Data Privacy and Sovereignty: Global Challenges in the Cloud

Sheila M. FitzPatrick
Worldwide Data Governance & Privacy Counsel
Chief Privacy Officer
26 April 2016
Agenda

- Sense of Urgency
- Data Privacy & Sovereignty Laws
- Shared Concerns
- Global Challenges in the Cloud
- Data Privacy vs. Data Security
- NetApp’s Global Program
- Intersection of Trust & Technology
EU Data Protection Regulation (GDPR)
EU Passes New Regulation
EU unanimously approved stricter data protection regulations – applies to any company doing business in EU – December 2015

Digital Privacy Act – Canada addresses new technology (cloud) – Canada imposes stronger accountability with greater sanctions – January 2016

Latin American countries enforce new Privacy Acts restricting the collection, processing and transfer of personal data to the U.S. - Is LatAm the new EU? – Jan 2015

The scramble is on as commissioners seek to determine “adequacy” of the new EU-US Privacy Shield – is it a cosmetic version of Safe Harbor? – February 2016

Privacy guardians warn multinationals to respect laws
Ten data protection authorities from around the world reiterated that US multi-national corporations are overlooking privacy values and legislation when they place personal data in the cloud. US companies concerned about security but not privacy.
– Washington, D.C., October 2015
Canadian Data Protection Laws

- Privacy Act
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Digital Privacy Act 2016
- Provincial and Sectoral Laws
- Data Sovereignty Obligations
- Cybersecurity Regulations
- Anti-SPAM Laws (CASL)
- Data Breach Regulations
Global Data Protection Laws

**European Union**
- General Data Protection Regulation (GDPR)
- Country specific data privacy laws
- Cloud computing directive
- Data sovereignty obligations
- Cybersecurity directive
- Anti-SPAM laws
- NIS Regulations
- Data breach regulations

**Asia Pacific Rim**
- Country-specific privacy laws
- APEC cyber privacy code
- Cross Border Privacy Rules (CBPR)
- Restrict marketing activities
- Restrictions on cloud computing
- Data breach regulations

**Russia**
- Data Protection Act
- Data sovereignty law
- Federal law on advertisement
- Russia code on administration of personal data
- Storage of all Russian data within Russian Federation

**Latin America**
- Cross-border transfer restrictions
- Country-specific privacy laws
- Cloud computing regulations
- OAS cybersecurity guidelines
- Data breach regulations
U.S. Data Protection Laws

- Federal Privacy Act (Consumer)
- NIST Regulations
- Cybersecurity Executive Order (Voluntary)
- Data breach regulations
- HIPAA/HITECH
- Regulated industries
- State Privacy Laws
- Privacy Shield
Foremost on Our Customers Minds...And Ours

- How to move to the cloud/new technology
- Compliance with data privacy laws
- Data location and sovereignty
- Data breach remediation and contingency plans
- Government access
- Loss of control
- Data security
- Accountability and liability
- Data retention and destruction capability
Challenges in the World of Cloud Computing

- Global restrictions
- Compliance with data privacy/sovereignty laws
- Data location, jurisdiction, and cross-border data flow
- Data control and/or ownership
- Data that could or should live in the cloud (and type of cloud)
- Data breach remediation and contingency plans
- Security – encryption and tokenization
- Use of third parties
- Litigation and eDiscovery
Five Challenges in Canada

1. Role of cloud computing provider
   - Data controller vs. data processor
   - Obligations/joint accountability
   - Use of third parties

2. Determine which data protection/sovereignty laws apply
   - Establishments in Canada?
   - Equipment in Canada?
   - Uses equipment outside Canada, but processes personal data of Canadian citizens

3. Provincial/International data transfers/flows
   - Strict regulations (BC and Nova Scotia)
   - Transparency
   - Data subject consent

4. Classification of Data

5. Records Management
Data Privacy Versus Data Security

- Data security is NOT data privacy
- Privacy – legal collection, use, sharing, storage & transfer of data
- Security – fortress around the data
- Companies can have world class security, but no data privacy
- ISO 27018 addresses security, but not data privacy
- All cloud vendors can address security – few can address privacy
- Legal Privacy Impact Assessment - critical decision mechanism
How Do You Mitigate the Risks?

- Clear and explicit policies and procedures
- Data Privacy Impact Assessment (PIA)
- Data Privacy Agreements/Model Contractual Clauses
- Know the difference between privacy and security
- Restricted access to data
- Well defined data ownership – Data Controller vs. Data Processor
- Classify data – what should/should not live in the cloud
- Transparency – Opt Ins/Opt Outs
- Vetted third parties
- Know your risk tolerance
How NetApp® Addresses These Concerns

Business Impacting Decisions

Global Data Privacy  Cybersecurity  Cloud Computing  Big Data

NetApp Expertise: A Model Company for Addressing These Concerns

NetApp Internal Model Program

Global Policies and Procedures  Monitor and Advocate  Internal/External Partnerships  Internal/External Training  Ensure Products Mitigate Privacy Risks  Execute on Laws

Key Business Needs

Store Data  Protect Data  Understand Legs and Regs  Balance the Risks  Manage Costs
Summary – Intersection of Trust and Technology

- Decide what data can reside in the cloud vs. on-premises
- Understand the legal requirements and challenges
- Develop data protection savvy program
- Understand data privacy and data security are NOT the same – assess both
- Chose a “trusted advisor” who will partner to mitigate risks
- Determine your risk acceptance level
Questions?
Thank you.