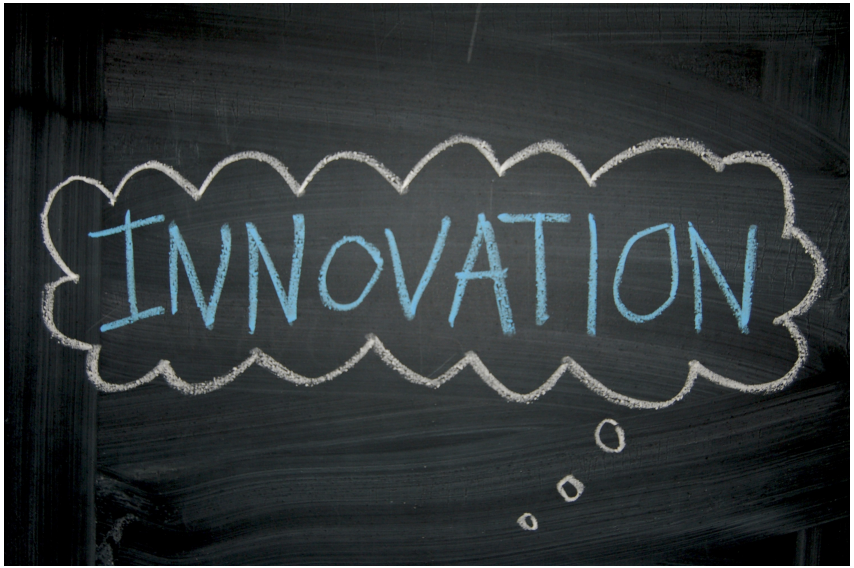
Seeing Privacy Enhancing Technologies as Business Enabling Technologies



Carmela Troncoso
(IMDEA Software Institute)
CPDP 2016
18th November 2015

The Usual approach

I want all data

Designing privacy-preserving ICT systems
Privacy-by-Design

The Usual approach

Designing privacy-preserving ICT systems
Privacy-by-Design

The Usual approach

The PbD approach

institute imdea software

Designing privacy-preserving ICT systems
Privacy-by-Design

The Usual approach

I want all data

Data I can collect

Data protection compliance

The PbD approach

Maintain service integrity

Data needed for the purpose

Data I will finally collect

institute imdea software

Designing privacy-preserving ICT systems
Privacy-by-Design

The Usual approach

I want all data

Data I can collect

Data protection compliance

The PbD approach

Maintain integrity

Data needed for the purpose

Data I will finally collect

institute imdea software

Designing privacy-preserving ICT systems
Privacy-by-Design

The Usual approach

I want all data

Data I can collect

Data protection compliance

The PbD approach

Maintain integrity

Data needed for the purpose

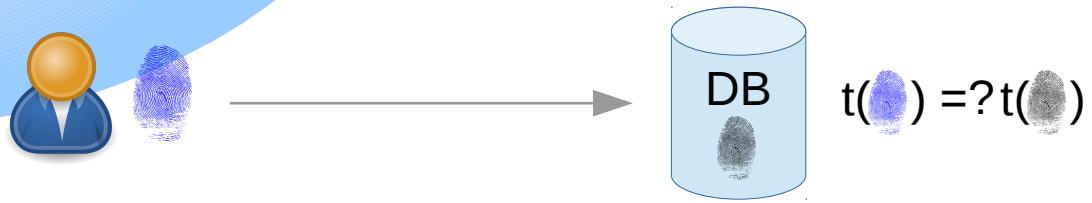
Data I will finally collect

More privacy! … and new opportunities

institute imdea software

Privacy-preserving biometrics

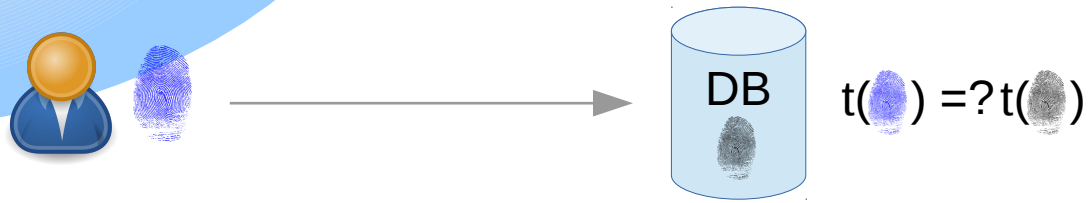
The Usual approach



Templates linkable across databases
Reveal clear biometric
Not revocable
Not externalizable

Privacy-preserving biometrics

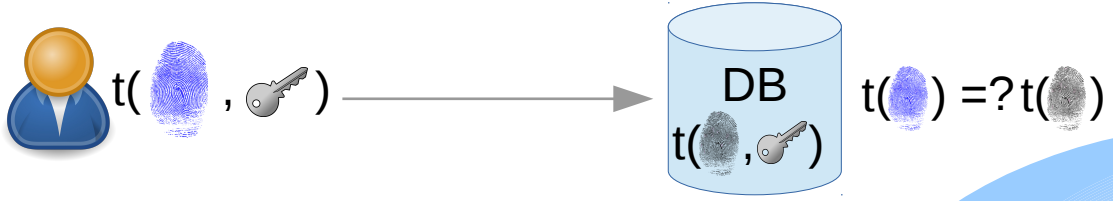
The Usual approach



Templates linkable across databases
Reveal clear biometric
Not revocable
Not externalizable

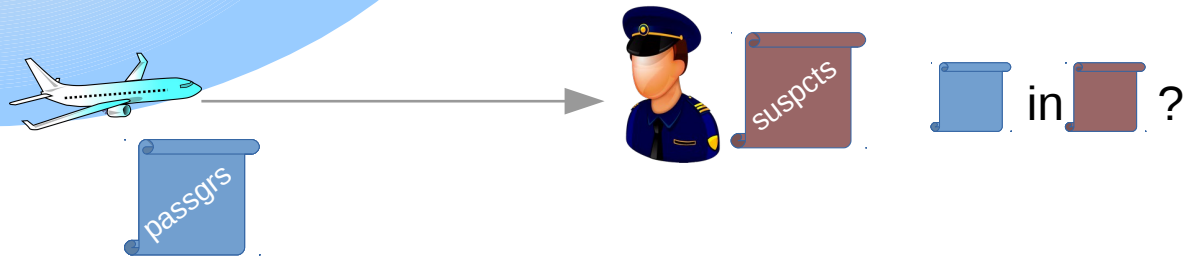
The PbD approach

Templates **not** linkable across databases
Not Reveal clear biometric
Revocable
Externalizable



Privacy-preserving Passenger Registry

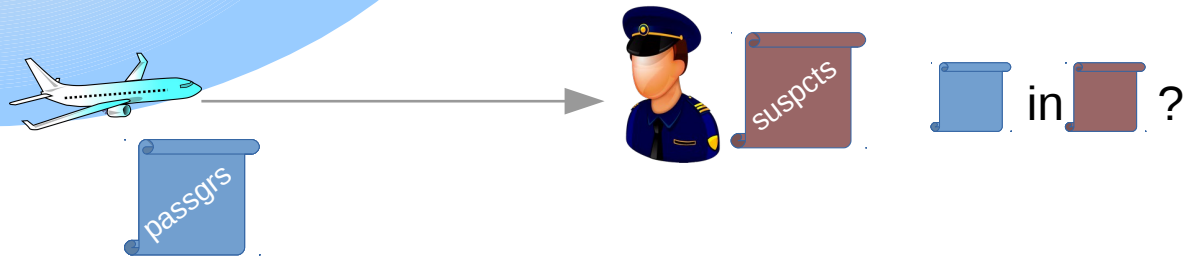
The Usual approach



Surveillance on all passengers

Privacy-preserving Passenger Registry

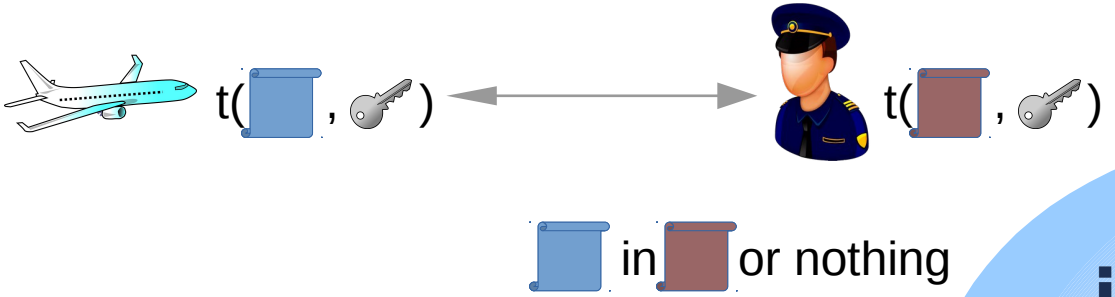
The Usual approach



Surveillance on all passengers

The PbD approach

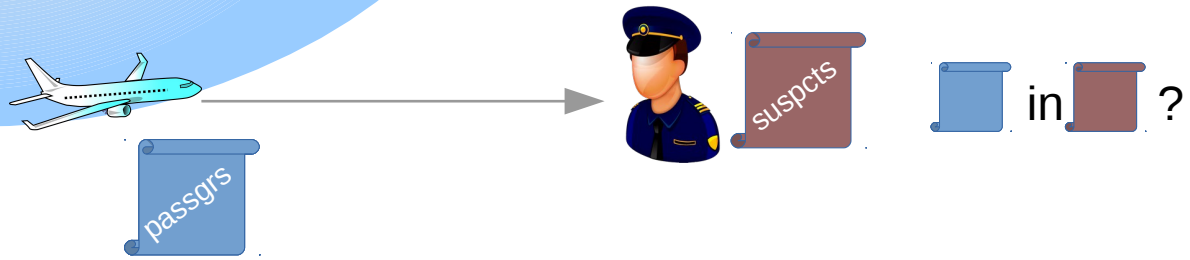
Only coincidences are revealed to law enforcement
No information is revealed to airline



institute imdea software

Privacy-preserving Passenger Registry

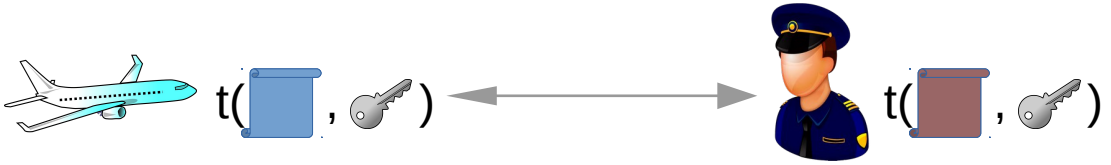
The Usual approach



Surveillance on all passengers

The PbD approach

Only coincidences are revealed to law enforcement
No information is revealed to airline



Other applications: finding common clients, comparing incidence reports, …

institute imdea software

The Usual approach

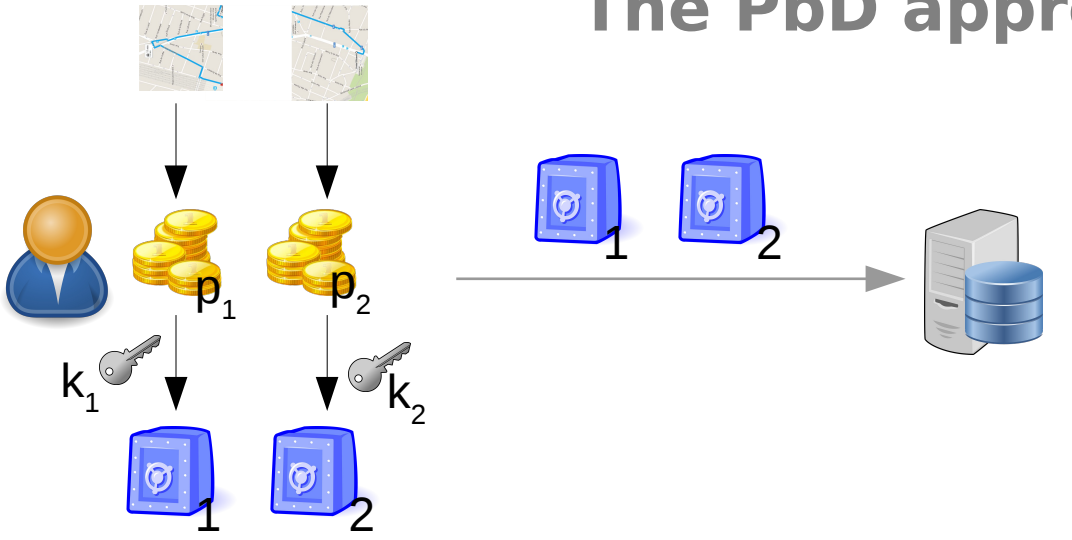
Profiling of users

Privacy-preserving pay-as-you-...

The Usual approach

Profiling of users

The PbD approach

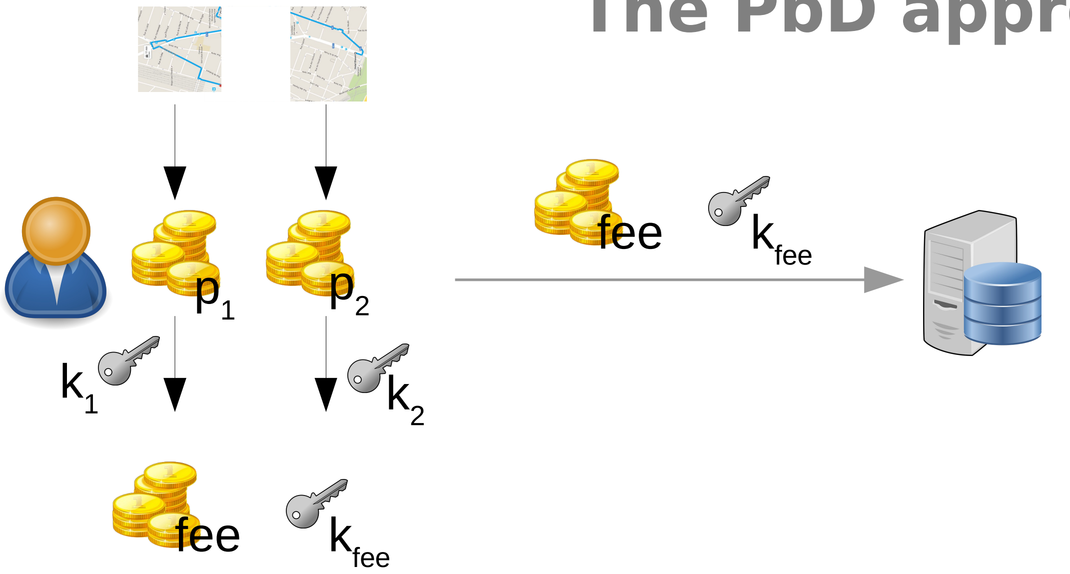


Privacy-preserving pay-as-you-...

The Usual approach

Profiling of users

The PbD approach

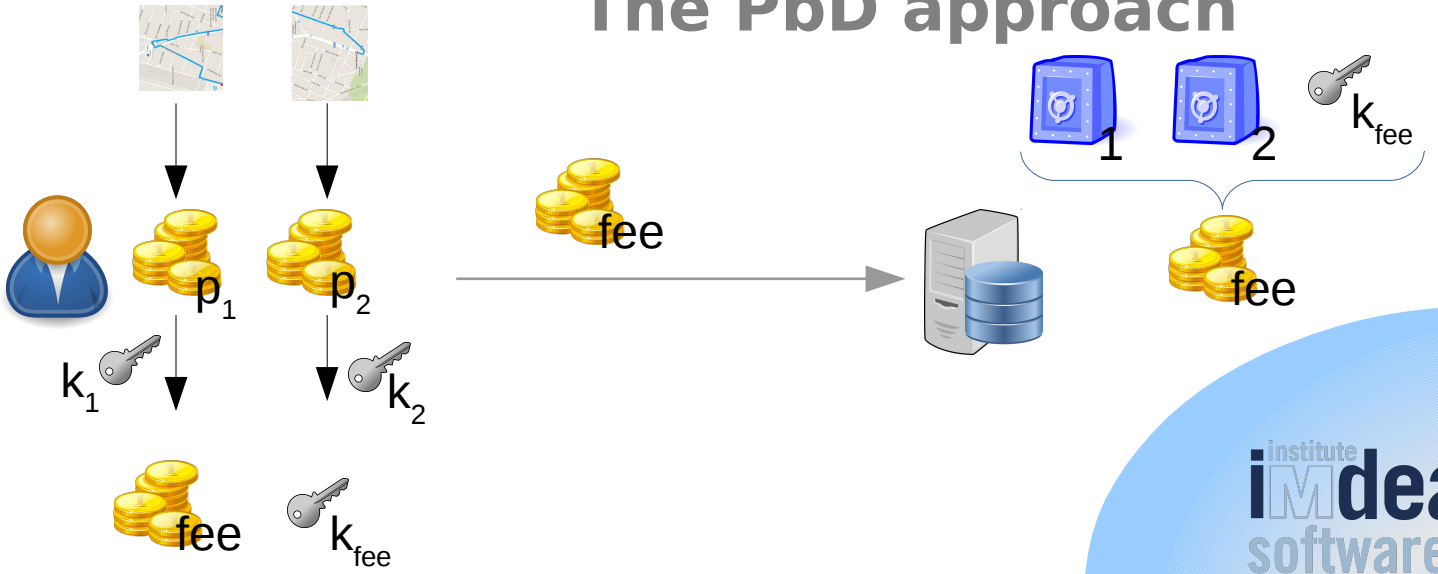


Privacy-preserving pay-as-you-...

The Usual approach

Profiling of users

The PbD approach

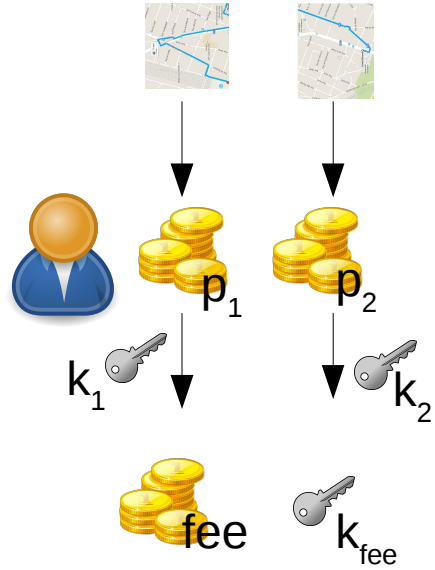


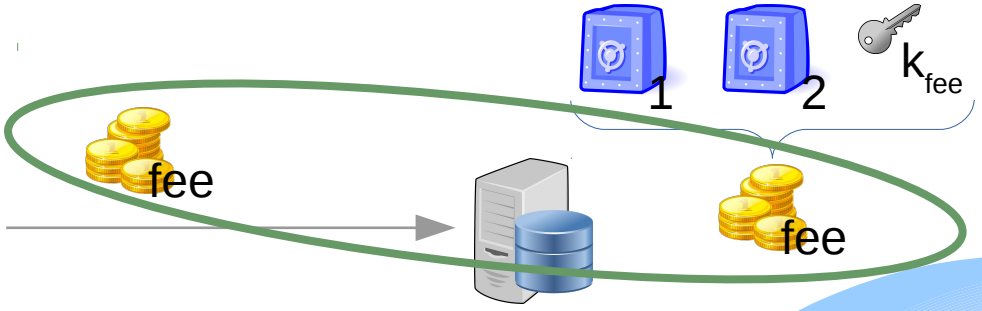
Privacy-preserving pay-as-you-...

The Usual approach

Profiling of users

The PbD approach





No location revealed
Integrity checks

institute imdea software

Advanced cryptography
Processing in the encrypted domain

What “magic”is possible?

- Private searches
- Private billing
- Private comparison
- Private sharing
- Private statistics computation
- Private electronic cash
- Private genomic computations

And 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 but Metadata are unique!
2- No linking data from one individual
3- No inference about individuals

And 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 but Metadata are unique!
2- No linking data from one individual
3- No inference about individuals

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

Seeing Privacy Enhancing Technologies as Business Enabling Technologies

Same (or more!) services, more privacy! (not always user-side!)

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

NEXTLEAP

EU Project – towards a privacy-preserving Internet
Starting Jan 2016

institute imdea software