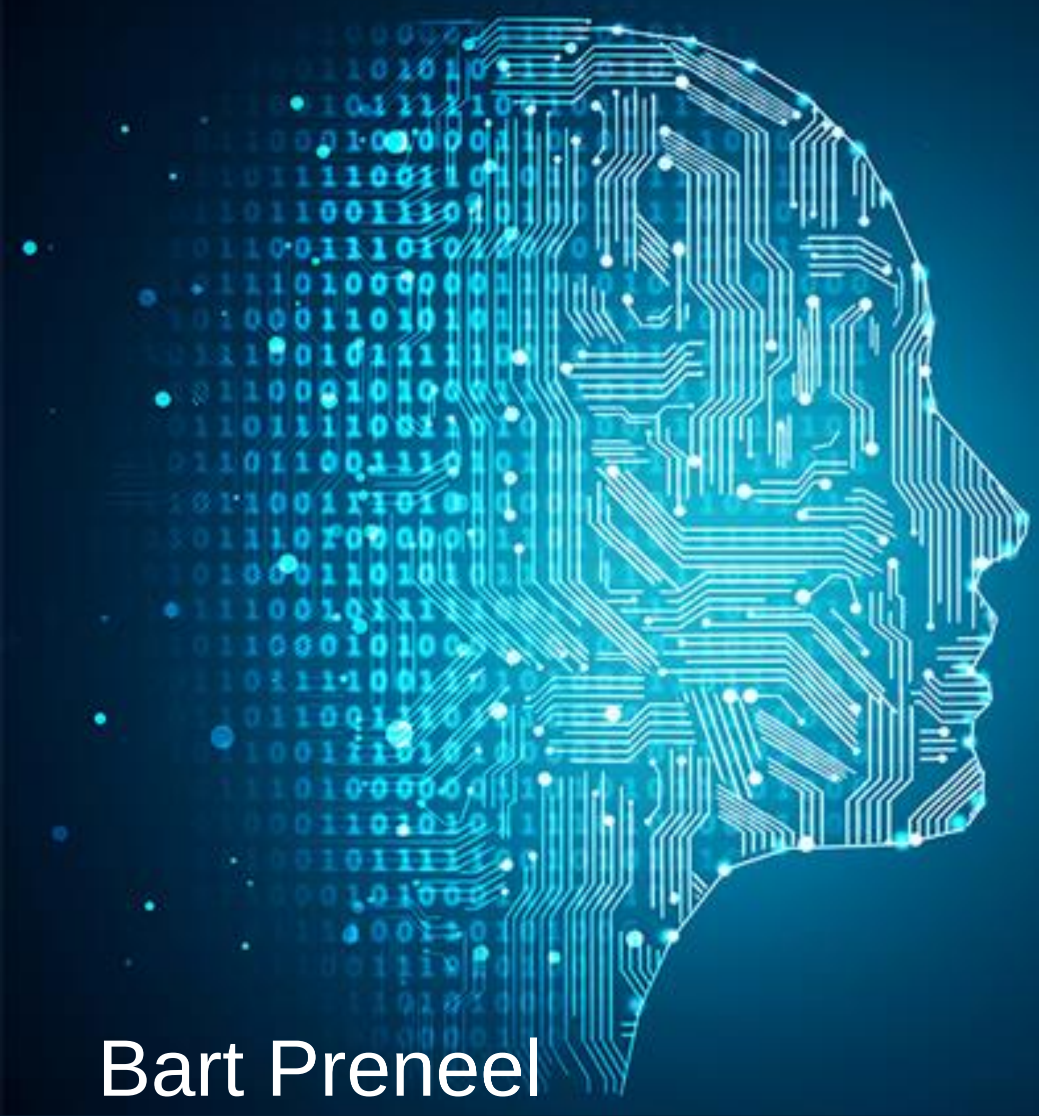


Data Protection in Smart Cities

Bart Preneel

COSIC, KU Leuven

@bpreneel1 - preneel@infosec.exchange

1 March 2024

KU LEUVEN

ArenBerg Crypto BV

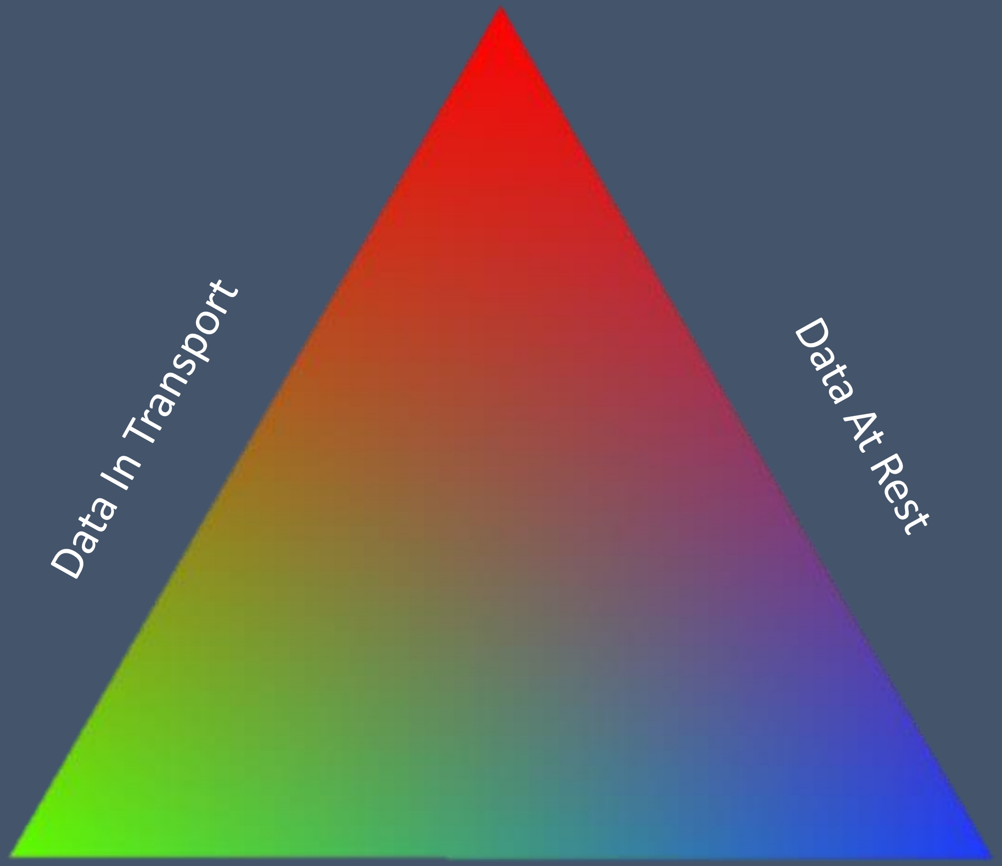
COSIC

Architecture is politics [Mitch Kaipor’93]

Avoid single point of trust that becomes single point of failure

Securing Data

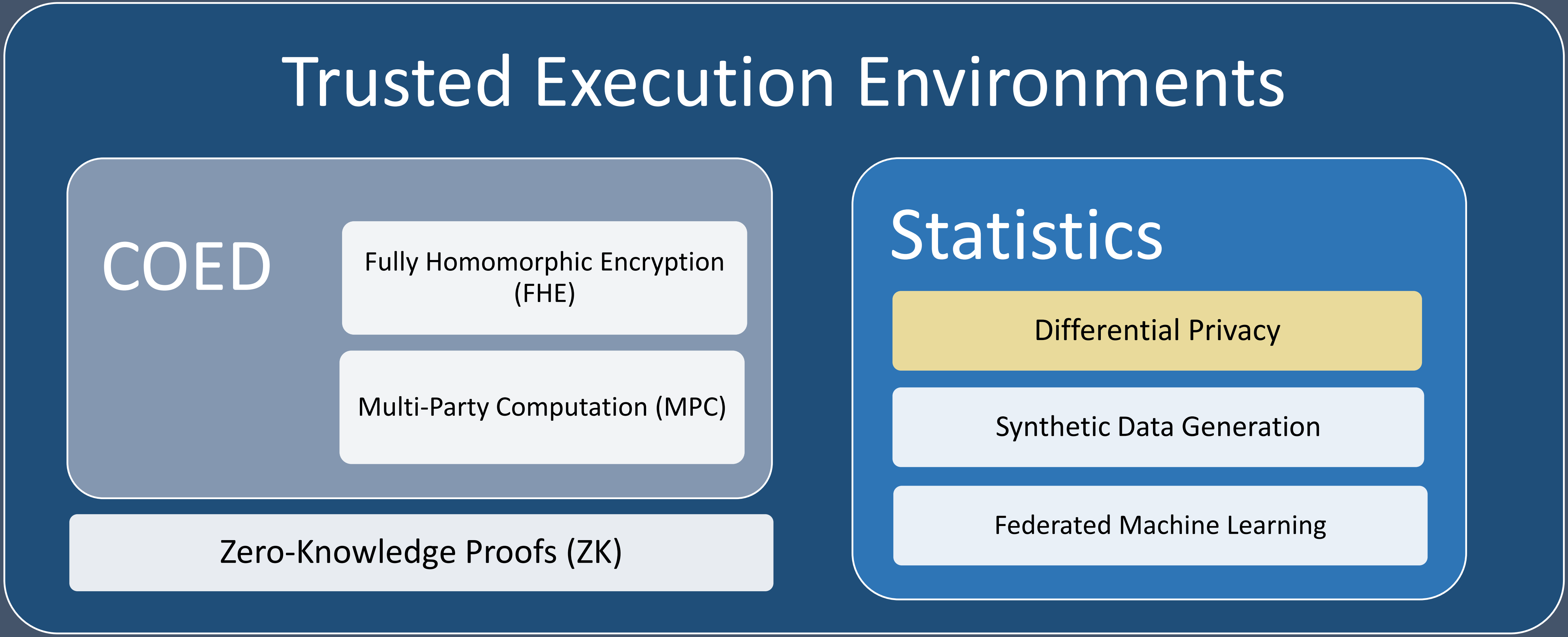
TLS/SSL
IPsec
WLAN
Bluetooth
3G/4G/5G



Data During Computation

Hard disk encryption
File encryption
Database encryption
HSM key storage

Cybersecurity helping AI: Computing on Encrypted Data (COED)



Trusted Execution Environments

COED

Fully Homomorphic Encryption (FHE)

Multi-Party Computation (MPC)

Zero-Knowledge Proofs (ZK)

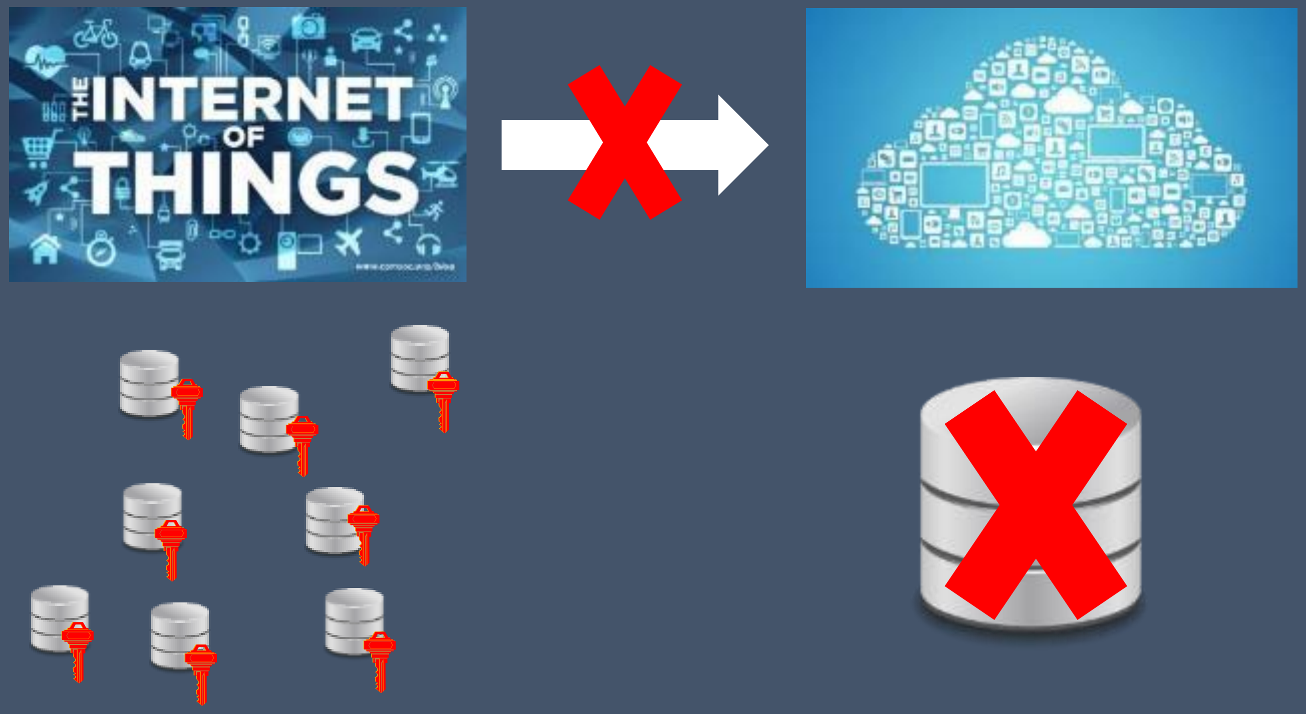
Statistics

Differential Privacy

Synthetic Data Generation

Federated Machine Learning

From Big Data to small local data



Data stays with users

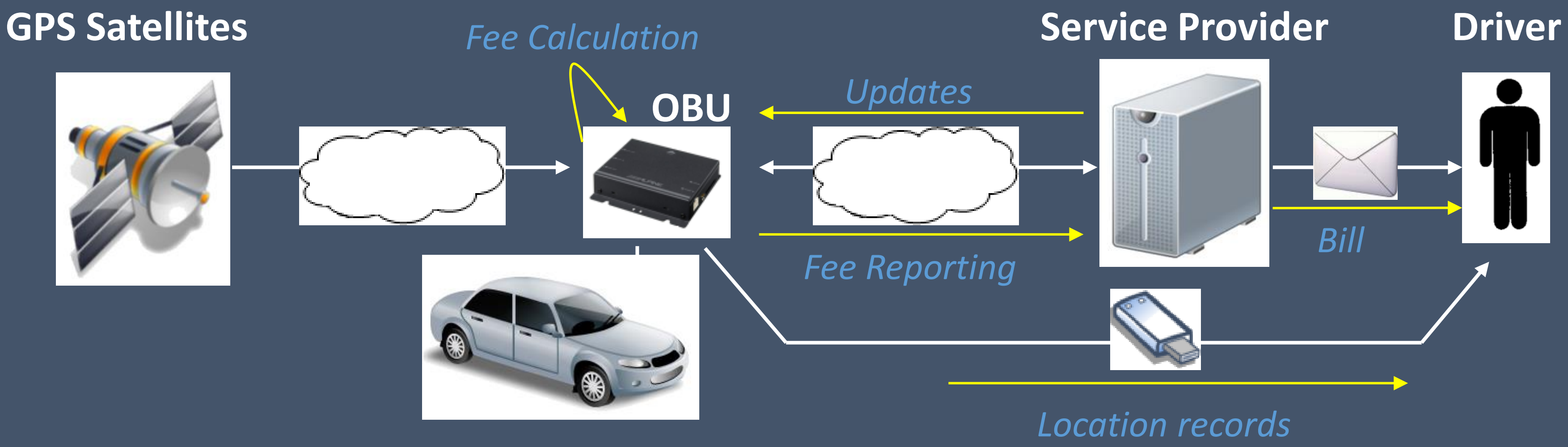
Privacy-preserving Tolling Model

Keep personal data in user’s domain [TDKP07]

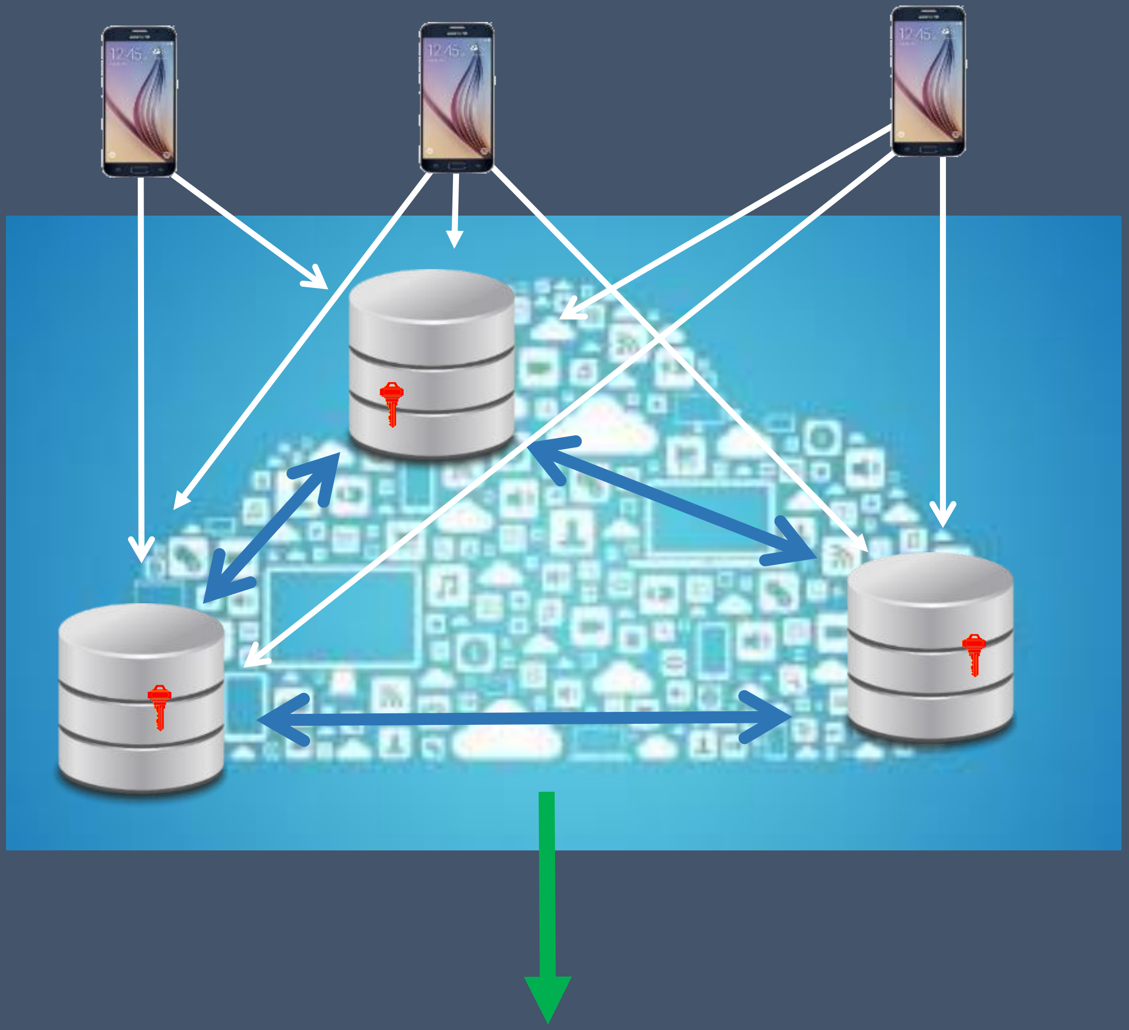
Data minimization

Only final fee is sent to Service Provider

Only driver has access to his own location records

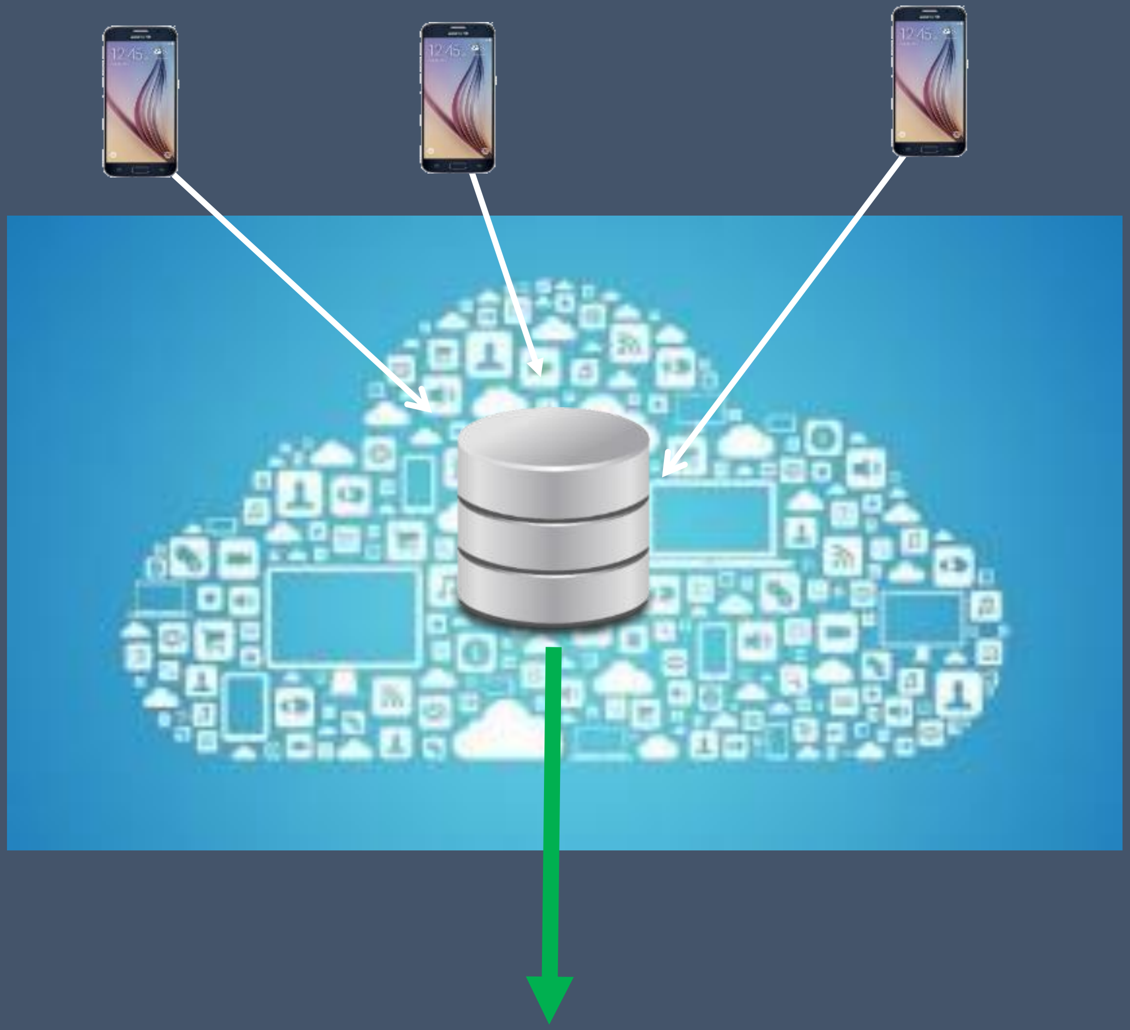


From Big Data to encrypted data
MPC (Multi-Party Computation)



+ secrets shared over multiple servers
+ moderate computation
- high communication overhead

From Big Data to encrypted data
(somewhat) Fully Homomorphic Encryption



+ single server
+ low communication
- high computation cost
- simple functions: basis statistics, neural networks

Some observations

- Power relation in society:
  - values
  - data should be used to help people rather than to manipulate, control or harm them
  - for which data should there be a market?
- Architecture is politics
- Access by law enforcement and intelligence agencies

Trust of Users?

Consent

Control (data & meta-data)

Engagement

Empowerment

More observations

- Involvement of DPOs in public procurement
- Further study of cameras
- Trust and governance for public-private partnerships: need to clarify the purpose of processing and repurposing

Some further observations

- Transparency and privacy: what can be open?
- Anonymization of mobility traces: only through aggregation
- Pseudonymization: additional data or additional effort?

- Vehicle:
  - Road pricing and insurance pricing: disaster so far
  - ANPR & beacons do not help
  - Who owns which data?
  - V2X and autonomous driving will change everything

Conclusions

- Architecture is politics
- Utility-privacy tradeoff: try to shift the curve
- Computations on encrypted data are cool but can still be unfair or unethical

Bart Preneel

ADDRESS:	Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE:	homes.esat.kuleuven.be/~preneel/
EMAIL:	Bart.Preneel@esat.kuleuven.be
MASTODON:	bpreneel@infosec.exchange
TWITTER:	@bpreneel1
TELEPHONE:	+32 16 321148

KU LEUVEN

ArenBerg Crypto
BV

COSIC