- Edward doming → doing it right when nobody is looking.
- ethical principles for data → respect for people,Justice, beneficence (do not harm,maximize benefits)
- United StatesDepartment of homeland security uses Belmont's principle (adds respect for law and public interest)

• European Data protection supervisor (future oriented, accountability,privacy conscious, empowered individuals)

- policies and laws try to codify ethics
- Samuel warren and Louis Brandeis 1890 -> introduced privacy as a human right
- US privacy act of 1974 = privacy is codified as a constitutional law
- Second World War led to push for human rights movement

> In 1980, the Organization for Economic Co-operation and Development (OECD) established Guidelines and Principles for Fair Information Processing that became the basis for the European Union's data protection laws.
>
> OECD's eight core principles, the Fair Information Processing Standards, are intended to ensure that personal data is processed in a manner that respects individuals' right to privacy. They include: limitations on data collection; an expectation that data will be of high quality; the requirement that when data is collected, it is done for a specific purpose; limitations on data usage; security safeguards; an expectation of openness and transparency; the right of an individual to challenge the accuracy of data related to himself or herself; and accountability for organizations to follow the guidelines.

- GDPR came out in 2016.
-

GDPR Principle	Description of Principle
Fairness, Lawfulness, Transparency	Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
Purpose Limitation	Personal data must be collected for specified, explicit, and legitimate purposes, and not processed in a manner that is incompatible with those purposes.
Data Minimization	Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data must be accurate, and where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay.
Storage Limitation	Data must be kept in a form that permits identification of data subjects [individuals] for no longer than is necessary for the purposes for which the personal data are processed.
Integrity and Confidentiality	Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
Accountability	Data Controllers shall be responsible for, and be able to demonstrate compliance with [these principles].

- Canada privacy obligation

Table 2 Canadian Privacy Statutory Obligations

PIPEDA Principle	Description of Principle
Accountability	An organization is responsible for personal information under its control and must designate an individual to be accountable for the organization's compliance with the principle.
Identifying Purposes	An organization must identify the purposes for which personal information is collected at or before the time the information is collected.
Consent	An organization must obtain the knowledge and consent of the individual for the collection, use, or disclosure of personal information, except where inappropriate.
Limiting Collection, Use, Disclosure, and Retention	The collection of personal information must be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
Accuracy	Personal information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
Safeguards	Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
Openness	An organization must make specific information about its policies and practices relating to the management of their personal information readily available to individuals.
Individual Access	Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Compliance Challenges	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

- US federal trade commission report recommendations:do not track option, data management throughout project lifecycle,privacy by design,consumer education
- even multi national companies have legal limits to sharing data.
- online Data in ethical context:ownership of data, the right to be forgotten, identity,
- Data can be used to misrepresent facts. Possible techniques:removing or only showing data of certain time,misleading visualizations,unclear indexes, irregularities comparisons,
- Bias in data collection, hunch and search, biased analysis, biased sampling and cultural biases
- precautions should be taken
- ethical ways of handling data: understanding data lineage,KPIs for data quality,proper metadata

- aggregating data can also help remove PII information
- Data should be classified based on sensitivity
- to establish an ethical data culture: current state of data ethics within an org should be identified,how data is shared should be understood.
- Data ethics principle should revolve around practices and potential risks.
- audit of data handling should be conducted
- A roadmap around data handling should be created with pre-defined values,compliance framework, risk assessments,and training plan.
- Data ethics and governance: oversight falls on the legal team,data governance provides with strategies and policies
- Data governance professionals should also review requested changes by analysts, data scientists, and data engineers.