THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

COMPX527 Week 11

Legal Issues

Assignment 2

Discussions:

- Everyone should have an understanding of the project
- Individual contribution
- Peer Evaluation form- opening on 20th Sep
- No Services can be used without my prior acknowledgment

Task 3: Demo and Presentation

- You will create a video of 7 minutes (maximum) presenting your slides and a short live demo of your solution, which will be played in front of the class and the invited panel.
- Your slides (3-4 slides) will include an introduction to your application, its architecture, and a **comment on your security** implementation.
- There will be 7 minutes for presentation with demo + 3-4 minutes for Q/A.

https://www.linkedin.com/posts/peter-smith-phd_yay-finally-an-aws-region-in-new-zealand-activity-7368467052879151104-j

Laws and Regulations

- When moving to a public cloud
  - Identify legal and regulatory requirements as well as legal risks associated with your application and data
  - Understand how laws and regulations apply to the business, cloud and your customers and partners
  - Work with the cloud provider to satisfy the legal and regulatory requirements

- Failure to comply often results in heavy punishment and liability issues

Legal Risks/Concerns

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

What are the legal risks/concerns when building a cloud-based application?

- Privacy
- Data location
- Data ownership
- Data retention
- Reputation fate sharing
- Investigation – Forensics

Privacy and Personally Identifiable Information (PII)

- Privacy means the ability to have control over one's life, actions and information
- NIST's PII definition: any information about an individual that "can be used to distinguish or trace an individual's identity"
- E.g. name, social ID, IRD number / tax ID, student ID, passport number, DOB, bank account number, (individual's) photo/voice/fingerprint/any biometric info, etc.
- Combination of data e.g. ethnicity, age, gender, home address and other information may be PII.
- Privacy risks:
  - Data breaches
  - Compliance challenges

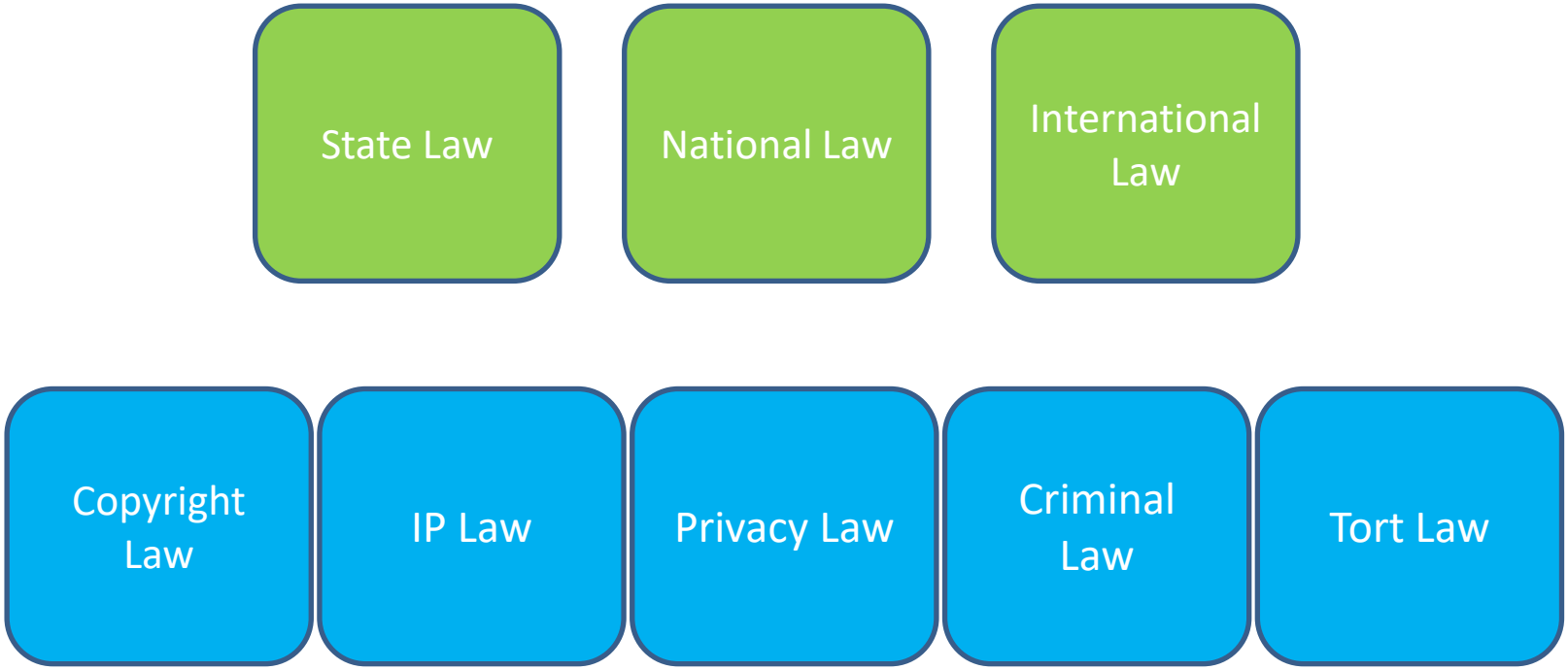
Reason for strong regulations

- Consumer protection
- Cybercriminal organisations ask for ransom in cryptocurrencies - bitcoin, etc.
  - If a country has weak laws it provides a safe haven for these cybercriminal organisations.
- Privacy

Legislation

- An organisation using cloud computing for storage or processing of personal data needs to navigate balance the legislation requirements with cloud computing benefits

Types of Legislation



Legal Due Diligence

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Companies are the custodians of data entrusted to them
- Numerous laws and regulations prohibit, restrict and limit disclosure and transfer of data to a third party.
- A cloud application provider should determine whether its business model allows for the use of cloud computing services, and legally under which conditions.
  - Do your customers accept the transfer of data to third parties
  - Is the data you are processing allowed to go beyond national borders
  - Etc.
- A cloud application provider should identify and take appropriate actions to mitigate any legal risks

Country-Specific Laws & Regulations

- Australia and New Zealand
  - The Privacy Act 2020
  - NZISM (NZ information security manual https://nzism.gcsb.govt.nz/ism-document#Chapter-17392
  - Australian National Privacy Act
- United States
  - GLBA – to control individuals' data stored & processed by financial institutions
  - SOX – to protect shareholders & the general public from accounting errors and fraudulent practices in the enterprise
  - CLOUD Act - US Law enforcement and government can ask for information from organisations incorporated in the US, even if their data center is outside the US

NZ Privacy Act 2020

- Replaces the Privacy Act of 1993
- Defines 13 Information Privacy Principles set out how agencies
  - collect personal information (IPPs 1 to 4)
  - store personal information (IPP 5)
  - provide access to (IPP 6) and correct (IPP 7) personal information
  - use (IPPs 8 and 10) and disclose (IPP 11) personal information
  - only keep personal information for as long as necessary (IPP 9)
  - disclose personal information outside of NZ(IPP 12)
  - use unique identifiers (IPP 13).

NZ Information Security Manual

- Manual on information systems security for government agencies as well as vendors, contractors and consultants who provide services to the agencies (any organization collecting and using personal information).
- All cloud computing decisions should be made on a case-by-case basis after a risk assessment and security is properly considered and implemented.

Standards

- Governance, Risk, Compliance
  - ISO/IEC 27001 and 27002, COBIT, ITIL, etc.
- Cloud Security
  - ISO/IEC 27017
  - ISO/IEC 27018
- Data Protection and Privacy
  - GDPR
  - ISO/IEC 29151
  - HIPAA in US, HISO standards in NZ
  - PCI-DSS
  - FIPS 140

Thank you.