Privacy and Data Security

1) What is privacy?

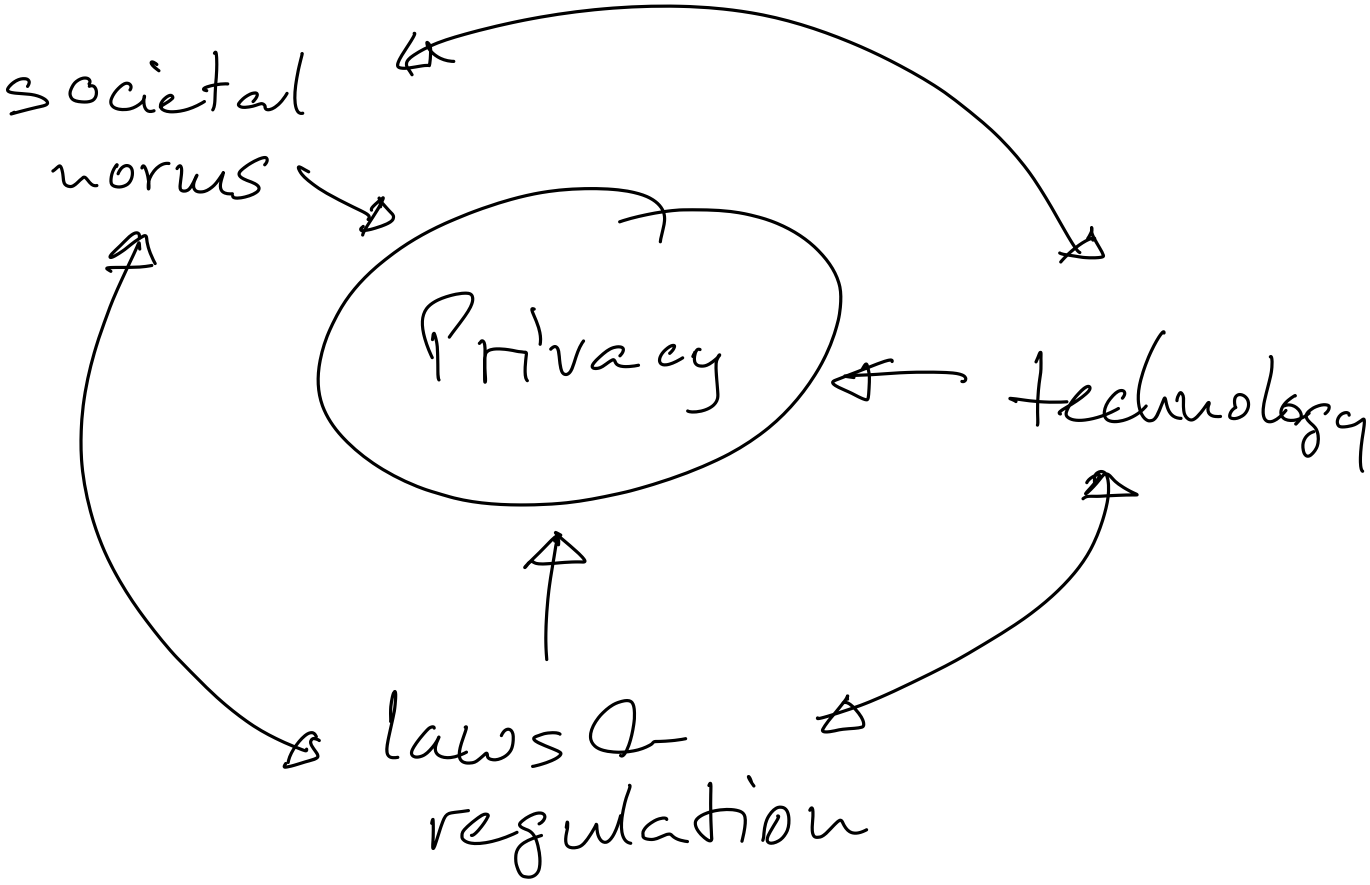
An answer using

Contextual Integrity (CI)

- Privacy concerns information about people, individual or groups of them

- Privacy is about the ability of an individual to be hidden or of hiding information about oneself

- Privacy allows to release information selectively and coupled to a purpose



Incomplete notions of privacy

- Privacy means that <u>no</u> info. flows to 3rd parties (some is desired)

- Divide data into "private" and "public" data (it depends on the context)

- Privacy means the right to control <u>all</u> information about oneself

⟹ the importance of <u>context</u>

Def: Context means a social domain, setting, or interaction in which information is transferred

synonyms:

- sphere
- field
- event

Ex. university, family, health care ...

Elements to define a context

- people
- relationships and trust
- traditions
- values

- purposes and goals
- time and place
- laws

Def: An informational norm is characterized by five elements and concerns an information flow (defined by these elements):

- sender
- recipient
- subject

} "actors" of this info. flow

- information type (attributes)
- transmission principle (circumstances of the info. flow, motivation, required by law..)

There are two kinds of this norm:

Normative: An information norm holds in a context and describes the expectations of the subject, how they *should* behave.

Descriptive: An information norm describes the *practice* followed by the actors.

Def: Privacy as *Contextual Integrity* means that an information flow respects the informational norm of its context.

Ex:

- * Blood pressure and heart rate data

  ... from patient to doctor

  ... from smart watch to cloud provider

  ... from smartwatch to healthcare organisation

  are all different contexts.

- * Phone books in 1990 and 2020

- * Listings of car license plates in 1980 and 2020