Turn ethical frameworks

Regulations
A regulation is a set of stipulations or rules made by a legislative elected body of Representatives in consultation with subject matter experts. Regulations have legal weight and are enforceable under the laws of the land. Not the same as an ethical framework. An ethical framework is instead a set of principles and values that can be used to formulate and inform regulations. They are not enforcible in and of themselves

Treaty 108
    Council of Europe 1981. Right to privacy data

The Code of Fair Information Practices regulation
    Notice and Awareness, Choice and Consent, Access and Participation, Integrity and Security, Enforcement and Redress

OECD Privacy Guidelines
    Organization for Economic Co-operation and Development
    Collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability

GDPR stands for general data protection regulation
    Collection of personal data, processing personal data, right to be forgotten, right to object to automated decisions, black box concerns

CCPA stands for the California Consumer Privacy Act
    who was gathering personal data, for what purpose, who that might be exposed to, to decline the sale of personal data, to gain access to any data held about them, and to request that a business delete any personal information that they may hold. It also includes stipulations to avoid being discriminated against for exercising their privacy rights

PIPEDA stands for the Personal Information Protection and Electronic Documents Act
    Why data is used, limits use to stated purpose, who protects data, right to request updates, organizations must obtain consent, policies must be clear and accessible, lawful collection of data

POPI stands for protection of personal information
    South African privacy landscape
    accountability, processing limitations, purpose specifications, further processing limitations, information quality, openness, security safeguards, and data subject participation

LGPD stands for Lei Geral de Proteção de Dados or the Brazilian General Data Protection Act

- Cross border jurisdiction, privacy principles from GDPR, Risk based approach, data portability rights, rights to erase information, data transfer restrictions, mandatory breach notification

COPPA stands for the Children's Online Privacy Protection Act

- Privacy protections for personal information about minors, guidelines for orgs that interact with minors, consent issues, vulnerable to deceptive practices and data abuse

Algorithmic Accountability Act

- Fairness in computer models, removal of biases

FERPA stands for Family Educational Rights and Privacy Act

- Access by public entities, access by parents, amendment of records, disclosure of records

BIPA stands for Biometric Information Privacy Act

- Org requirements to obtain consent for data use, destroy biometric information, securely store biometric information

Standards and Best Practices

A standard is a mutually agreed upon set of rules or guidelines that are created by sets of generally industry players. A regulation has the backing of legal authority and is directly enforceable by the legal system of a territory

Standards drive inclusion of ethics, support privacy by design, support security by design

PCI DSS stands for payment card industry data security standard

- Secure networks, protect cardholder data, vulnerability management, access control, monitor and test networks, maintain policy

NIST stands for the National Institute of Standards and Technology

- 800.53: Guidelines for federal agencies, manage info security systems, protect privacy data
- Cybersecurity framework (CSF): Guidance for private sector, access security activities, improve security activities, manage security outcomes

CIS CSC stands for Center for Internet Security Critical Security Controls

- Cyber offense informs defense, counter threats, use automation, use consensus, privacy and security of data, requirements for IT pros

International Organization for Standardization (ISO)

27001: Information Security Management

Risk-based approach, security management system, certification for compliance

27017: Cloud security

Security for CSP, who is responsible, removal or return of assets, protection of environments

27018: Information Technology Security Techniques

CSPs who process PII, common security categories, common controls

National Institute of Standards and Technology Internal Report (NISTIR) 8288

IoT devices and the physical word, IoT devices and configuration, IoT devices and security needs

Mitre attack framework

Attack methods, threat intelligence, threat profiles

IEEE is the Institute for Electrical and Electronic Engineers

P7000 series: Ethical values in development, traceability of ethical values, all size of Orgs

Detect and Mitigate Ethical Risks

Risks and Ethics

Identification, analysis, mitigation

Types of ethical risks

- Privacy
- Accountability
- Transparency and explainability
- Fairness and non-discrimination
- Safety and security

Basic Stats

- Distributions
    - Frequency of all values in a variable\
- Central tendency
    - Mean: simple average of all relevant numbers
    - Median: true middle of all values
        - In a normal distribution the mean is the same as the median

    - Mode: most frequent number
        - In a normal distribution, the is the same as the median and mean

- Variance and Standard Deviation
    - Variance: how far the data is from the mean
    - Standard deviation: square root of variance
        - In a normal distribution, around 68% of all data examples, are within one standard deviation, of the mean in both directions
        - Around 95% of the sample is within two standard deviations of the mean
        - Around 99.7% of the sample is within three standard deviations of the mean

- Skewedness and Kurtosis
    - Skewedness
        - Left or positive skewedness
            - Mode < median < mean
        - Right or negative skewedness
            - Mode > median > mean
    - Kurtosis
        - Mesokurtic
            - Normal distribution
        - Leptokurtic
            - Distribution bunched in the center
            - Skinner tails
            - Indicates outliers
        - Platykurtic
            - Distribution of long, broad tails
            - Lack of outliers

- Correlation
    - The association between two variables

Evaluation Metrics

- Machine learning
    - Supervise learning
        - Classification
            - Place new data in a category
        - Regression
            - Predict the value of a numerical target
    - Unsupervised learning
        - Clustering
        - Dimensionality reduction

        - Remove unwanted attributes
- Classification
    - True positive
    - True negative
    - False positive
    - False negative
    - Positive predictive value = TP/TP+FP
    - Negative predictive value = TN / TN + FN
- Reliability
    - Overfitting is when the model is tuned to predict the examples in the training set too well
    - Underfitting occurs when a predictive model is too simple to capture the underlying patterns in the data, resulting in poor performance on both the training and test datasets. This happens when the model fails to learn the complexity of the data, leading to high bias and low variance.
    - The holdout method is a simple and widely used technique for evaluating the performance of a machine learning model by splitting the data into two separate sets: one for training and one for testing. This approach helps estimate how well the model will generalize to new, unseen data

- Goodhart's Law
    - If you focus too much on achieving good results for a specific measurement, then the measurement itself becomes the goal

Detect and Mitigate Ethical Risks

Privacy: Choosing not to share info, refers to individuals or groups

First-party data: is any data that you have collected directly from customers or any other audience that you work with

Third-party data: is usually collected from one or more sources where you, the collector, do not have a direct relationship with the users that the data is about.

Whenever data is used in accordance with its purpose, it is referred to as the primary use of data. Any use of data that falls outside of this intent is referred to as secondary use of data.

Anonymization removes all ability to identify a subject
Pseudonymization disguises one's identity, using a false name or other identifier

Regular encryption, you use an algorithm plus a key to encode a message. This makes the message incomprehensible. The encoded message is called ciphertext
Asymmetric encryption: In this approach, there are two distinct keys; the public key and

private key. The keys may be different, but they are mathematically linked

Homomorphic encryption enables you to process and manipulate data while it's still Encrypted

- Partially homomorphic encryption enables you to perform only certain types of mathematical operations on encrypted data
- Somewhat homomorphic encryption enables you to perform up to two kinds of operations from a limited subset
- Fully homomorphic encryption enables you to perform an unlimited number of operations of any type.

Bias

- Implicit bias
    - An inclination to what a group of people, or a prejudice against a group of people that is unconscious to the person with the buyers
- Sampling bias
    - Sample data from the population does not adequately reflect the distribution of the population
- Reinforcement bias
    - Repeated sampling of past events can lead to poor judgment
- Temporal bias
    - We may believe something at some point in time, but fail to account for how factors change over time

STEEPV

- Social, technological, economic, environmental, political, and values
- The purpose of such an analysis is to understand the influence of market factors on business decisions and operations