Stockholm, 2014

Some lines of research

Vicenç Torra

Högskolan i Skövde

Outline

- Data privacy (perturbative, data-driven methods)
- Other research topics

Data Privacy

Data privacy. Broad area

neighbouring: databases, statistics, official statistics (SDC), data mining (PPDM), communications, security, cryptography, . . .

Dimensions. Classification of the methods according to

- Whose privacy is being sought (respondent, holder, user)
- The computations to be done (known, unknown)
- The number of data sources (one, multiple)

Data Privacy

Data privacy. Broad area

neighbouring: databases, statistics, official statistics (SDC), data mining (PPDM), communications, security, cryptography, . . .

Dimensions. Classification of the methods according to

- Whose privacy is being sought (respondent, holder, ~~user~~)
- The computations to be done (~~known~~, unknown)
- The number of data sources (one, ~~multiple~~)

Data Privacy

Data privacy. Broad area

neighbouring: databases, statistics, official statistics (SDC), data mining (PPDM), communications, security, cryptography, . . .

Dimensions. Classification of the methods according to

- Whose privacy is being sought (respondent, holder, ~~user~~)
- The computations to be done (~~known~~, unknown)
- The number of data sources (one, ~~multiple~~)

That is, data-driven (perturbative) methods

Data Privacy

Data-driven methods.

- Data X needs to be transferred to third parties for analysis

Data Privacy

Data-driven methods.

- Data X needs to be transferred to third parties for analysis

Generic approach.

- Start with the original data X
- Compute $\rho(X)$ (perturbation)
  - E.g., $\rho(X) = X + \epsilon$
- Publish $\rho(X)$

Data Privacy

Data-driven methods.

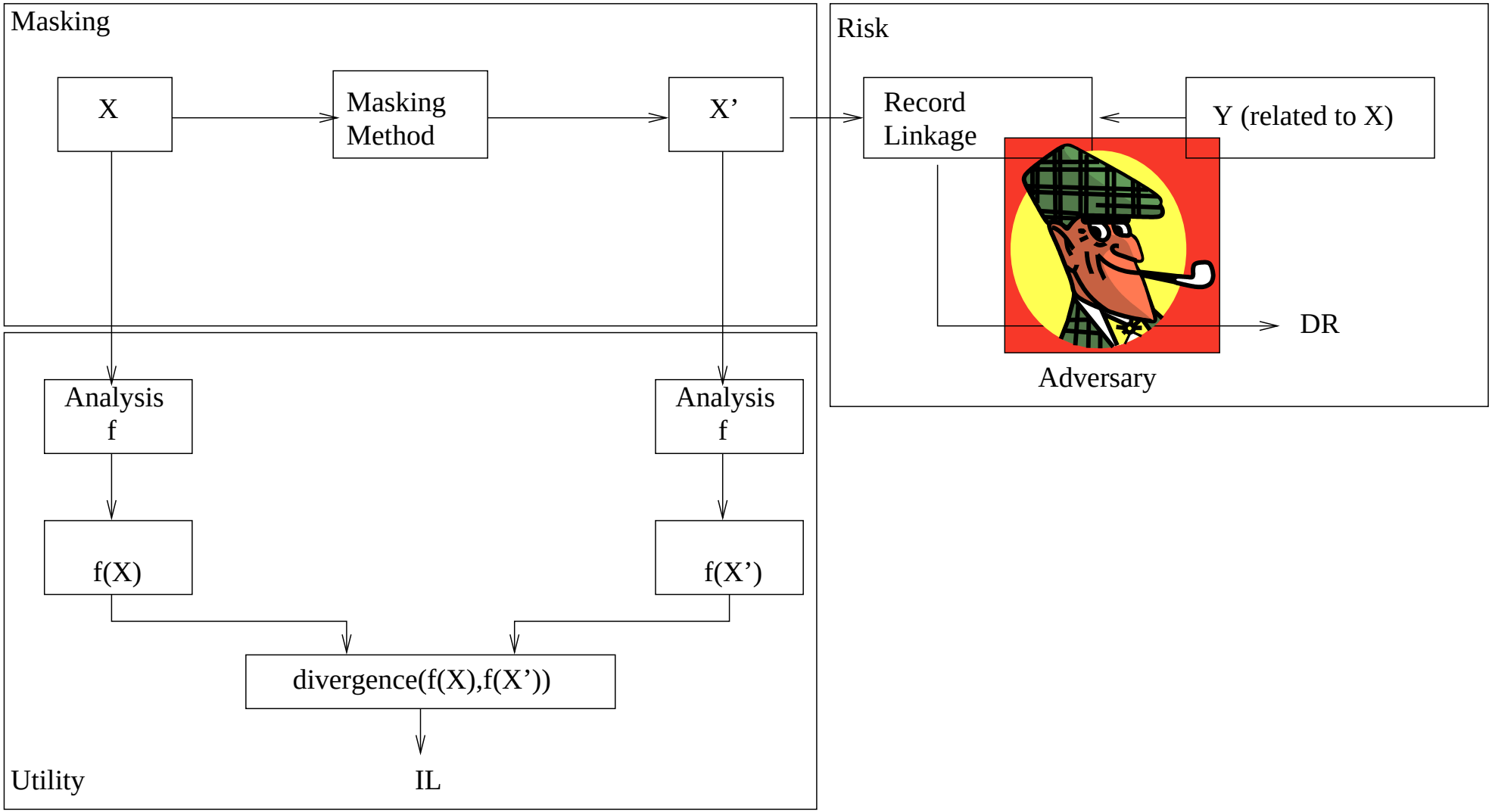
- Data X needs to be transferred to third parties for analysis
- Publish $\rho(X)$

Issues.

- How to compute $\rho(X)$ (data masking methods)
- How to assess the utility of $\rho(X)$ (information loss measures)
- How to assess the risk of $\rho(X)$ (disclosure risk measures)

Data Privacy

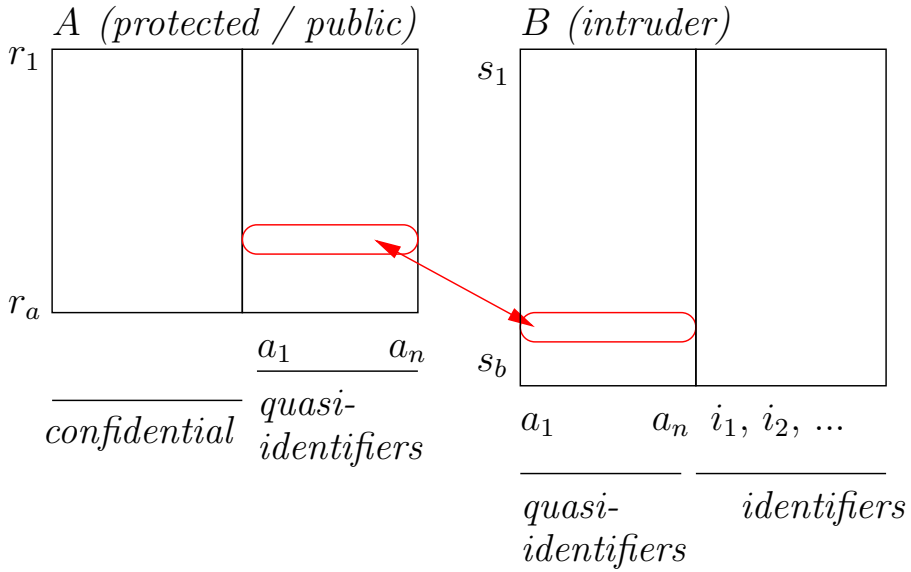
Data-driven methods.



Data Privacy

Data privacy: Disclosure risk measures

- A Boolean condition
  - k-Anonymity
  - Differential privacy
- A measurable condition (e.g., probability of reidentification)
  - Risk as a proportion of reidentification
  - Attack: an adversary links his database with the released file



Data Privacy

Data privacy: Disclosure risk measures

- Measurable using reidentification (tools and approaches)
  - Record linkage (database integration, data matching, . . .)
    $\rightarrow$ link intruder's and published data

Data Privacy

Data privacy: Disclosure risk measures

- Measurable using reidentification (tools and approaches)
  - Record linkage (database integration, data matching, . . .)
    $\rightarrow$ link intruder's and published data
  - Specific attacks
    $\rightarrow$ accurate risk in the case of the transparency principle
    (transparency principle: publish data + protection method)

Data Privacy

Data privacy: Disclosure risk measures

- Measurable using reidentification (tools and approaches)
  - Record linkage (database integration, data matching, . . .)
    $\rightarrow$ link intruder's and published data
  - Specific attacks
    $\rightarrow$ accurate risk in the case of the transparency principle
    (transparency principle: publish data + protection method)
  - Supervised machine learning to improve performance
    $\rightarrow$ ML to evaluate the worse case scenario
    (the intruder knows optimal parameters of a parametric distance)

Data Privacy

Data privacy: Disclosure risk measures

- Specific attacks (transparency)
  Intersection attack: $B = \cap B_i$
- Supervised machine learning to improve performance (worse case)
  Example WM-distance

$$Minimize \quad \sum_{i=1}^{N} K_i$$

$$Subject\ to:$$

$$dWM_p^2(a_i, b_j) - dWM_p^2(a_i, b_i) + CK_i > 0 \quad \forall i, j \text{ with } i \neq j$$

$$K_i \in \{0, 1\}$$

$$\sum_{i=1}^{n} p_i = 1$$

$$p_i \geq 0$$

Data Privacy

Data privacy: Masking methods (data driven masking methods)

- Data bases, files and tables
- Time series
- Search and access logs
- Documents (index, sanitization)
- Graphs and online social networks

Data Privacy

Data privacy: Information loss

- They depend on the data use f

$$IL_f(X, X') = divergence(f(X), f(X')$$

  where $X' = \rho(X)$.
- On f:
  - generic measures databases (statistics)
  - clustering and classification

Data Privacy

Data privacy: Using knowledge in data privacy

- Semantics for categorical / textual data
  Open directory project, wordnet
- Schema and metadata in the database
  Masking methods preserving constraints

Data Privacy

Data privacy. Broad area

neighbouring: databases, statistics, official statistics (SDC), data mining (PPDM), communications, security, cryptography, . . .

Dimensions. Classification of the methods according to

- Whose privacy is being sought (~~respondent~~, ~~holder~~, user)
- The computations to be done (known, ~~unknown~~)
- The number of data sources (one, ~~multiple~~)

Data Privacy

Data privacy. Broad area

neighbouring: databases, statistics, official statistics (SDC), data mining (PPDM), communications, security, cryptography, . . .

Dimensions. Classification of the methods according to

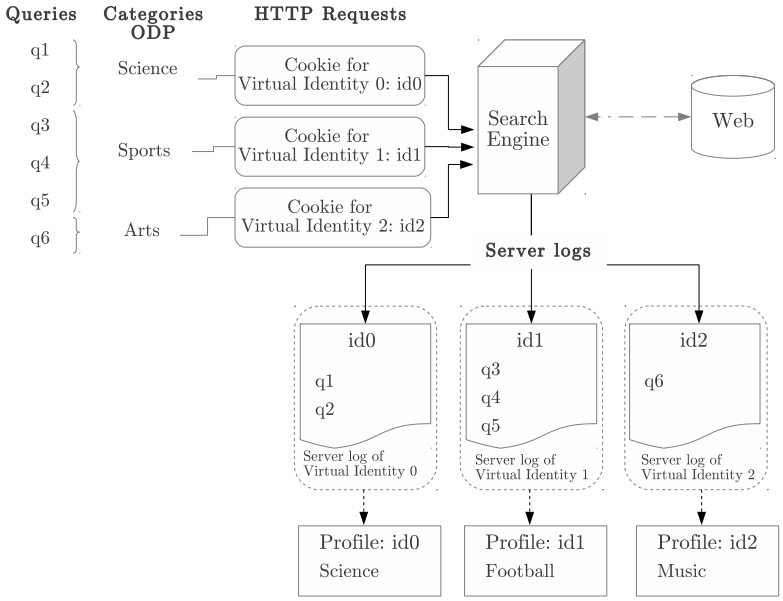
- Whose privacy is being sought (~~respondent~~, ~~holder~~, user)
- The computations to be done (known, ~~unknown~~)
- The number of data sources (one, ~~multiple~~)

That is, user-driven (perturbative)

User privacy

User privacy: agent for searching

- The user has a proactive behavior to ensure his own privacy
- Tools to help to achieve the user
- Implementation of a plug-in for firefox to protect user search logs
- Several virtual identities, distributes queries in the identities



User privacy

Data privacy: summary

Data driven	Masking	DB files, tables Time series / location Logs Documents Social networks
	Information loss	
	Disclosure risk	Formalization Worst-case Transparency
User privacy		
Knowledge		

Other research topics

Approximate reasoning in AI: data fusion/aggregation, decision making

- Aggregation functions: $f : D^N \to D$
  - Selection of functions and parameters, study of properties
- Fuzzy (non-additive) measures and integrals (Choquet and Sugeno integrals)
  - To deal with non-independent attributes
  - Theory and applications

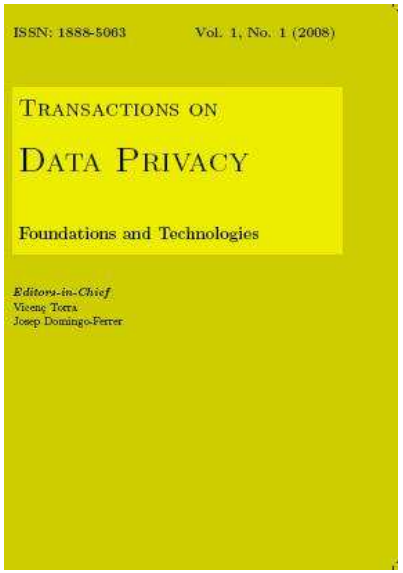
    e.g., use of Choquet integral based distance for disclosure risk assessment
- Parameter selection (optimization: e.g. quadratic programming)

Some final SPAM (I)

A journal. Transactions on data privacy

http://www.tdp.cat

- V. Torra, J. Domingo-Ferrer (editors).
- Vol. 7 (2014) completed.



Some final SPAM (II)

A conference.

12th Int. Conf. on Modeling Decisions for Artificial Intelligence
MDAI 2015, Skövde, Sweden

http://www.mdai.cat/mdai2015

- Deadline: March 24th, 2015.
- Conference: September 21-23, 2015.