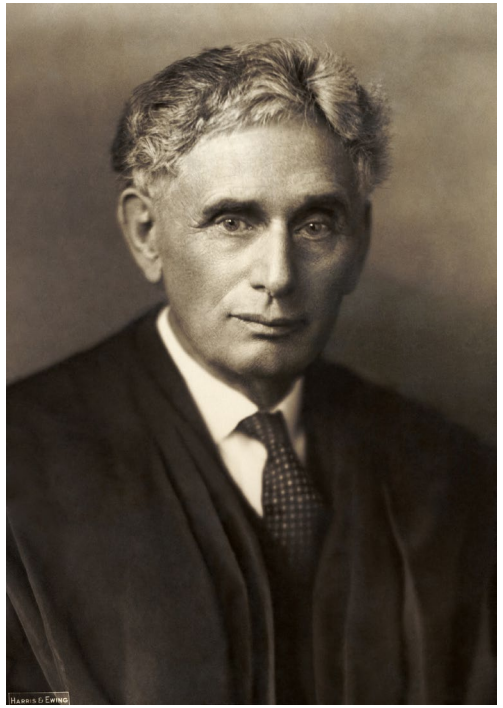
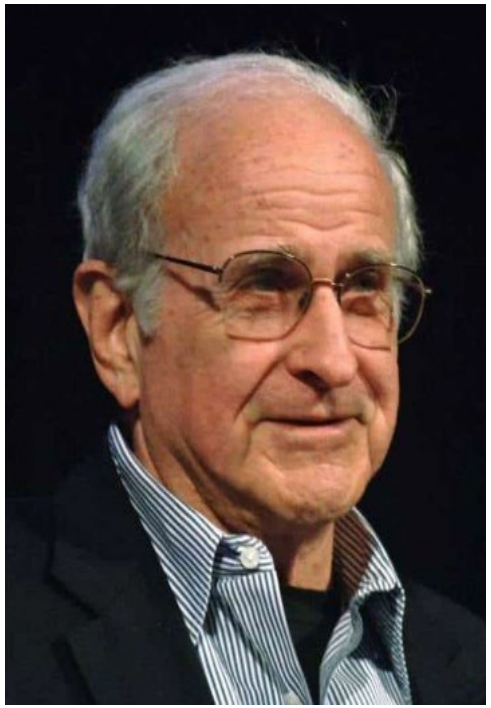
MSBA 5507.1 Ethics, Risk Management and Data Security

Privacy and Risk Management
July 22, 2022





Ken DeJarnette
ken@kdejarnette.com
ken.dejarnette@dominican.edu
213-399-8706
Office hours: Wed 1-3 pm

TOPIC	DESCRIPTION/SOURCES

Recap General Privacy Principles

- General Privacy Principles
  - Management: Establishing accountability and responsibility for privacy within the organization.
  - Notice: Informing individuals about the collection, use, and disclosure of their personal information.
  - Choice and Consent: Providing individuals with options and obtaining their consent for the collection, use, and disclosure of their personal information.
  - Collection: Collecting personal information in a lawful and fair manner.
  - Use, Retention, and Disposal: Using personal information only for the specified purposes, retaining it only for as long as necessary, and disposing of it securely.
  - Access: Providing individuals with the ability to access and correct their personal information.
  - Disclosure to Third Parties: Disclosing personal information to third parties only with appropriate consent and safeguards in place.
  - Security: Implementing appropriate measures to protect personal information against unauthorized access, disclosure, alteration, or destruction.
  - Quality: Maintaining accurate, complete, and relevant personal information.

TOPIC	DESCRIPTION/SOURCES
CCPA	**California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)**
Discussion	❑ Applies to businesses that collect the personal data of California residents ❑ Personal information that: ❑ Identifies ❑ Relates to ❑ Describes ❑ Is capable of being associated with ❑ Could reasonably be linked (directly or indirectly) with a particular individual or household. ❑ Includes inferences (preferences, characteristics, psychological trends, predispositions, etc. ❑ Expands sensitive personal information to information that reveals ones: ❑ Precise geolocation ❑ Racial or ethnic origin ❑ Religious or philosophical beliefs ❑ Union membership ❑ Also, includes biometric information for the purposes of uniquely identifying an individual and information collected and analyzed concerning an individual's health, sex life or orientation

TOPIC	DESCRIPTION/SOURCES
CCPA	**California Consumer Privacy Act (CCPA)**

Discussion

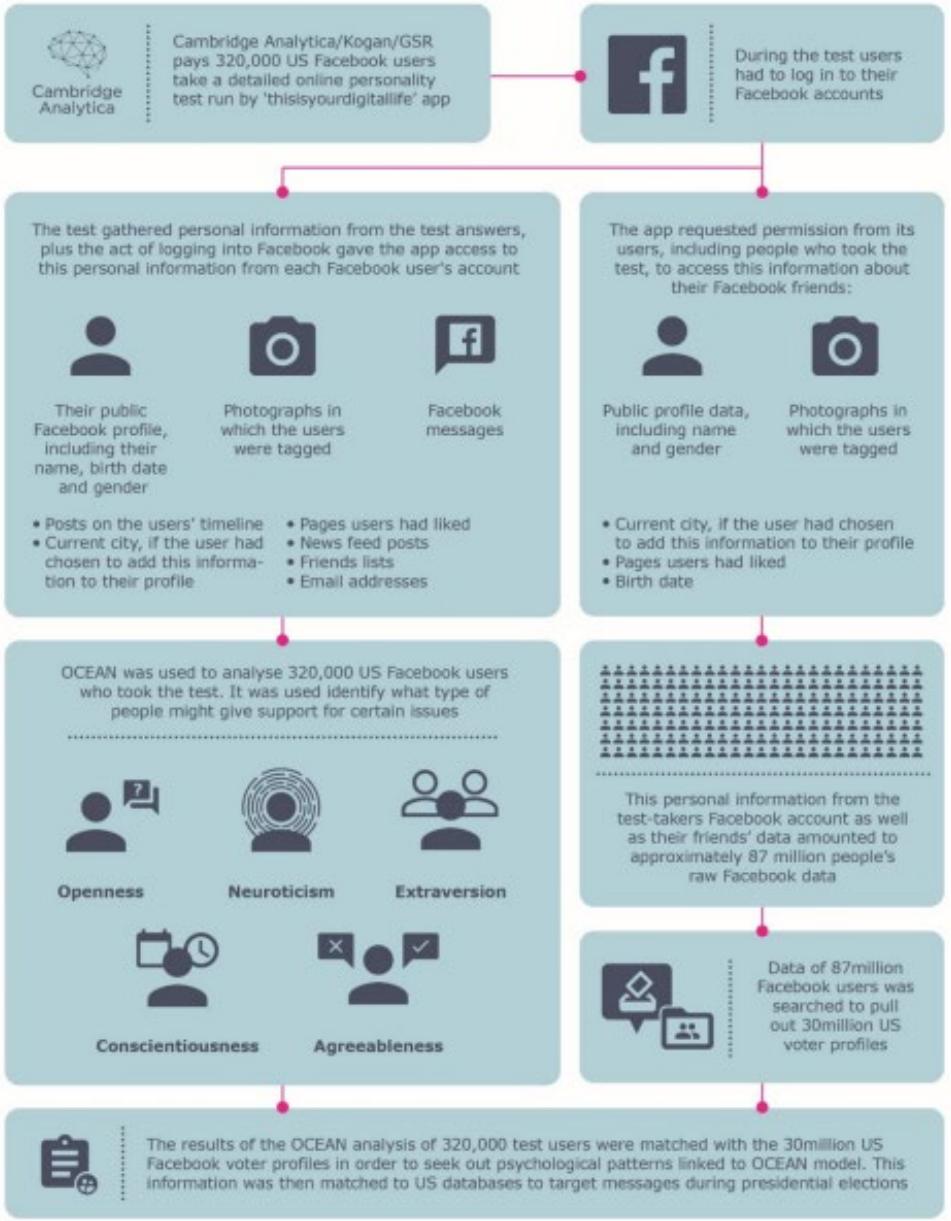
- ❑ Basic rights include:
  - ❑ Right to Know
  - ❑ Right to Delete
  - ❑ Right to Opt Out
  - ❑ Right to Opt In for Minors
  - ❑ Right to Limit the Use and Sharing of Sensitive Personal Information
  - ❑ Right to Not Be Discriminated Against for Exercising CCPA Rights
- ❑ Exemptions
  - ❑ Law Enforcement
  - ❑ Deidentified and Aggregate Data
  - ❑ Personal Information or Practices Covered Under Other Law (e.g., HIPPA, GLBA)

TOPIC	DESCRIPTION/SOURCES
CPRA	**California Privacy Rights Act**

Discussion	❑ California Privacy Rights Act (substantively effective 2023)
	❑ Sensitive personal information
	  ❑ Special notices
	  ❑ “Limit The Use Of My Sensitive Personal Information” link (subject to exemptions)
	❑ Right to correction
	❑ Automated decision making (opt-out/access)
	❑ Audit obligations
	❑ Data portability
	❑ Data minimization
	❑ Storage limitation

Case Study

- UK Information Commissioners Office
- Investigation into the use of data analytics in political campaigns
- Page 17



"OCEAN" refers to how the test calculates performance on a measure of five personality traits: Openness, Conscientiousness, Extroversion, Agreeableness, and Neuroticism.

TOPIC	DESCRIPTION/SOURCES
Case Study	**Facebook/Cambridge Analytica**
Discussion	❑ What are the implications of Facebook's business when it comes to managing the operational risks associated with users' privacy? ❑ Using the general privacy principles, how well did Facebook manage risks associated with users' privacy? ❑ What should Facebook do to achieve the right balance between privacy profits? ❑ Assess the Facebook case from an ethical perspective focusing on fairness and justice and transparency and autonomy.

TOPIC	DESCRIPTION/SOURCES
Governance	**An Introduction to Privacy For Technology Professionals,** Editor, Travis D. Breaux **Cybersecurity Fundamentals, Study Guide, 3rd Edition,** ISACA

Discussion

- ❑ Governance ensures that
  - ❑ Stakeholder needs are evaluated to determine balanced, agreed on business objectives
  - ❑ Direction is set through prioritization and decision making
  - ❑ Performance and compliance are monitored against direction and objectives
- ❑ Responsibility of Board
  - ❑ Duty to protect assets and operations
  - ❑ Set strategy and risk appetite
    - ❑ "Strategy is the organization's plan to achieve its mission and vision and apply its core values to drive performance and value."*
    - ❑ Risk appetite is "the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value"*
  - ❑ Ensure robust/effective governance processes

Markkula Center for Applied Ethics at Santa Clara University: Board Ethical Responsibilities

- Health of ethical culture
- Ethics of strategy
- Monitor ethical risks to business
- Monitor ethical risks of leadership
- Verify that ethical processes are strong

* Frank Martens and Dr. Larry Rittenberg, "Using Risk Appetite to Thrive in a Changing World," COSO (May 2020)

TOPIC	DESCRIPTION/SOURCES
Governance	**An Introduction to Privacy For Technology Professionals,** Editor, Travis D. Breaux **Cybersecurity Fundamentals, Study Guide, 3rd Edition,** ISACA

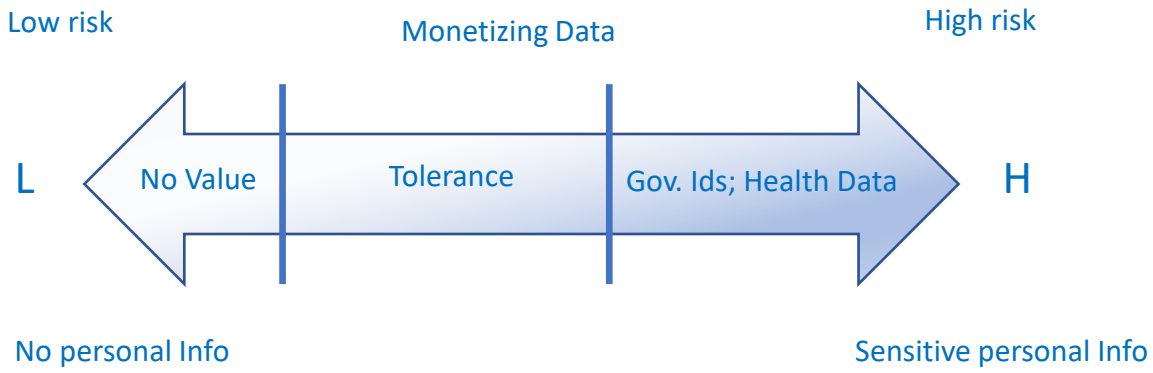
Discussion

- ❑ Management plans, builds, executes and monitors activities
- ❑ Requires formal structure
  - ❑ Governance (strategy, polices and procedures)
  - ❑ Risk (processes to identify, assess and respond to risk)
  - ❑ Compliance (processes to demonstrate adherence)
- ❑ Key considerations/issues
  - ❑ Working with multiple stakeholders across domains
  - ❑ Translation between boundaries
  - ❑ Embedding throughout organization

TOPIC	DESCRIPTION/SOURCES
Risk	**An Introduction to Privacy For Technology Professionals,** Editor, Travis D. Breaux **Cybersecurity Fundamentals, Study Guide, 3rd Edition,** ISACA

Discussion

- Balance risk and reward
  - Identify, assess and respond (controls)
  - Informed and deliberate risk taking
- Risk appetite
- Risk tolerance
- Addressing risks
  - Accept
  - Mitigate
  - Shift
  - Avoid
- Residual risk
- Risk appetite statement
  - "Data is an important asset we possess and to the extent we can monetize our data we are willing to accept moderate risks, provided it does not jeopardize our brand and reputation."
- Risk tolerance



TOPIC	DESCRIPTION/SOURCES
Compliance	**An Introduction to Privacy For Technology Professionals,** Editor, Travis D. Breaux **Cybersecurity Fundamentals, Study Guide, 3rd Edition,** ISACA

Discussion

- ❑ Compliance typically means adherence to requirements (e.g., policies, procedures, etc.)
  - ❑ Examination of controls
    - ❑ Mapping/rationalization
  - ❑ Ownership/responsibility
  - ❑ Demonstrate/Validate
- ❑ Reasonable assurance with respect to the effectiveness of controls
  - ❑ Performed by resources that are
    - ❑ Objective/independent
    - ❑ Exhibit professional skepticism
  - ❑ Risk based
  - ❑ Follow defined processes
  - ❑ Supported by tools/technology
- ❑ Auditable (external/internal)
  - ❑ Measurable
  - ❑ Transparent
  - ❑ Access

	Control Function			
		Preventative	Detective	Corrective
Control Type	Physical	Locks, access cards	CCTV	Replace access cards
	Technical	MFA	IDS	Patching, quarantine
	Administrative	Least privilege policy,	Review of access rights	Incident response plan

TOPIC	DESCRIPTION/SOURCES
Case Study	**Perfect Grocery**

- ❑ What governance problems do you see? How would you improve governance?
- ❑ What risk management problems do you see? How would you improve risk management?
- ❑ What compliance problems do you see? How would you improve compliance?

Discussion

TOPIC	DESCRIPTION/SOURCES
Model Risk	SR 11-17: Guidance on Model Risk Management, Board of Governors of the Federal Reserve System
Discussion	❑ Governance ❑ Board ultimate responsibility ❑ Senior management ❑ Adequate policies and procedures ❑ Ensuring compliance ❑ Assigning competent staff ❑ Ensuring effective challenge ❑ Reviewing validation and internal audit findings ❑ Taking prompt remedial action when necessary ❑ Formalize model risk management activities ❑ Policies and the procedures ❑ Testing and analysis ❑ Established targets/tolerances ❑ Prioritization, scope, and frequency of validation activities ❑ Identify roles and assign responsibilities ❑ Expertise, authority, reporting lines, and continuity ❑ Ownership, controls, and compliance ❑ Role of internal audit function ❑ Importance of inventory and adequate documentation

TOPIC	DESCRIPTION/SOURCES
Model Risk	SR 11-17: Guidance on Model Risk Management, Board of Governors of the Federal Reserve System

Discussion

- ❑ Processes through lifecycle (model development, implementation, and use)
  - ❑ Purpose aligned with intended use
  - ❑ Assessment of data quality and relevance
  - ❑ Continuous testing to ensure the model is performing as intended
- ❑ Risks
  - ❑ Adverse consequences
  - ❑ Fundamental errors
  - ❑ Incorrect or inappropriate use
- ❑ Managing risk
  - ❑ Effective challenge
  - ❑ Limits on model use
  - ❑ Monitoring model performance
  - ❑ Adjusting or revising models over time

TOPIC	DESCRIPTION/SOURCES
Model Risk	SR 11-7: Guidance on Model Risk Management, Board of Governors of the Federal Reserve System

Discussion

- ❑ Compliance and Validation
  - ❑ Processes to verify that models are performing as expected
    - ❑ Design objectives
    - ❑ Business uses
  - ❑ Independent
    - ❑ From model development and use
    - ❑ Degree of skepticism
  - ❑ Explicit authority to challenge developers and users
  - ❑ Three core elements
    - ❑ Evaluation of conceptual soundness
    - ❑ Ongoing monitoring
    - ❑ Outcome analysis

TOPIC	DESCRIPTION/SOURCES
Midterm	How are you going to approach the midterm?

Discussion

Focus	Facts	Do any cases help?
Ethics (Material Life Interest)	Key Facts	Fred & Tamara
❑ Security & Privacy	List them	Williams vs Detroit
❑ Fairness & Justice	Organize them	OK Cupid
❑ Transparency & Autonomy		Facebook Contagion
❑ Deceptive & Unfair		Zoom
Security		Facebook
Privacy		RealPage
Governance, Risk & Compliance		Perfect Grocery