Portability Act (“HIPAA”)
  - Gramm-Leach-Bliley (“GLBA”)
  - General Data Protection Regulation (“GDPR”)
- Existence of adequate policies and procedures
- Data collection processes
- Past data security breaches, service interruptions, investigations or incidents
- Security controls
- Audit reports (internal or external)
- Agreements with third parties that act as the Company’s agents or contracts and receive sensitive information

Addressing Cybersecurity Risks

Cybersecurity Representations and Warranties

- Compliance with laws vs. policies/statements and contractual commitments vs. industry standards and practices
- All applicable cybersecurity policies have been provided
- No written notices related to investigations
- No data security breaches or loss of data
- No unauthorized disclosure of personal information or sensitive information
- No complaints, notices, audits regarding collection or processing of personal information

Addressing Cybersecurity Risks (cont.)

Cybersecurity Representations and Warranties

- Maintenance of commercially reasonable information security programs
- Cybersecurity representations on behalf of target's key third-party service providers
- Ownership of personal information
- Maintenance of commercially reasonable security, disaster recovery and business continuity plans, procedures and facilities
- To the extent relating to the Business, personal data will be solely and exclusively owned and available for use by, and in the possession and control of, the Company, immediately following the Closing Date, without any restrictions or other limitations or any obligations to any other Person.

Addressing Cybersecurity Risks (cont.)

Indemnification

- Typically, representations and warranties form the basis for post-closing indemnifications for damages due to breaches that occurred pre-closing.
- It is becoming more common to see indemnification provisions related to data privacy and cybersecurity as stand-alone provisions.

Negotiating Key Cloud Contract Terms

Negotiating Key Cloud Contract Terms

- **Security**
  - Definition
  - Legal requirements
  - Industry standards
  - Penetration testing and reports
- **Access to data**
  - Frequency, process and form
- **Service levels and credits**
- **Third-party service providers**
  - Pre-approval by customer
  - Contract requirements
  - Liability
- **Breach notification responsibilities**
  - Legal requirements
  - Process
  - Root cause analysis, prevention, mitigation
  - Preservation of evidence

Negotiating Key Cloud Contract Terms (cont.)

- **Indemnification**
  - Third party claims vs actual breach
  - Government investigations
  - Customer responsibilities
- **Limitation of liability**
  - Standard carve-outs
  - “Super-cap”
- **Suspension rights and termination**
  - What should trigger a suspension? For how long?
  - Should a refund by offered?
  - What is a reasonable cure period prior to termination?
  - What transition period is needed?
- **Links to external terms and conditions**
- **Audit rights**
- **Post-termination access to data**

Mitigation Cloud Computing Risk: Cybersecurity Insurance

Cybersecurity Insurance Coverage

Initially, cybersecurity coverage focused on privacy breaches, breach notification costs and investigatory costs. Scope of coverage has since expanded substantially but still varies from product to product.

First-Party Coverage: Most common, exists in most policies

- Direct expense of responding to breach
- Loss of income due to breach
- Fines/Penalties
- Event Management
- In some circumstances, extortion demands related to security threats

Third-Party Coverage

- Third-party claims based on a failure to protect confidential information
- Regulatory actions

Cybersecurity Insurance Limitations and Exclusions

- Notification during specified period
- Cooperation with insurer
- Pre-authorization of certain expenses
- PCI fines and penalties sometimes excluded
- Voluntary notification
- Contractual liability
- Criminal conduct
- Unencrypted data
- Vicarious liability
- Unauthorized collection of customer data

Cybersecurity Events and Traditional CGL Policies

- Cybersecurity damage as property damage
- Crime insurance
- D&O liability insurance
- Cases to note:
  - Cottage Health v. Columbia Casualty Co.: Court has been asked to interpret cyber insurance policy language requiring the policyholder to comply with specified network security requirements.
  - Rosen Millennium v. St. Paul: Insured is arguing that the St. Paul policy did not specifically exclude data breach claims from its CGL coverage
  - Aqua Star v. Travelers: Social engineering schemes, what constitutes a direct loss under computer fraud coverage? Does the actual transfer itself need to be carried out through fraudulent means to constitute a direct loss?

General Data Protection Regulation: Cloud Processors

General Data Protection Regulation: Cloud Processors

- **Obligations on processors**
  - Direct legal obligations
  - Exposes processors to fines, penalties and compensation claims for failure to satisfy those obligations
- **Security**
  - Appropriate technical and organization measures to protect personal data and what is appropriate is assessed in terms of a variety of factors including:
    - the sensitivity of the data
    - the risks to individuals associated with any security breach
    - the cost of implementation
    - the nature of the processing in general
- **Subcontracting**
  - Written consent must be obtained from the controller to subcontract their activities.
  - Processor must inform controller of any new sub-processors, allowing the controller to object.
- **Recordkeeping**
  - Processors must maintain a record of all categories of processing activities including details of the controller and any other processors as well as the relevant contact details of the Data Protection Officer (DPO), the categories of processing carried out, details of any transfers or data exports, and a description of technical and organizational security measures.

General Data Protection Regulation: Cloud Processors (cont.)

- **Data breach notification**
  - Processors are required to notify the controller of any breach without "undue delay" after becoming aware of it.
  - May need to be addressed in the contract to establish precisely what is to be done in the event of a breach.
- **Data Protection Officer**
  - Processors under the GDPR must appoint an independent, reliable and knowledgeable data protection officer under the same conditions as controllers, meaning they are obliged to do so if their core activities consist of
    - Processing which requires regular and systematic monitoring of data subjects on a large scale,
    - Processing on a large scale of special categories of data (e.g. health, religion, race, sexual orientation etc.) and personal data relating to criminal convictions and offenses.

General Data Protection Regulation: Cloud Processors (cont.)

- **Data Processing Agreement:** Under the Directive, data processing agreements between controllers and processors have been mandatory, but the contract was often limited to basic terms. Under the GDPR, the contract should contain greater detail, including with respect to following processor's obligations:
  - To generally process the personal data only pursuant to **documented instructions** from the controller
  - At the controller's election, **delete or return all personal data** to the controller upon completion of the services and return any existing copies of the data, unless otherwise required by law
  - To make available to the controller all information necessary to demonstrate compliance with obligations regarding processing by a processor and allow for and contribute to audits, including inspections
  - **To assist the controller in ensuring compliance with its security and certain other obligations**, taking into account the nature of the processing and the information available to the processor
  - To comply with **stricter subprocessing rules** (the subprocessing contract needs to impose upon the subprocessor the requirements of the data processing contract between the controller and the processor, and prior written approval of subprocessors by the controller will be required)
  - To ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
  - **Make available to the controller all information necessary to demonstrate compliance** with its obligations and allow and cooperate fully with **audits**, including inspections, conducted by the controller or another person authorized to this end by the controller

DOND 2017: NOTES

ACC Association of Corporate Counsel
SAN FRANCISCO BAY AREA

DEAL OR NO DEAL 2017:
EPISODE VII – THE LAST CONTRACT