

Privacy Enhancing Technologies

Claudia Diaz

K.U.Leuven ESAT/COSIC

Workshop on Privacy by Design
Brussels, June 23, 2010

Perspectives on privacy

- Popular definitions:
 - “The right to be let alone”
 - “Informational self-determination”
 - “The freedom from unreasonable constraints on the construction of one's own identity”
- Solove:
 - identifies 16 privacy threats relating to information collection, processing and dissemination, and invasion
- Data protection:
 - purpose, proportionality, consent, data subject's rights, data security obligations, ...
- Technical privacy properties:
 - Anonymity, Pseudonymity, Unlinkability, Unobservability, Plausible deniability (OTR), Location privacy...

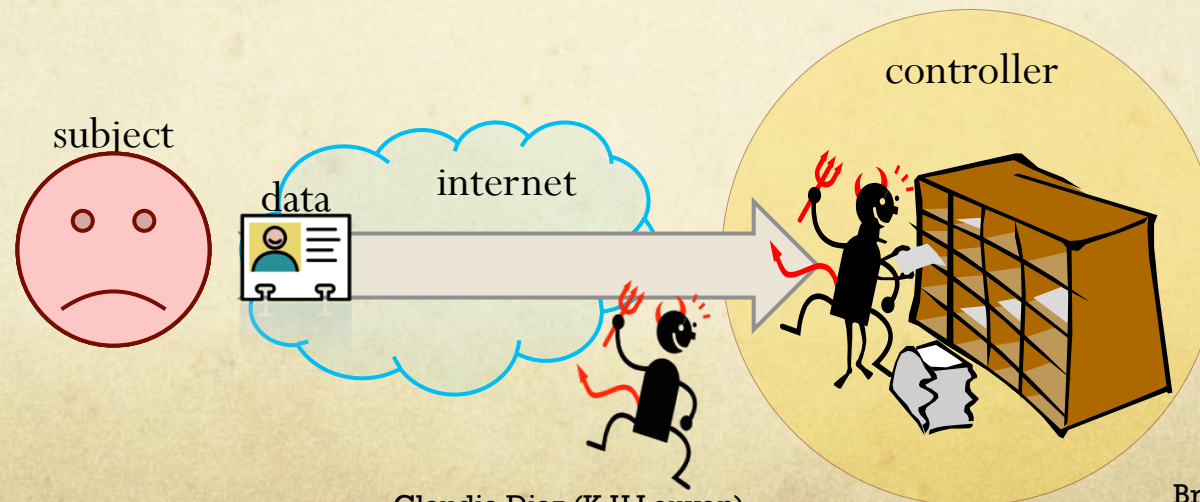
“Trust-based” or “Soft” privacy

○ System model

- Data subject provides her data
- Data controller responsible for its protection

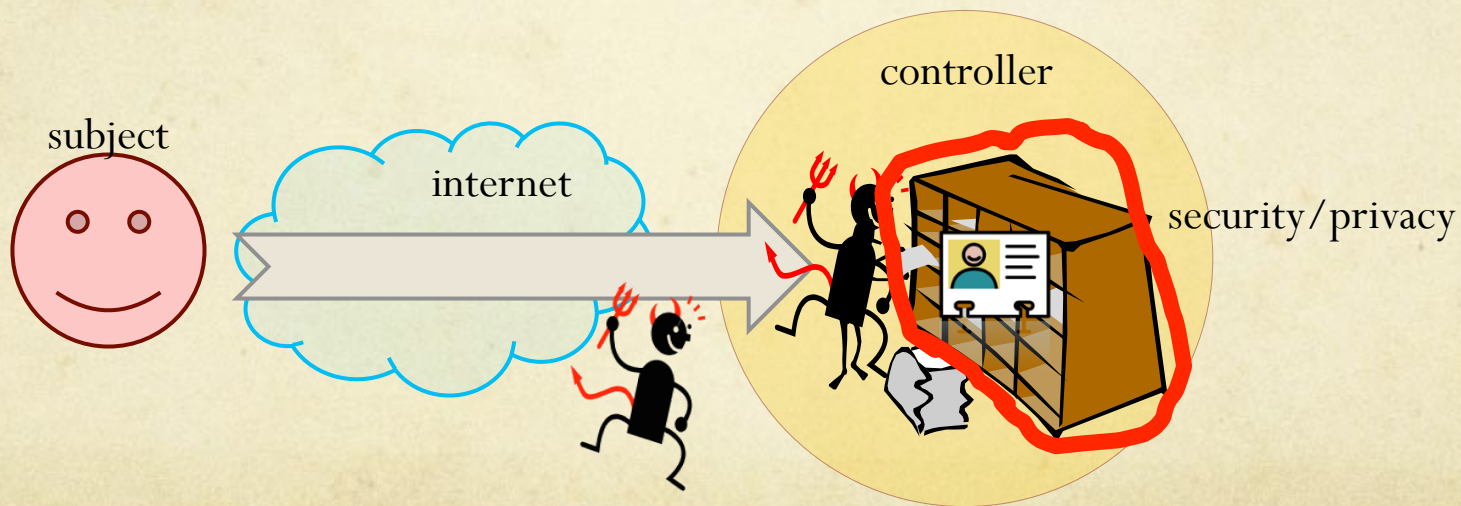
○ Threat model

- External parties, errors, malicious insider



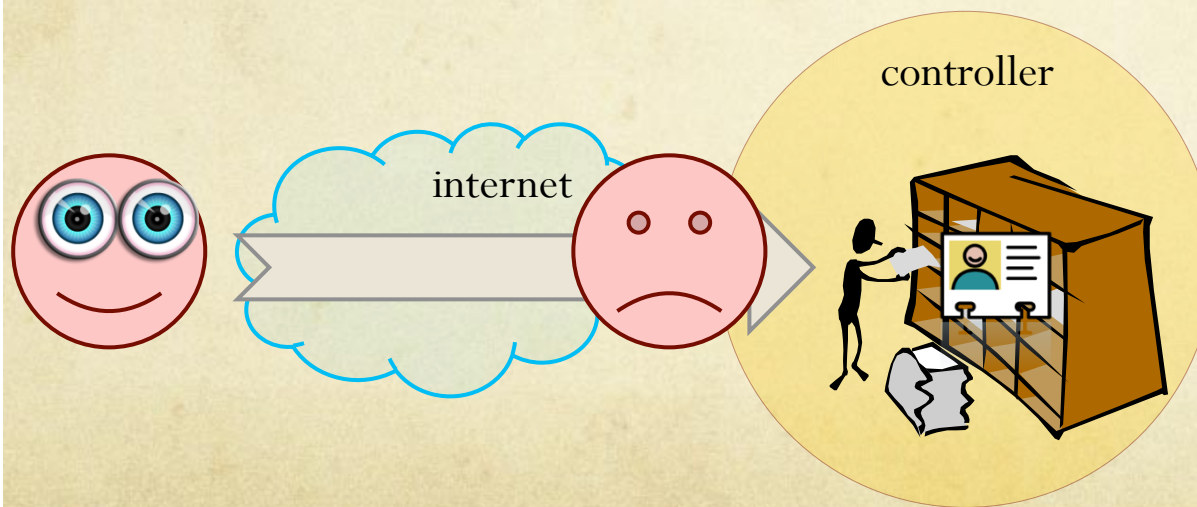
Soft privacy

- Focus on data security (for organizations)
- Policies, access control, trust, audits (liability)



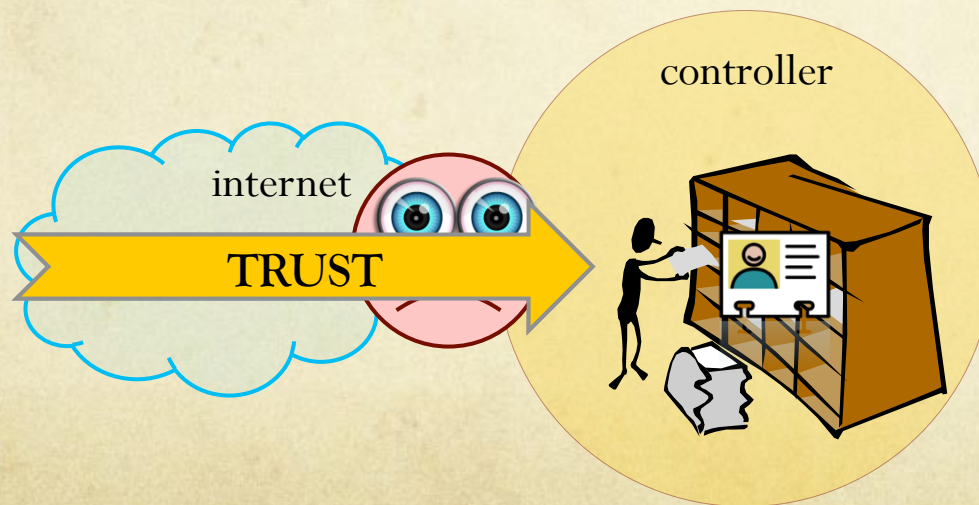
Soft privacy

- Data subject has already lost control of her data
 - In practice, very difficult for data subject to verify how her data is collected and processed



Soft privacy

- Data subject has already lost control of her data
 - In practice, very difficult for data subject to verify how her data is collected and processed
 - Need to trust data controllers (honesty, competence) and hope for the best
 - Weak enforcement, low penalties



TRUST ASSUMPTIONS?

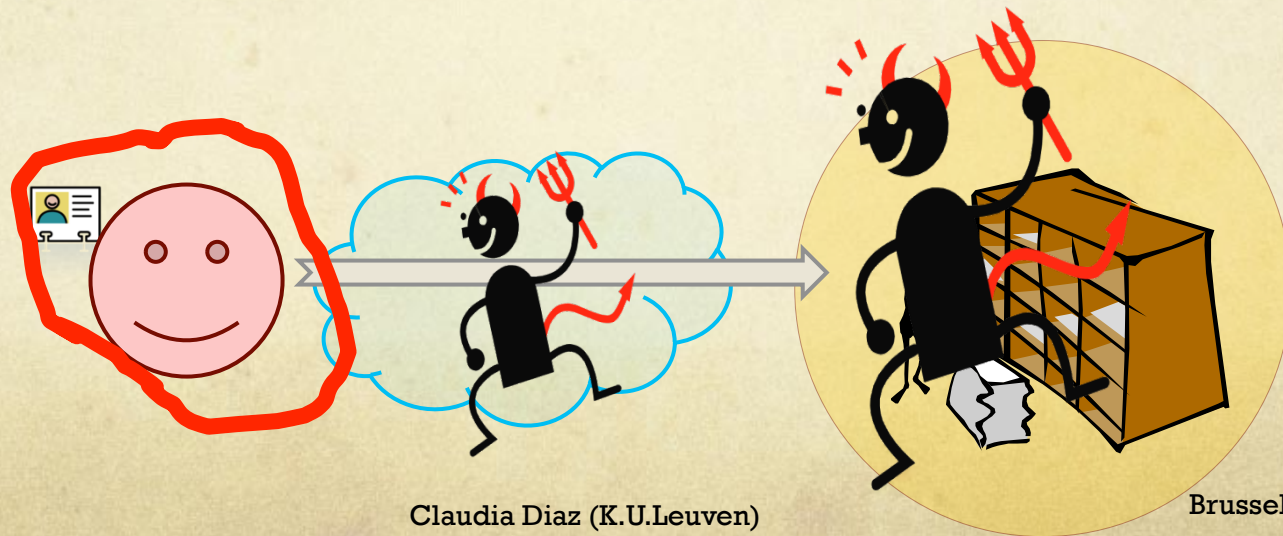
INCENTIVES?

TECHNOLOGICALLY
ENFORCED?

6

Hard privacy

- System model
 - Subject is able to access services while providing **minimal** data
- Reduce as much as possible the need to “trust” other entities



Privacy = Security Property

- Governments / Military
 - Protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations
- Companies
 - Protection of trade secrets, business strategy, internal operations, access to patents
- Individuals
 - Freedom from intrusion, profiling and manipulation, protection against crime / identity theft, control over one's information
- Shared infrastructure
 - Despite varying capabilities infrastructure is shared
 - Telecommunications, operating systems, search engines, on-line shops, software...
 - **Denying security to some, means denying it to all !**

Two main approaches

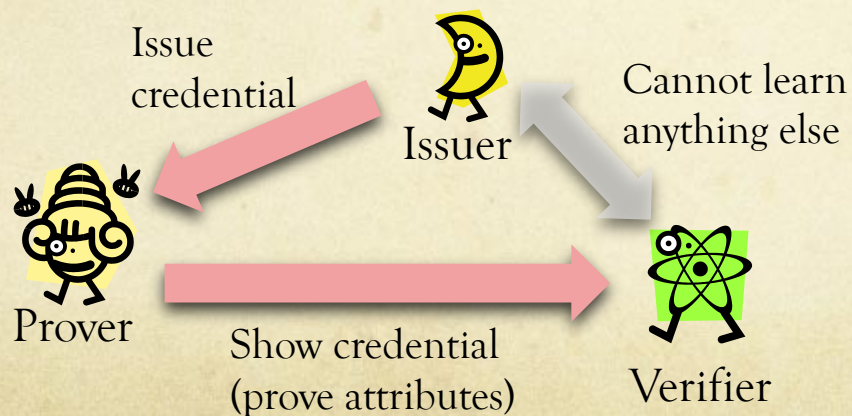
- Anonymity
 - Service provider can observe access to the service
 - Cannot observe the identity of the user
- Oblivious Transfer (OT) / Private Information Retrieval (PIR)
 - Service provider can identify user
 - Cannot observe details of the access to the service
 - Which records were accessed
 - Which search keywords were used
 - Which content was downloaded
 - ...
- All parties have assurance that the other participants in the protocol are cannot cheat

Anonymous authentication

- Are anonymity and authentication incompatible?
- Many transactions involve attribute certificates
 - ID docs: state certifies name, birth dates, address
 - Letter reference: employer certifies salary
 - Student card: university certifies student status
- Do you want to show all attributes for each transaction?
- Credential: token certifying attributes

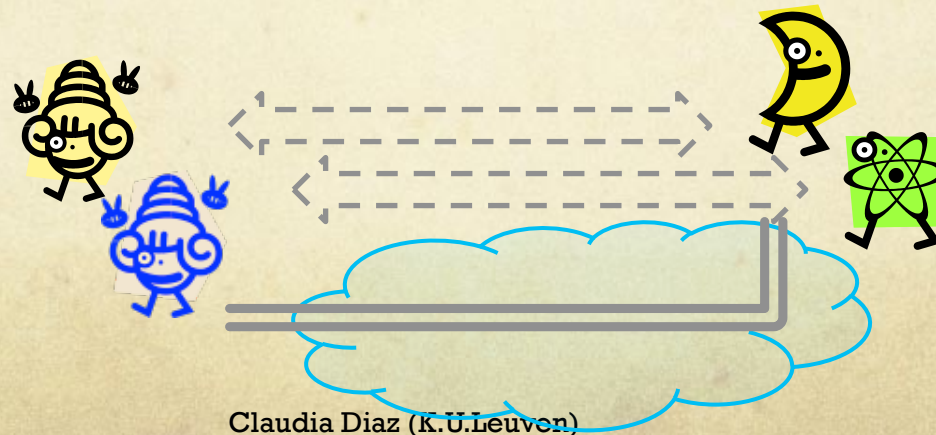
Anonymous credentials

- Properties:
 - The prover convinces the verifier that he holds a credential with (certified) attributes that satisfy some conditions:
 - Example “salary>30.000 AND contract= permanent”
 - Prover cannot lie
 - Verifier cannot infer anything else aside the formula
 - Anonymity maintained despite collusion of V & I



Protection at all layers

- Easy to defeat by “changing” abstraction layer
 - Privacy properties (e.g., anonymity) do not compose
- Example: previous protocols are useless if the adversary can link transactions based on traffic data (e.g., IP address)
- Secure and private channels: protection against traffic analysis



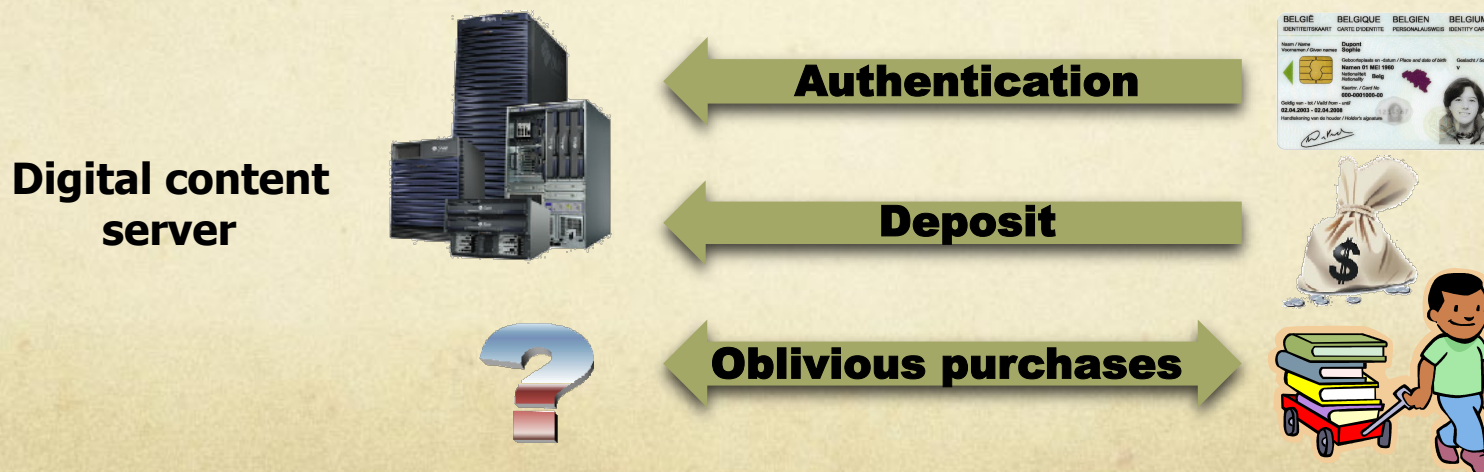
Oblivious Transfer (OT)



- A inputs two information items, B inputs the index of one of A's items
- B learns his chosen item, A learns nothing
 - A does not learn which item B has chosen;
 - B does not learn the value of the item that he did not choose
- Generalizes M instead of 2, etc.
- Example: retrieving location-based content

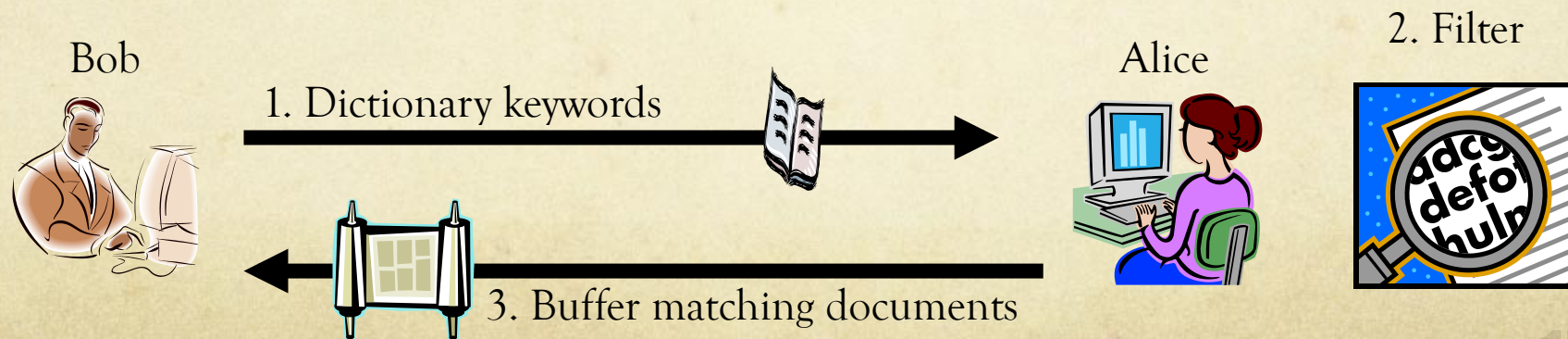
Buying digital goods (Priced Oblivious Transfer)

- Privacy of the buyer:
 - Vendor does not learn which particular item she buys
 - Vendor learns neither the amount of money paid nor the new value of the deposit ($\text{NewDeposit} = \text{OldDeposit} - \text{price}$) – only that $\text{NewDeposit} > 0$
- The vendor is assured that:
 - Buyer does not learn anything about content for which she did not pay.
 - Buyer pays the right price for the item she buys and updates the deposit correctly.



Private Search

- Alice stores documents
- Bob wants to retrieve documents matching some keywords
- Properties:
 - Bob gets documents containing the keywords
 - Alice does not learn Bob's keywords
 - Alice does not learn the results of the search



Conclusions

- Privacy is not “opposed” to security, but rather a security property
- Soft and hard privacy: two privacy paradigms
- Current privacy technologies are able to reconcile requirements that seem (intuitively) incompatible
- Privacy properties do not compose: need for taking into account multiple system layers