Expert Meeting on

CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE:
INCLUDING CASE STUDIES AND LESSONS LEARNED
25-27 March 2015

Cybersecurity and Data Protection - First Principles

By

Chris Connolly
Director
Galexia

The views reflected are those of the author and do not necessarily reflect the views of UNCTAD
Cybersecurity and Data Protection – First Principles

EXPERT MEETING ON CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE (UNCTAD)
March 2015, Geneva

Chris Connolly
Overview

- The tension between cybersecurity and data protection

- The increased role of cloud computing services (and related challenges)

- The role of Government
  - The ‘Do No Harm’ principle
  - Improving cybersecurity infrastructure
  - Mutual legal assistance
  - Ensuring global rights

- The role of the private sector
  - Global companies – global responsibilities
  - The failure of Intermediaries
Major Tensions between cybersecurity and data protection

Persistent issues

- Mass collection and retention of data (usually communications meta-data)
- Identity and authentication of individuals vs anonymity
- Governance, oversight, transparency and legal redress

Newer issues

- Cross-border surveillance
- Forum shopping and outsourcing illegal surveillance practices
- Attacks on privacy enhancing technology and infrastructure
# The increased role of cloud computing services

<table>
<thead>
<tr>
<th>Positive impact</th>
<th>Negative impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>The most innovative development in computing for years</td>
<td>Benefits not spread evenly, especially in developing countries</td>
</tr>
<tr>
<td>Significant cost savings, allowing reallocation of resources</td>
<td>Potential for dominance by multinational vendors</td>
</tr>
<tr>
<td>Multiple fail-safes and backups that reduce the risk of data loss</td>
<td>Lack of standards / consistency in security certifications and audits (although now improving)</td>
</tr>
</tbody>
</table>
| Privacy protection ‘layers’ rather than a single point of privacy protection | Massive data sets now a ‘honey pot’ for attacks  
Data held offshore subject to law enforcement / security access |
| New opportunities for ‘big data’ analysis and collaboration | Potential for exploitation of data and concerns about the absence of data custodians |

The role of Government (1)

- The ‘Do No Harm’ principle
  - First Principle for Governments should be to avoid harm to individual rights and security infrastructure when pursuing cybersecurity objectives.
  - Examples of harm include the deliberate undermining of encryption standards, requiring ‘back door’ access to IT infrastructure etc.

- Improving cybersecurity infrastructure
  - National cybersecurity strategies and Public Private Partnerships (PPPs)
  - See the BSA / Galexia EU CyberSecurity Maturity Dashboard 2015 at:
  - [http://cybersecurity.bsa.org/index.html](http://cybersecurity.bsa.org/index.html)
The role of Government (2)

- Mutual legal assistance
  - Complex labyrinth of multinational and bi-lateral agreements
  - Each agreement contains a different data protection test
  - The strongest test is that surveillance requests should be ‘necessary, proportionate and narrowly tailored’ (EU-US terrorist finance tracking program – TFTP 2010)
  - Many agreements only state ‘necessary and proportionate’
  - However, some agreements have no test

- Ensuring global rights
  - Important for countries to extend human rights protections to all residents / consumers, not just “citizens”, to ensure global coverage and protection
The role of the private sector

Global companies – global responsibilities

» Key participants in cybersecurity (through innovation, PPPs, reporting to CERTs, community education etc.)
» Important to keep egos in check and collaborate for the common good
» The Do No Harm principle should also apply to the private sector

The failure of Intermediaries

» Banking / payments sector failing to restrict cybercrime
» Trustmark and security certification schemes failing to protect consumers
  – FTC prosecution of TRUSTe 2015 ($200,000 fine for misleading and deceptive conduct)
  – “Sites certified as secure often more vulnerable to hacking, scientists find”:
Outstanding Issues?

- There are still significant gaps in basic cybersecurity infrastructure.
- Complex and overlapping international agreements on cybersecurity legal assistance often lack strong data protection tests.
- Disappointing that intermediaries have not played their part in managing cybersecurity and data protection (a single intermediary might manage thousands of companies).
- Important to recover trust in law enforcement, national security and the private sector through developing global protections and following the Do No Harm principle.