Privacy - An overview and interactive discussion

ARMA HOUSTON WORKSHOP May 22, 2019

Presenter: Sandy R Miller, CRM, CIP, IGP, CIPM

AGENDA

- Overview
- Terms
- Frameworks
- Challenges
- Conclusion
- Questions

OVERVIEW

*The heart of the matter is that we want the information we share about ourselves – private information that personally identifies us – to remain in good hands. That goal has never been more challenging**

*Building a Privacy Program A Practitioner's Guide Edited by K Herath, pg 1, IAPP, 2011

OVERVIEW

Privacy is a global issue

- Focus is on the General Data Protection Regulation (GDPR)
  - High level summary: #GDPR – 1 minute to understand and take action (published 3/21/17)

Source: https://www.youtube.com/watch?v=Cgzd32FJJ8I&feature=youtu.be

TERMS

Privacy*

Four main areas of privacy are of particular interest with regard to data protection and privacy laws and practices:

(1) information privacy

The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others

(2) bodily privacy

(3) territorial privacy

(4) communications privacy

*IAPP website Glossary

TERMS

General Data Protection Regulation*

The General Data Protection Regulation (GDPR) replaced the Data Protection Directive in 2018. The aim of the GDPR is to provide one set of data protection rules for all EU member states and the European Economic Area (EEA). The document comprises 173 recitals and 99 articles.

*IAPP website Glossary

TERMS

Data Controller*

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by EU or member state law, the controller or the specific criteria for its nomination may be provided for by EU or member state law.

*IAPP website Glossary

TERMS

Data Processer*

A natural or legal person (other than an employee of the controller), public authority, agency or other body which processes personal data on behalf of the controller. An organization can be both a controller and a processor at the same time, depending on the function the organization is performing.

*IAPP website Glossary

TERMS

Information Life cycle management*

- aka data life cycle management (DLM) or data governance

ILM is a policy-based approach to managing the flow of information through a life cycle from creation to final disposition.

- provides a holistic approach to the processes, roles, controls and measures necessary to organize and maintain data
- has 11 elements including: minimalism; adequacy of infrastructure; information security.

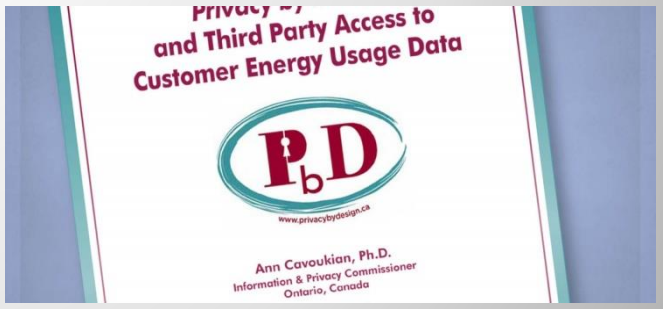
*IAPP website glossary

TERMS

Privacy by Design*

(Generally regarded as a synonym for Data Protection by Design)

The PbD framework dictates that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.



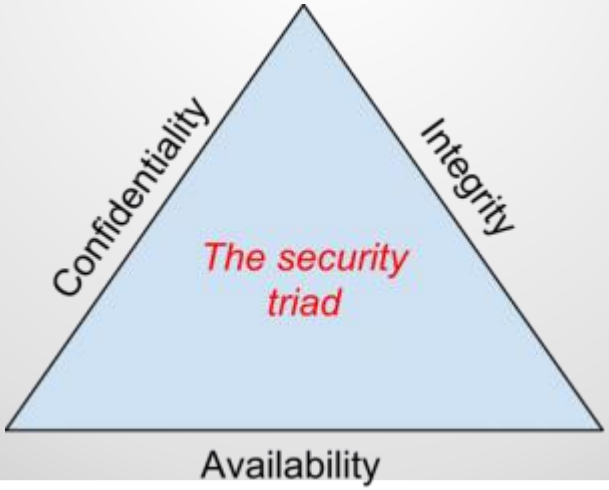
*Privacy Program Management Tools for Managing Privacy Within Your Organization, R Densmore, IAPP, p. 88, 2013

TERMS

CIA Triad

Also known as information security triad, three common information security principles from the 1960's

***C**onfidentiality, **I**ntegrity, **A**vailability.*



FRAMEWORKS

Privacy Frameworks began emerging in the 1970's

- Frameworks:
  - Many choices
  - Based on geographic, political and national boundaries
  - Serve as an implementation roadmap that provides structure
- Examples:
  - APEC Privacy Framework
    - Asia-Pacific Economic Cooperative
  - PIPEDA principles
    - Personal Information Protection and Electronic Documents Act, Canada
  - OECD guidelines
    - Organisation for Economic Co-operation and Development. Includes Europe, US, Australia
  - Generally Accepted Privacy Principles (GAPP)
    - Promulgated by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA).

FRAMEWORKS

APEC Privacy Framework

- *The APEC Framework, published by the Asia-Pacific Economic Cooperative, is a framework to protect privacy within and beyond economies and to enable regional transfers of personal information to benefits consumers, businesses, and governments. This framework is used as a basis for the APEC Cross-Border Privacy Rules (CBPR) System**

*IAPP website

FRAMEWORKS

Generally Accepted Privacy Principles (GAPP)*

A framework promulgated by the American Institute of Certified Public Accountants (AICPA) in conjunction with the Canadian Institute of Chartered Accountants (CICA).

The ten principles are management, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security for privacy, quality, monitoring and enforcement.

*IAPP website Glossary

CHALLENGES

- Identifying your data/information
- Adhering to laws and regulations
- Collecting the minimum amount of data
- Measuring the effectiveness of the Program
- Main an up-to-date Incident Response Plan
- Performing ongoing training

CHALLENGES

Technology

- Data Breaches
  - Limit access to high risk data
  - Adhering to Retention Periods decreases the impact from breaches

CHALLENGES

Transformational change from a compliance function to a data governance function

CONCLUSION

Privacy is:

- a complex field
- a moving target
- all about partnerships
- becoming more of an integral part of data governance

QUESTIONS