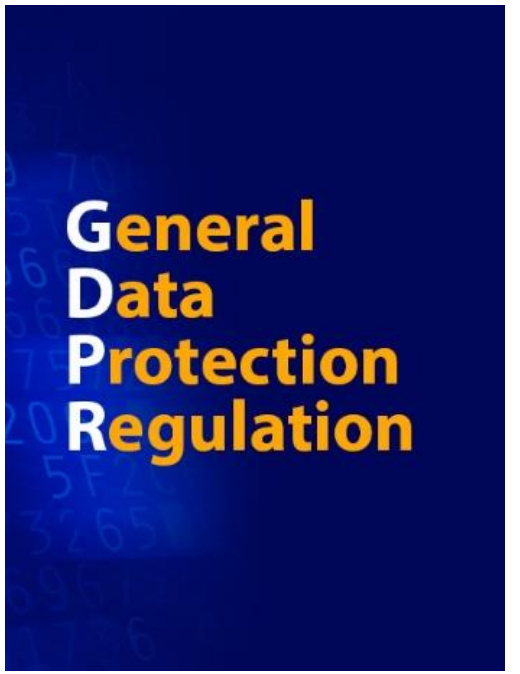
GDPR Privacy Implications for the Internet of Things

Daniel Bastos
Fabio Giubilo

4th December 2018

GDPR

On May 25th of 2018 all EU countries began to apply the General Data Protection Regulation (GDPR). GDPR aims to protect and regulate data privacy and applies to any organization that holds or processes data on EU citizens, regardless of where it is headquartered. The penalties for non-compliance can be as high as 4% of global revenue for companies. As a result, compliance with GDPR is a must for companies who deal with users data.



Concepts and Definitions

Data Subject

Data Controller

Data Processor

"Alexa, I want a pizza!"

Consent

amazon

Processing

Data Breach

Domino's Pizza

Data Breach

Processing

mastercard

Data Breach

BT

Principles

GDPR Principles (Article 5)

Accuracy

Security

Minimisation

Purpose Limitation

Retention Periods

Fair, Lawful and Transparent Processing

Accountability

BT

Rights and Obligations of Data Subjects, Controllers and Processors

GDPR Rights and Obligations of Data Subjects, Controllers and Processors

Data Subjects

- Right to Access
- Right to be Forgotten
- Right to withdraw Consent
- Right to Data Portability

Art. 12 to 22

Data Processors and Controllers

- Privacy by Design and by Default
- Breach Reporting and Notification
- Appoint a DPO
- Cooperate with DPAs

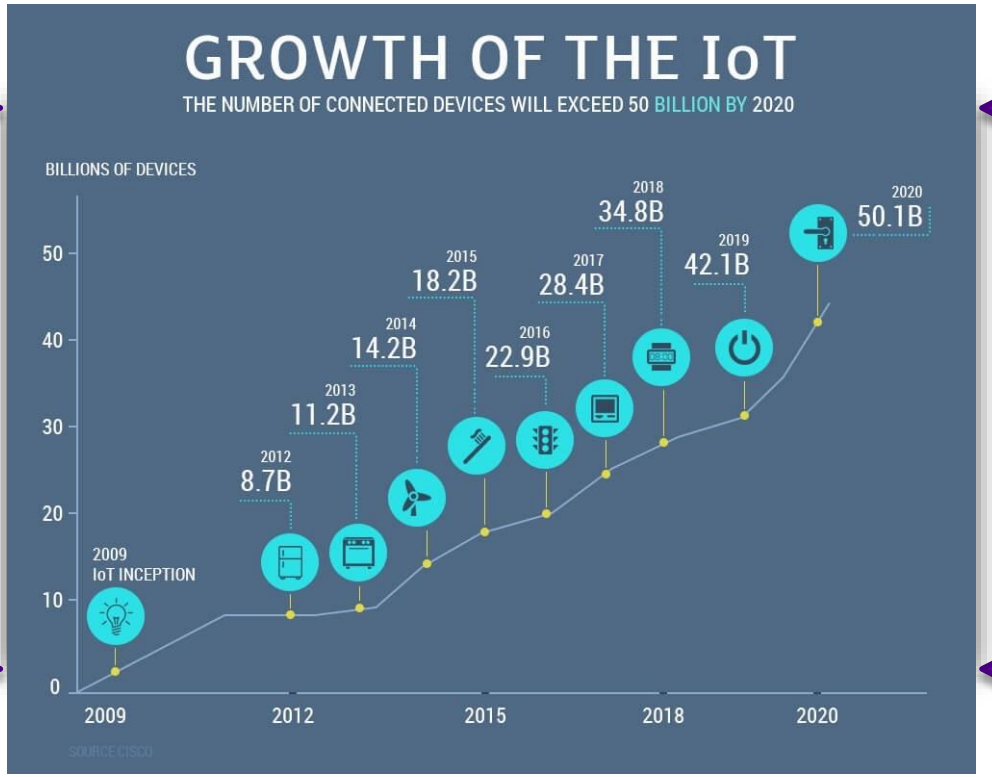
Art. 24 to 34

Challenges in IoT environments

GDPR Challenges in IoT environments

Consent

Transparent Processing and Right to be Forgotten



Data Minimisation

Data Breach Reporting

BT

Privacy Implications

Privacy & GDPR

"Someone's right to keep their personal matters and relationships secret."
Cambridge Dictionary

- GDPR article 32: *controllers* and *processors* **must** implement effective privacy preserving mechanisms
- Anonymization vs Pseudo-anonymization
- PII: Personal Identifiable Information
- ISO 27001?

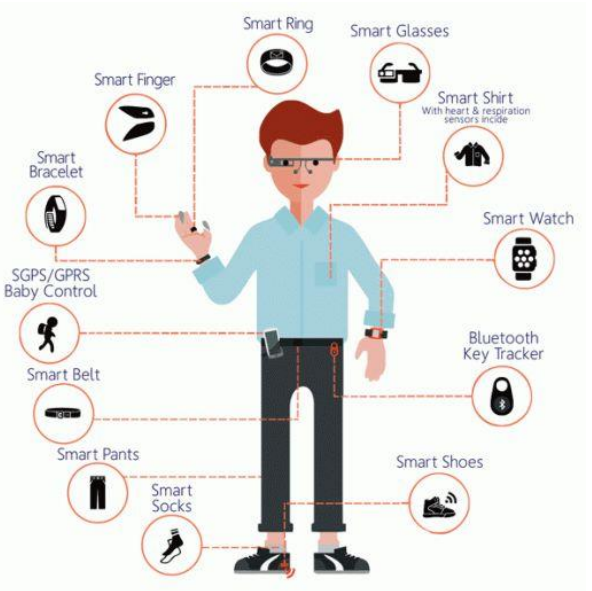
Privacy Concerns – Smart Home Use Case

- Devices:
  - > TV, bed, home pod, lights, fridge, toothbrush, smart readers
- Data ownership?
  - > “Terms & Conditions Agreement”
- Potential Threats:
  - > Selling data to 3rd party
  - > More data it is actually collected
  - > Data weakly protected
  - > Individuals profiling

Credits to: https://gizmodo.com/the-house-that-spied-on-me-1822429852

Privacy Concerns – Healthcare Use Case

- Wearable devices
- Users awareness?
- Marketing purposes
- Very dangerous scenario!
  - > Why?

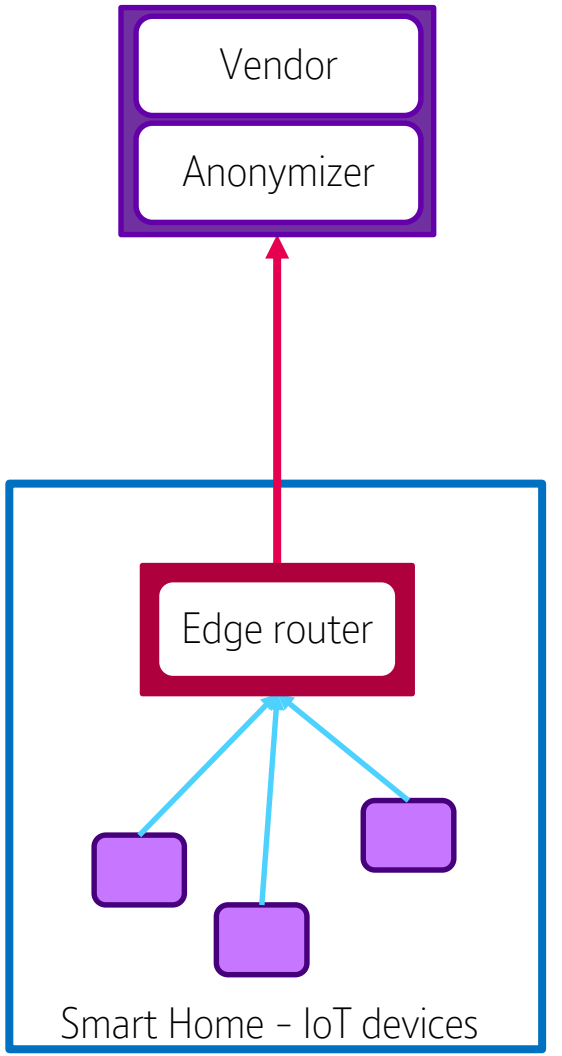


Mitigation Approaches

Mitigation Approach 1

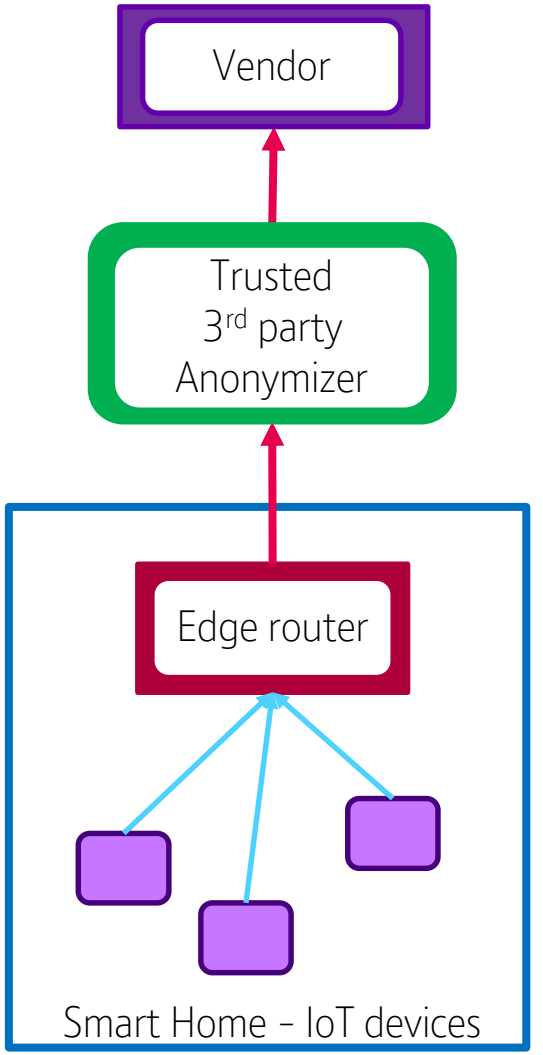
- Based on the user's trust with regards to IoT vendor:

  > Trust in vendor: high
  > Implementation difficulty: easy
  > Risk: high



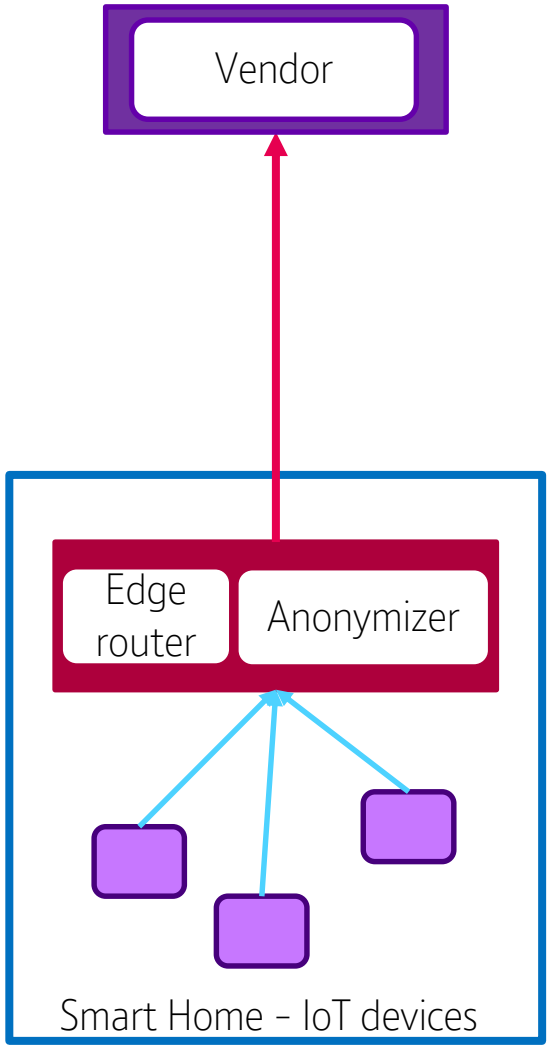
Mitigation Approach 2

- "Anonymization As a Service" (AnaaS)
  - > Trust in vendor: low
  - > Trust in 3rd party service: high
  - > Implementation difficulty: medium
  - > Risk: low in vendor, medium/high in 3rd party service



Mitigation Approach 3

- Anonymization is applied locally:
  - > Trust in vendor & 3rd party service: very low
  - > Implementation difficulty: hard
  - > Risk: very low



Daniel Bastos
daniel.bastos@bt.com
Fabio Giubilo
fabio.giubilo@bt.com

Thank You!

- *Thank you to the European Union, British Telecom and my distinguished supervisors for giving us this opportunity.*
- *This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 675320.*
- *This work reflects only the author's view and the Research Executive Agency is not responsible for any use that may be made of the information it contains.*