COM-402 exercises 2025, session 12: Privacy: definitions and properties

Exercise 12.1

- Are the following statements true or false? Justify.
  1. It is possible to deploy surveillance only on end-users of systems.
  2. Privacy as control ensures that only the minimal amount of information is provided to the service.
  3. Fine-grained accountability and auditability make it difficult to implement systems with strong privacy protection.

Exercise 12.2

- Aggregation is a privacy-protection technique consisting in regrouping data before processing (e.g.: by binning and taking the mean of the data instead of the data itself). Discuss what kind of privacy this is from the point of view of the paradigms (confidentiality, control, practice) or adversary (social, institutional, anti-surveillance) when:
  1. the aggregation is made locally by the user before releasing her data.
  2. the aggregation by all users is made by a third party

Exercise 12.3

- Consider a privacy-preserving forum to ask questions in the class. To provide privacy, when a student posts a question, instead of publishing the student's name, it chooses uniformly at random another name in the class that starts by the same letter. For the following students, discuss what is the privacy this mechanism gives in terms of error (probability) the professor will face when guessing who wrote a question. Who has more protection?
  - Charlie, who is in the class with Celia, Carla, Constantin, and Colin.
  - Louisa, who is in the class with Lorenz, Lex, and other two Louisas