PERKINSCOIE

COUNSEL TO GREAT COMPANIES

Key Customer Issues to Consider Before Entering into a Cloud Services Arrangement

Law Seminars International
December 9, 2014

Peter J. Kinsella
303/291-2328

The information provided in this presentation does not necessarily reflect the opinions of Perkins Coie LLP, its clients or even the author

Risk Investigation

Customers will often want to consider a variety of financial, data, security and regulatory issues before entering into a cloud services arrangement.

Customers will typically attempt to mitigate risk through a variety of mechanisms:

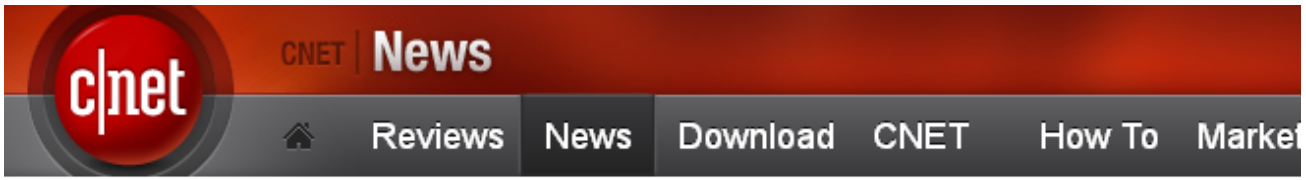
- Diligence
- Audit pre- and post-contract execution
- Contract risk allocation

Common Customer Concerns

- Integration – What is the onboarding process?
- Availability – will the service be available for use?
- Legality – can the customer legally use the service?
  - Privacy – how do I know the provider won't use the data in an unauthorized manner?
  - Security - will the data be secure?
- Integrity - will the data be stored and processed accurately?
- Termination – what happens upon termination?

Availability -1

Financial Health of Service Provider



CNET › News › E-Business

October 17, 2000 6:15 PM PDT

Red Gorilla can't survive capital-market jungle

By Stefanie Olsen
Staff Writer, CNET News

Red Gorilla has shut down its site and turned over its current customers to another application service provider, its chief executive told CNET News.com on Tuesday.

"Right now the (Red Gorilla) system is offline, all the employees were let go, and there's no money in the bank," said chief executive John Witchel. "Officetool.com has agreed to continue operating the Web site so that our customers can continue to use our software."

Availability -2

Data Center/Location Issues

Where is the data stored?

- Does the service provider use subcontractors to host data?

What are the characteristics of the data center?

- Redundant telecommunications, power, and cooling?

Physical security of data centers?

- Who has access to: facilities, infrastructure, platforms, applications, and data?

Availability -3

Business Continuity

Has the provider (or its subcontractor(s)) experienced past outages?

Does the service provider:

- have a business continuity plan?
- provide redundant operations from different sites?
- routinely test its back-up capability?
- routinely attempt to restore data?

It is important to consider the impact of bankruptcy on the ability to access the service and data

Legality/Privacy

Frequently implicated data protection laws:

- EAR/ITAR (prohibits "export" of information)
- Sarbanes-Oxley (controls over financial information)
- EU Data Protection Act (see next slides)
- Patchwork of Federal Laws, For example:
  - Gramm-Leach-Bliley (banking/insurance information)
  - HIPAA (employee or third party health information)
  - FERPA (information concerning students)
- Patchwork of evolving state laws

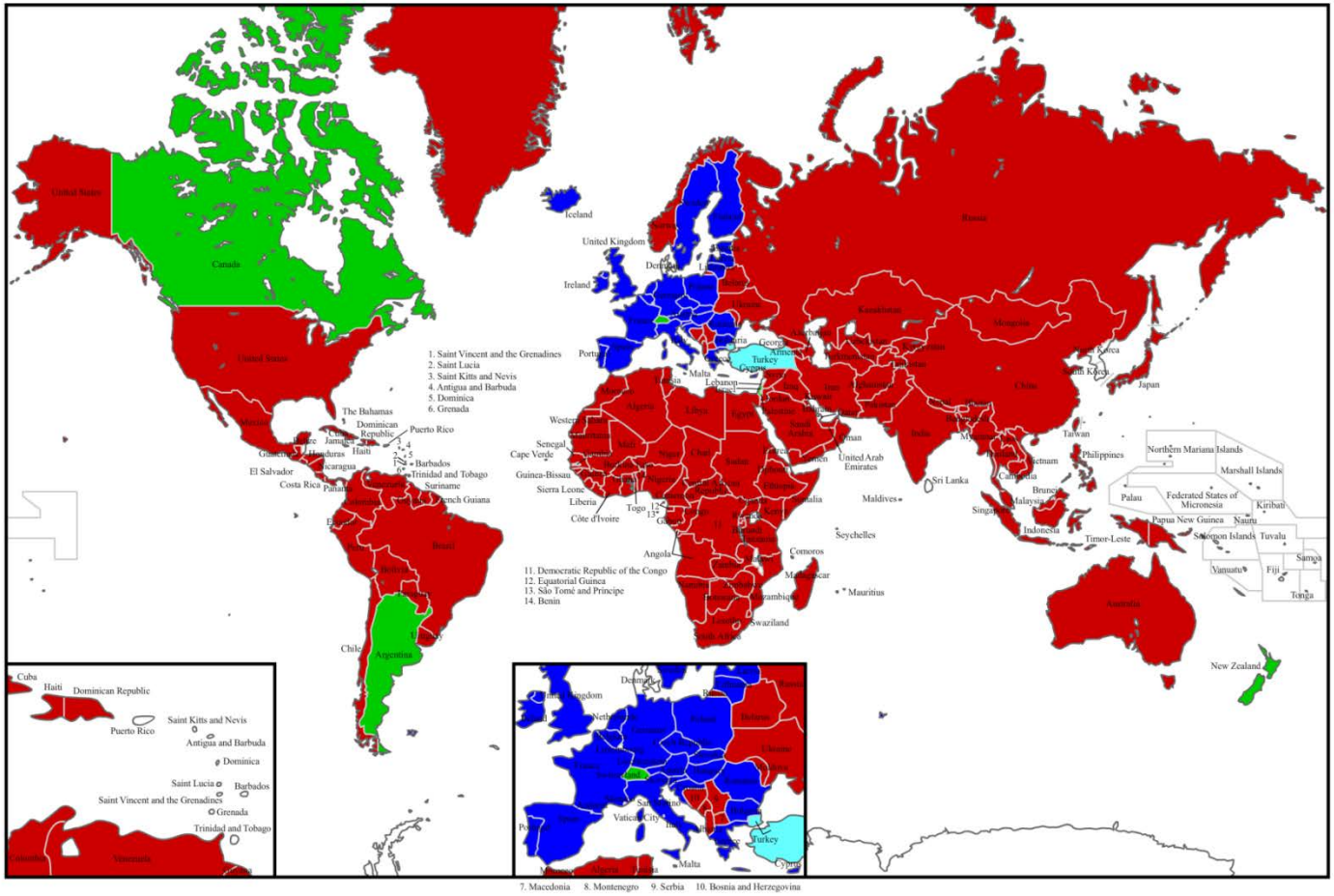
Peter J. Kinsella 303-291-2300

Common Privacy Issues

- Privacy policies
- Who is permitted to “access” the data?
- How can the data be used by the provider?
- How does the provider destroy data? When?
- What other information is the provider collecting?
- Can the customer access data and meta-data?
- Does the provider follow its procedures?
- Does the data require the flow-down of specific obligations?

EU Data Protection Laws -1

EU Restrictions on Data Transfer



Peter J.

PERKINSCOIE

EU Data Protection Laws -2

EU Data Protection Laws Issues

- Rule: Data must not be transferred to countries outside the EU that do not offer an “adequate level of protection”
  - Currently only: Andora, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay.
- Exceptions:
  - ask permission from every “data subject” involved
  - for US - Dept. of Commerce “safe harbor” registration
  - EU model contract clauses
  - “Binding Corporate Rules”

Peter J. Kinsella 303-291-2300

EU Data Protection Laws -3

- Legislation makes fundamental distinction between:
  - **data controller**: party that defines the purpose and the means of processing the data
  - **data processor**: the party performing the tasks
- Data controller is liable towards the “data subjects”
- Data controller is obligated to select appropriate data processors, and must obtain adequate contractual protection from them

Peter J. Kinsella 303-291-2300

EU Data Protection Laws -4

EU law will apply when:

- A “controller” is located in its territory; or,
- When a “controller” outside the EU uses “equipment” within the EU territory

Applied to cloud computing:

- using an EU-based data center triggers legal compliance obligation
- Many authorities interpret “equipment” in an extremely broad way (e.g., browser cookies)

Peter J. Kinsella 303-291-2300

Security -1

Target Boosts Card Security After Data Breach

By Richard Davies
@daviesnow

Apr 30, 2014 8:41am

Home Depot's 56 Million Card Breach Bigger Than Target's

'Unique, Custom-Built Malware' Eliminated From Retailer's Systems After Five-Month Attack on Termi

Email

By ROBIN SIDEL CONNECT

Updated Sept. 18, 2014 5:43 p.m. ET

Home Depot Inc. said 56 million cards may have been compromised in a five-month attack on its payment terminals, making the breach much bigger than the holiday attack at Target Corp.

Available to WSJ.com Subs

Fresh Signs of Global Slump Challenge U.S.

Peter J. Kinsella 303-291-2300

PERKINSCOIE

Security -2

Data Segregation

- Public vs. Private Cloud
- Encryption?
  - Transmission? Rest?
  - Who has the keys?
- Where and how is backed-up data stored?

Does the system have software and other access controls to prevent unauthorized access?

Is penetration testing routinely performed?

Security -3

- Are physical and logical security procedures required?
- Employee background screening?
- How is security verified?
  - Note that a customer audit may not be permitted under law or under other provider contracts
- Is a separate Data Protection Agreement needed?
  - Often used when handling EU data

Peter J. Kinsella 303-291-2300

Security - 4

Some Commonly Used Security Standards

SSAE-16 (replaces SAS-70) requires management to provide a written assertion concerning the organization's systems, suitability and effectiveness

ISO-27001/27002 – comprehensive controls in areas such as access control, asset management, business continuity and how to handle security breaches.

PCI DSS – credit card security

HIPAA – security requirements for health information

Subcontractor Privacy/Security Issues

- Are subcontractors used to provide the service?
- Can vendor identify the subcontractors?
- What data can the subcontractor access?
- Can the service provider impose contractual obligations on the subcontractors?
  - This may be required for certain types of data (e.g., HIPAA, EU Data)

Peter J. Kinsella 303-291-2300

Thanks!

Peter J. Kinsella

pkinsella@perkinscoie.com

303-291-2300