Privacy-preserving Smart Cities

¿utopia or reality?

Carmela Troncoso
(IMDEA Software Institute)
Smart City Expo World Congress
18th November 2015

(Big) data

(Big) data

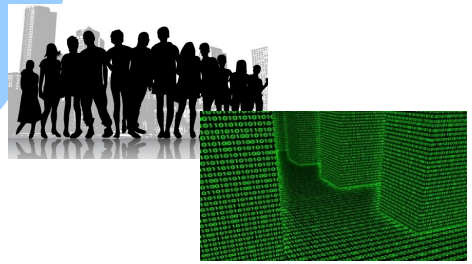
Data processing & analytics

institute IMDEA software

(Big) data

Data processing & analytics

institute IMDEA software

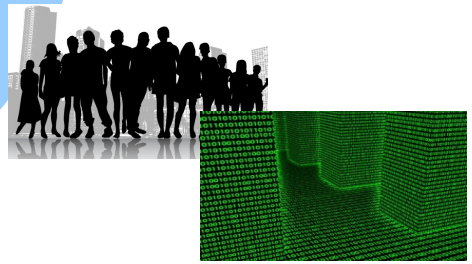


Data processing & analytics

- Whereabouts
  - Shopping
  - Religion
  - Restaurants
- Relationships
  - Friends
  - Professional
- Habits at home
- ...

(Big) Personal data

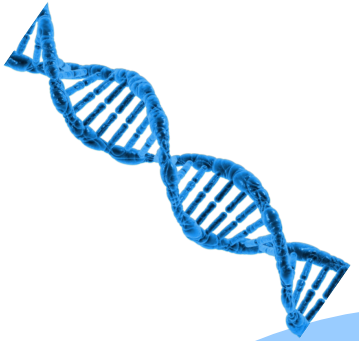
institute imdea software



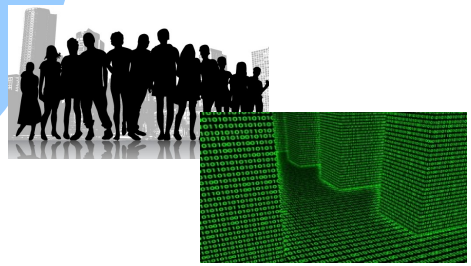
Data processing & analytics

- Whereabouts
  - Shopping
  - Religion
  - Restaurants
- Relationships
  - Friends
  - Professional
- Habits at home
- ...

(Big) Personal data

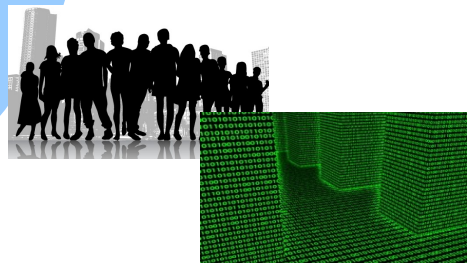


institute IMDEA software



(Big) Personal data

Data processing & analytics

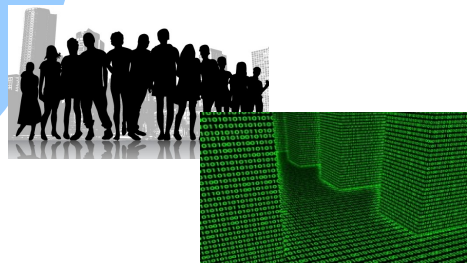


(Big) Personal data

Data processing & analytics

1) Ethical issues, public opinion
2) Legal framework – Data Protection:
   - consent
   - proportionality
   - purpose limitation

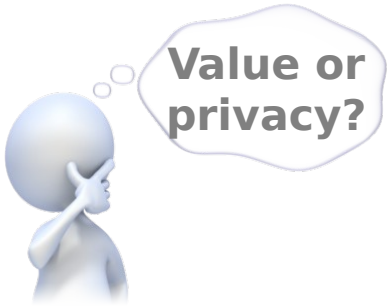
institute IMDEA software



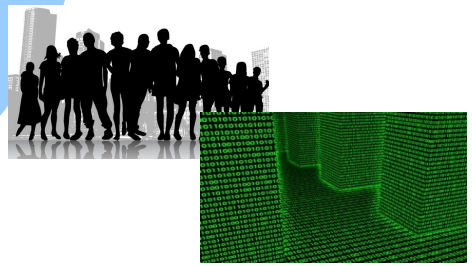
(Big) Personal data

Data processing & analytics

1) Ethical issues, public opinion
2) Legal framework – Data Protection:
   - consent
   - proportionality
   - purpose limitation



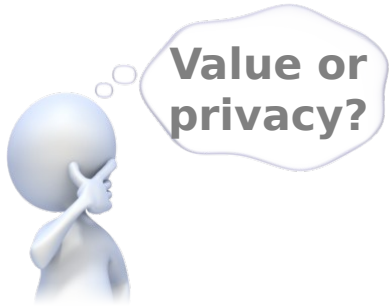
institute IMDEA software



(Big) Personal data

Data processing & analytics

1) Ethical issues, public opinion
2) Legal framework – Data Protection:
   - consent
   - proportionality
   - purpose limitation



Two technological paths to reconciliation

- Data anonymization
- Advanced cryptography (processing in the encrypted domain)

institute imdea software

Anonymization

EU legislation evolves to harder constraints Art. 29 WP's opinion on anonymization techniques

3 criteria for anonymization

1- No singling out of individuals

Metadata are unique!

- **Location**:
  - "the median size of the individual's **anonymity set in the U.S. working population is 1, 21 and 34,980**, for granularity of a census block, census track and county"
  - "if the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, **four spatio-temporal points** are enough to uniquely identify 95% of the individuals." [15 montsh, 1.5M people]"
- **Browser**: "83,6 % of browsers have unique fingerprints"
- **Demographic**: "It was found that 87 % (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}"
- **Credit card transactions**: "need four purchases to identify an individual on the anonymizied credit card records, or three purchases if the prices are known" [3 months 1.1 million people]

institute imdea software

Anonymization

EU legislation evolves to harder constraints Art. 29 WP's opinion on anonymization techniques

3 criteria for anonymization

1- No singling out of individuals

Metadata are unique!

- Locati

- "the
  pop
  and
- "if t
  equ
  eno

g

sus track

lution

nts are

ople]"

- **Brows**
- **Demog**

the

populati

nade

them un

-Credit

ual on the

anonymized credit card records, or three purchases if the prices are known" [3 months 1.1 million people]

2- No linking data from one individual

- **Social network data**: take two graphs representing social networks and map the nodes to each other based on the *graph structure alone*—no usernames, no nothing (**Netflix Prize, Kaggle contest)**
  - Techniques to do this automatically

institute imdea software

Anonymization

EU legislation evolves to harder constraints [Art. 29 WP's opinion on anonymization techniques]

3 criteria for anonymization

1- No singling out of individuals

Metadata are unique!

- **Locati**
  - "the **pop** and
  - "if t equ eno

- **Brows**
- **Demog** populati them un
- **Credit** anonymized cr months 1.1 mill

2- No linking data from one individual

g

sus track

- **Soci** netwo the *gr* (**Netf**
  - T

3- No inference about individuals

- **Location**: infer workplace, home, religion,...
- **Energy**: infer concrete appliances, home habits

...

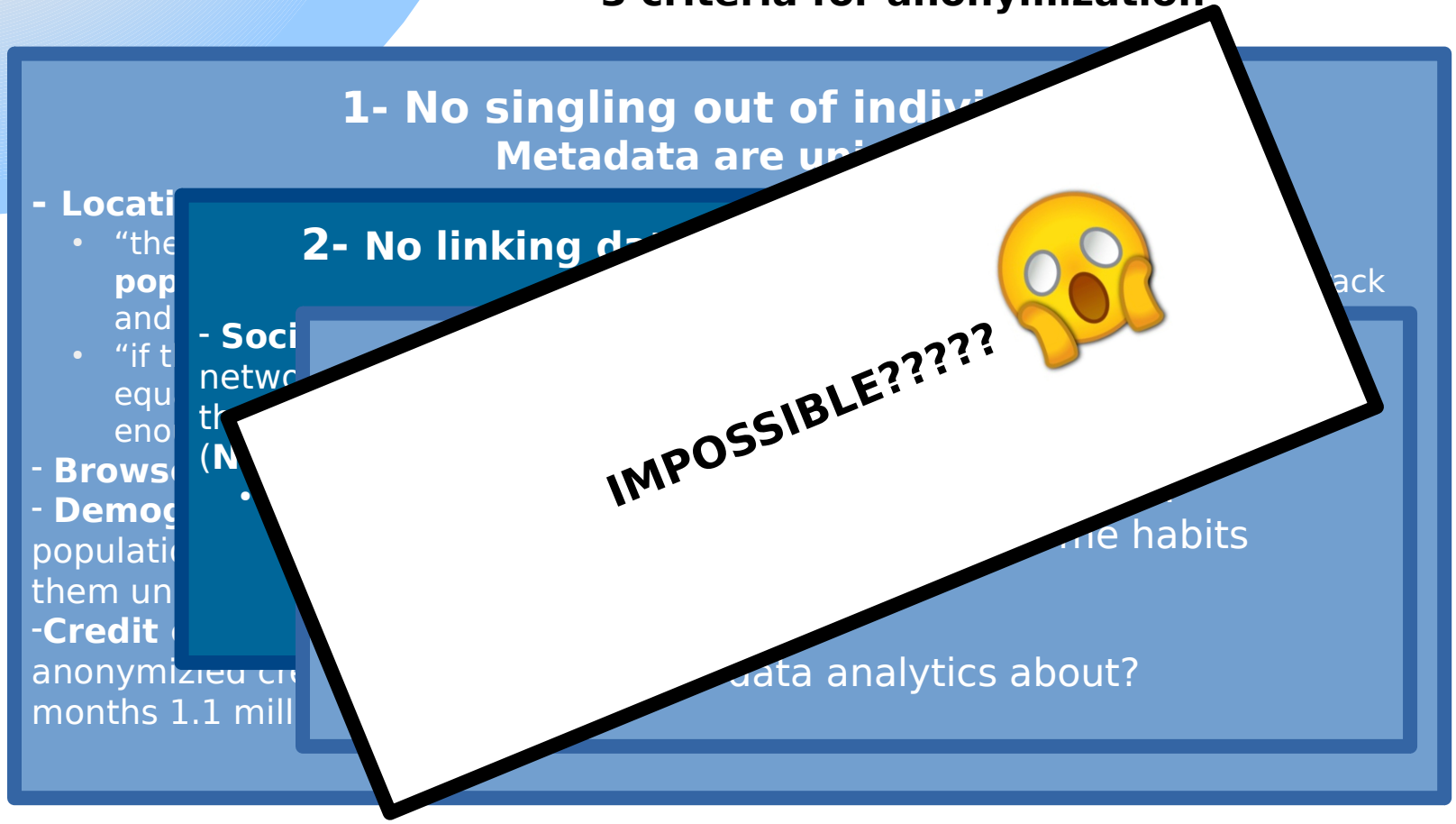
What is data analytics about?

institute imdea software

Anonymization

EU legislation evolves to harder constraints [Art. 29 WP's opinion on anonymization techniques]

3 criteria for anonymization



Anonymization

EU legislation evolves to harder constraints [Art. 29 WP's opinion on anonymization techniques]

3 criteria for anonymization

1- No singling out of individuals

IMPOSSIBLE IS NOTHING

Art 29 – Risk of de-anonymization

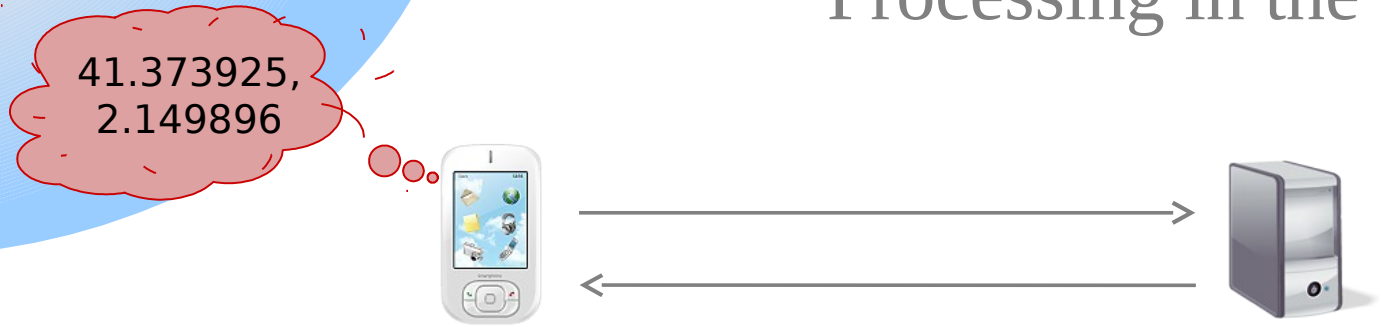
- Traditional identification suppression methods will not do the trick (hash, encryption, random noise…)
- But…
  - We can evaluate anonymity degree and remaining information
  - General anonymization ← little utility
  - Targeted (application dependent) anonymization ← better utility

institute imdea software

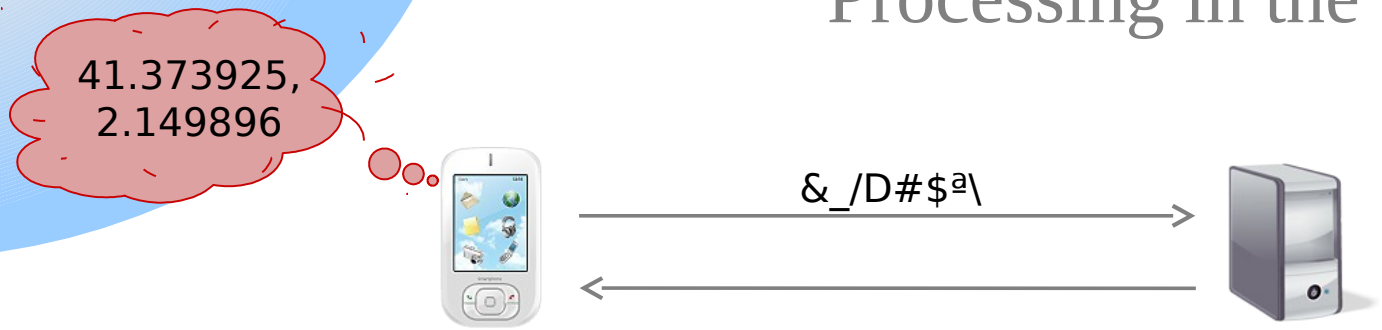
Advanced cryptography
Processing in the encrypted domain

Advanced cryptography
Processing in the encrypted domain

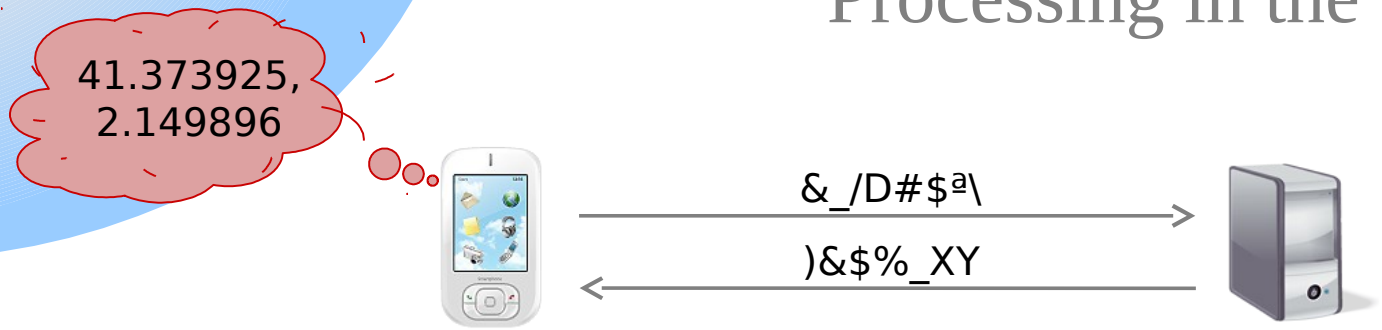
Advanced cryptography
Processing in the encrypted domain



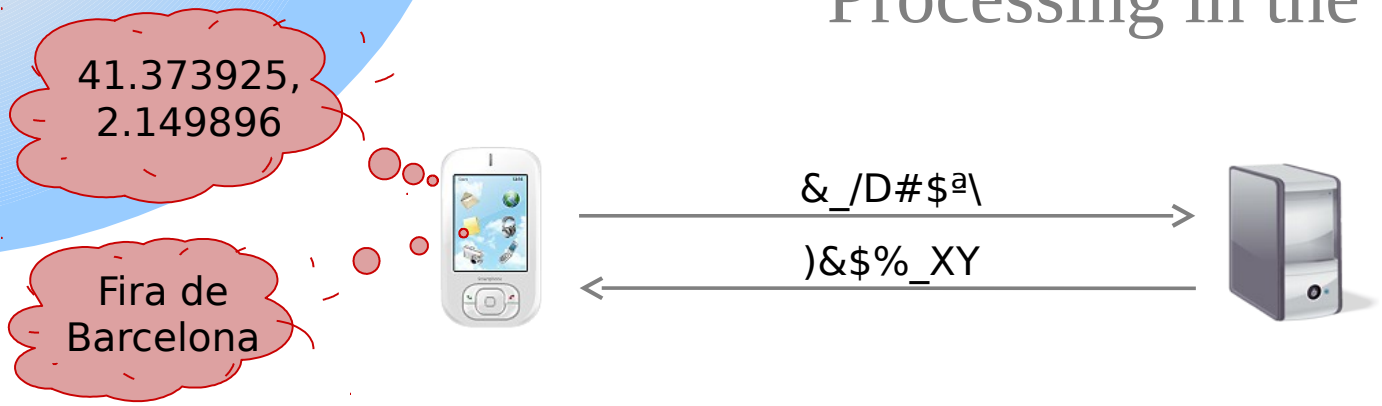
Advanced cryptography
Processing in the encrypted domain



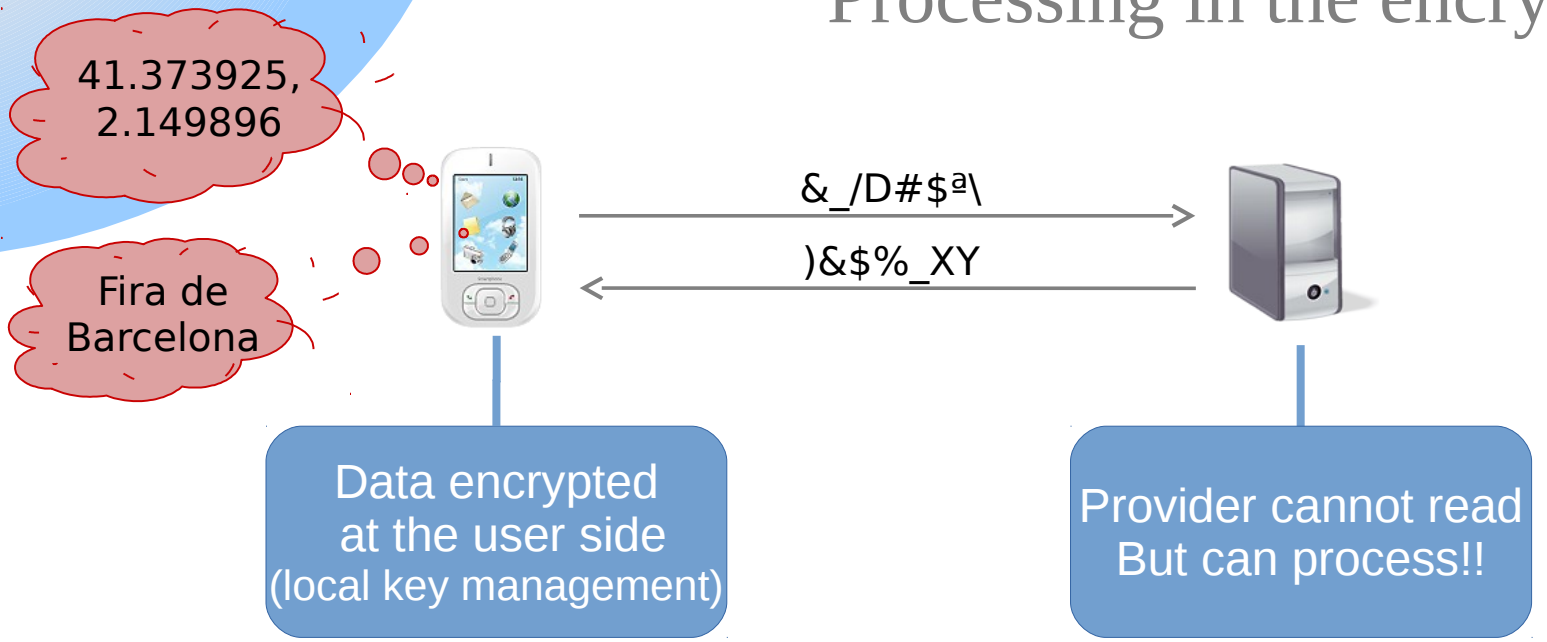
Advanced cryptography
Processing in the encrypted domain



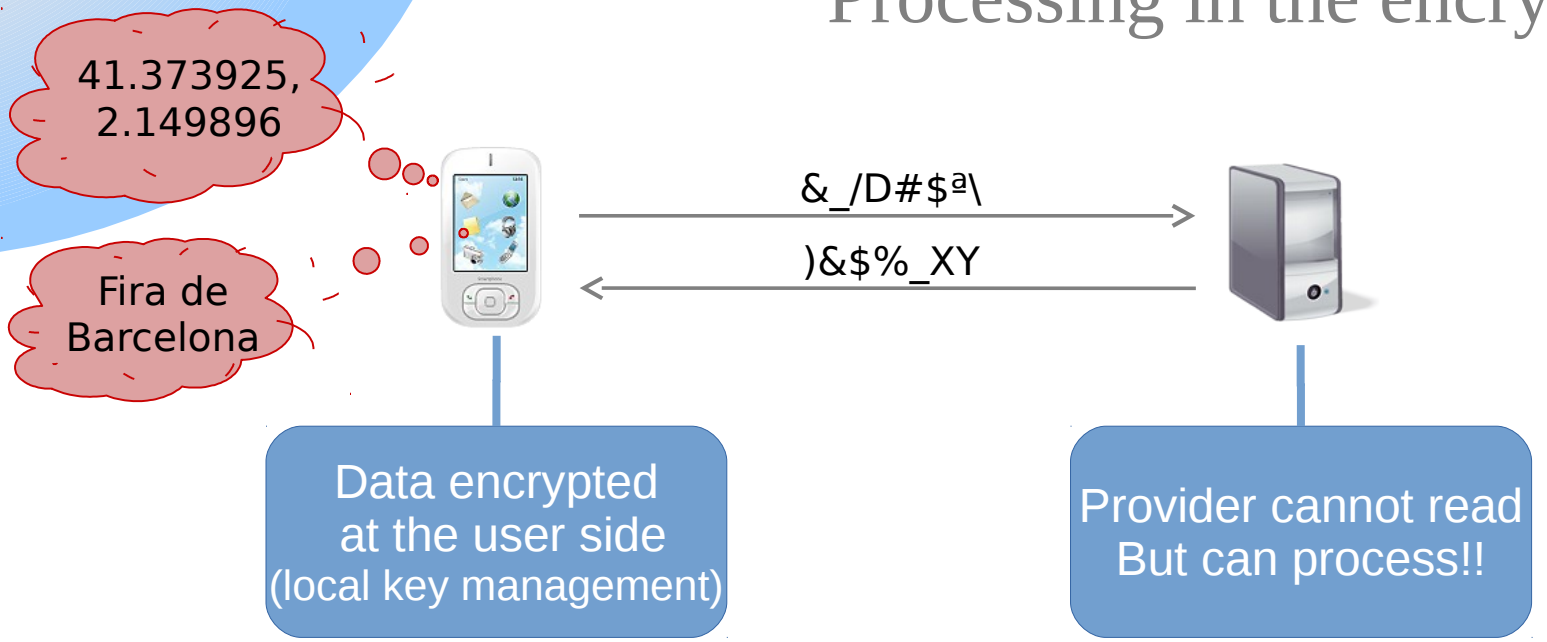
Advanced cryptography
Processing in the encrypted domain



Advanced cryptography
Processing in the encrypted domain



Advanced cryptography
Processing in the encrypted domain



Best of both worlds: service AND privacy!

Advanced cryptography
Processing in the encrypted domain

What “magic”is possible?

- Private searches
- Private billing
- Private comparison
- Private sharing
- Private statistics computation

Privacy-preserving Smart Cities
¿utopia or reality?

No personal data involved: is a reality!

Personal data: not yet guaranteed, but there is a path!

- Anonymization and privacy evaluation
- Advanced cryptography

Carmela Troncoso
Carmela.troncoso@imdea.org
www.software.imdea.org

institute imdea software

Privacy-preserving Smart Cities
¿utopia or reality?

No personal data involved: is a reality!

Personal data: not yet guaranteed, but there is a path!

- Anonymization and privacy evaluation
- Advanced cryptography

We need to work together to walk this path!

Carmela Troncoso
Carmela.troncoso@imdea.org
www.software.imdea.org

institute imdea software