



# Colloquium on Electronic Commerce

## Session II: Mobile Commerce

“Other” Aspects of the Legal and  
Regulatory Enabling Environment:  
Focus on Good Practices in  
Liberalization & Cyber-security

14 February 2011

New York

David Satola  
Senior Counsel

[dsatola@worldbank.org](mailto:dsatola@worldbank.org)



# Legal Enabling Environment

- [e-Commerce]
- Infrastructure and Services Competition
- [Financial Sector Regulation]
- [Consumer Protection]
- [IPR]
- “Cyber-Security”
  - CIR
  - CII/CIIP
  - Digital Data Protection
  - [Authentication]
  - Cybercrime
- Institutional Aspects

## Stocktaking:

Who's doing what where  
and where is there scope  
for WG IV  
to add value?



# Regulatory coherence will support m-commerce

- Convergence of telecoms, financial sector and cybersecurity raises policy issues.
  - *Market entry* – limited scope of mobile licenses may restrict advanced money transfer services.
  - *Competition* – discriminatory access to financial services, or exclusive relationships might lead to dominance.
  - *Consumer interest* – regulatory responsibility in case of consumer complaints will need clear definition, data security and privacy will have to be ensured.
  - *Tariff regulation* – passing on costs of new financial services (e.g., stored value) to consumers.
  - *Legacy policy* – existing regulatory policy may create conflicts (e.g. number portability and bank account numbers).
- Regulators have a central role in m-commerce
  - Removing any existing restrictions on m-banking.
  - Creating an enabling policy and regulatory environment.
  - Supporting increased access to ICTs and new applications.



# Leverage synergies to drive collaboration

Coordination can enhance governance and prevent non-transparent practices

- Sector regulators already have common interests in consumer protection and data security.
- Inter-regulator coordination will reduce the risk of arbitrage and improve familiarity with new actors and business models.
- Leverage a coherent enabling environment to promote non-discriminatory access between financial service providers and mobile networks.



# Trends

- Liberalized environment
- Pro-entry licensing
- Technology neutrality
- Private sector led
- Role of NGOs



# telecom infrastructure & services



# Infrastructure & Services

## Substantive Issues:

- Liberalization & Pro-Competition
- Licensing that facilitates new entry
  - Class Licensing
  - Unified Licensing
- Technology Neutrality
- Independent Regulator

## Status:

- Mainly national level
- But Int'l & Regional influences
  - ITU
  - EU & other Regional Orgs
- Private Sector

## Issues for WG IV:

- Recognition of issues & roles played, impact on x-border legal framework



cybersecurity







Ecommerce

CIR

CIIP

Cybercrime

Privacy

Institutional

# “Cyber-Security” is ...?

# Layers

Applications/Services

---

Software

---

Infrastructure



# Issues affecting evolution of cyber-security

- *Dissonance in national approaches to cyber-security*
- *Policy and implementation incoherence*
- *Outdated legal architecture doesn't fit cyberspace well*
- *Existing tools and instruments are not fully applied or are only partially implemented*



# Critical Internet Resources

## Substantive Issues:

Mainly technical

- DNS SEC
- IPv4 – IPv6

## Status:

- ICANN
- Standards Bodies
  - IETF

## Issues for WG IV:

- Recognition of issues & roles played, impact on x-border legal framework



# CII / CIIP

## Substantive Issues:

Mainly Technical

- Internet is mainly PS
- CERTs

## Status:

- Mainly NGO, Academic & PS
- ICANN DNSSEC
- FIRST
- Regional
  - EU Gov't's CERTs (ECG)

## Issues for WG IV:

- Enhance coherence in managing x-border cooperation



# Digital Data Protection / Privacy

## Substantive Issues:

### Constitutional/Rights-Based

- Confidentiality of Data
  - PII
  - IPRs
  - Client data
- Security vs. Privacy
- Timely verification& correction
- Safeguards *viz.* secondary use
- Breach Notification
- Institutions - Commissioners

## Status:

- Mainly National Law, but
- Different int'l/regional approaches
  - Int'l
    - CoE Convention
    - Madrid Declaration
  - Regional
    - EU Directives
    - APEC Cross-Border Privacy Enforcement Arrangement
- Stds – ISO
- Guidelines - OECD

## Issues for WG IV:

- ?



# Cyber-crime

## CoE Budapest Convention

### Substantive Issues:

A Law enforcement approach

- Offences
  - Data
  - Computer Offences
  - Content Offences
  - IPR Offences
- Procedural Rules
- Int'l Coop

### Status:

- Only substantive int'l instrument
- 30 Countries + 21 pipeline
- Issues with effective x-border cooperation
- Safe havens

### Issues for WG IV:

- Implementation of X-border cooperation?



# Lessons from the cloud

Identifying the shifting frontier of liability





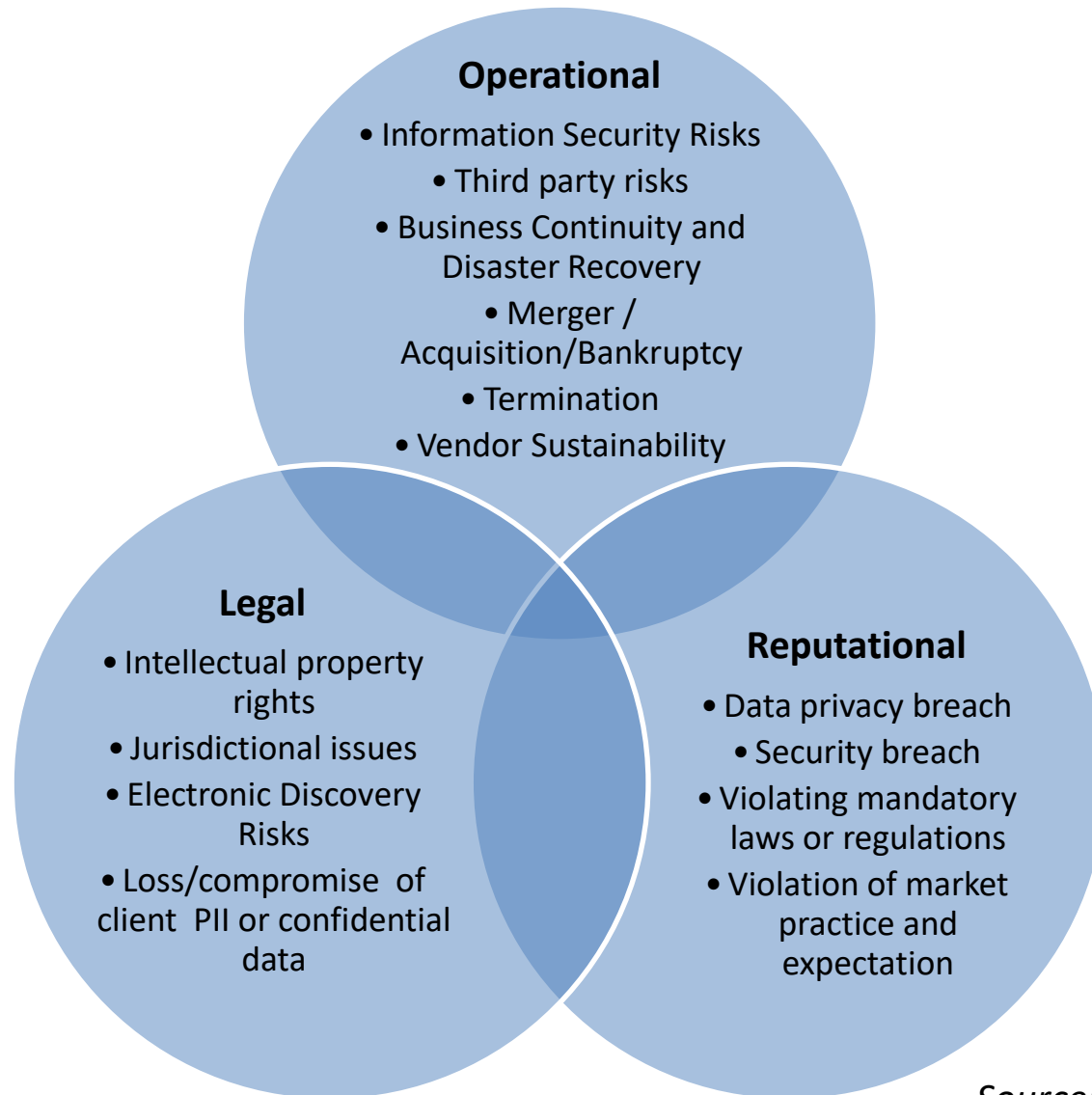
# Types of Clouds

Cloud Type	Definition
<b>Private</b>	A Private Cloud is a dedicated or single-tenant Cloud environment where the user exerts control over information to the extent it controls information on its own internal network. Computing resources can either be owned by the organization or their service provider, but this Private Cloud is typically located on the user's own premises or at another designated venue under the user's control.
<b>Highly Managed</b>	A Highly Managed Cloud is like other highly managed IT services in that the Customer has a high degree of visibility and management over how vendor services are delivered. It is controlled and managed by a provider where the physical infrastructure may be owned by the organization and/or run on the organization's premises.
<b>Public</b>	Public Clouds are provided and owned by service providers. These Cloud Computing resources may be offered to a single consumer, but it is far more likely that they will be shared by multiple tenants. Because Public Clouds are shared and available to multiple unrelated consumers these Clouds have “untrusted” consumers. In this configuration, it may be difficult for the user to exercise meaningful control over its information.



*Source: World Bank*

# Risks Associated with Cloud Computing



*Source: World Bank*

# Cloud

## Substantive Issues:

### Contract-Based

- Liability:
  - Data Security/loss/compromise
  - Network Security
- Multi-jurisdictional compliance
- Vendor Continuity
- Jurisdiction

## Status:

PS-led

## Issues for WG IV:

Dealing with a dynamic liability frontier depending on type of “Cloud”



# Some considerations for WG IV from int'l practice in crafting a comprehensive x-border legal framework for m-commerce

- **UNCITRAL IS THE FORUM TO ADDRESS THESE ISSUES**
- Gaps to be filled?
  - Take note of other international, regional efforts
  - Benefit from coordination
  - Build linkages
- Guidance across constitutional, law-enforcement, legal, contractual and technical realms
- Recognition of range of actors – Gov't, Inter-Gov't, NGOs, PS
- How to cope with a *Dynamic Liability Frontier* posed by realities of x-border m-commerce



# Some Cyber-Security Resources

2010 IGF Workshop on Legal Aspects of Internet Governance: International Cooperation on Cyber-security at :

<http://www.intgovforum.org/cms/component/chronocontact/?chronoformname=WSProposals2010View&wspid=123> and <http://www.afilias.info/igf10-ws-123>

David Satola and William J. Luddy, Jr., *The Potential for an International Legal Approach to Critical Information Infrastructure Protection*, 47 **Jurimetrics J.** 315–333, Spring 2007.

David Satola and Henry Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cyber-security Legal Frameworks*, Wm. Mitchell Law Journal (expected 2011).

