# *New Emergency Management in a Resilience Era Facing Health, Climate and Energy Challenges*

## *6th to 10th December 2021*

Session 12: IMEPTUS presentations

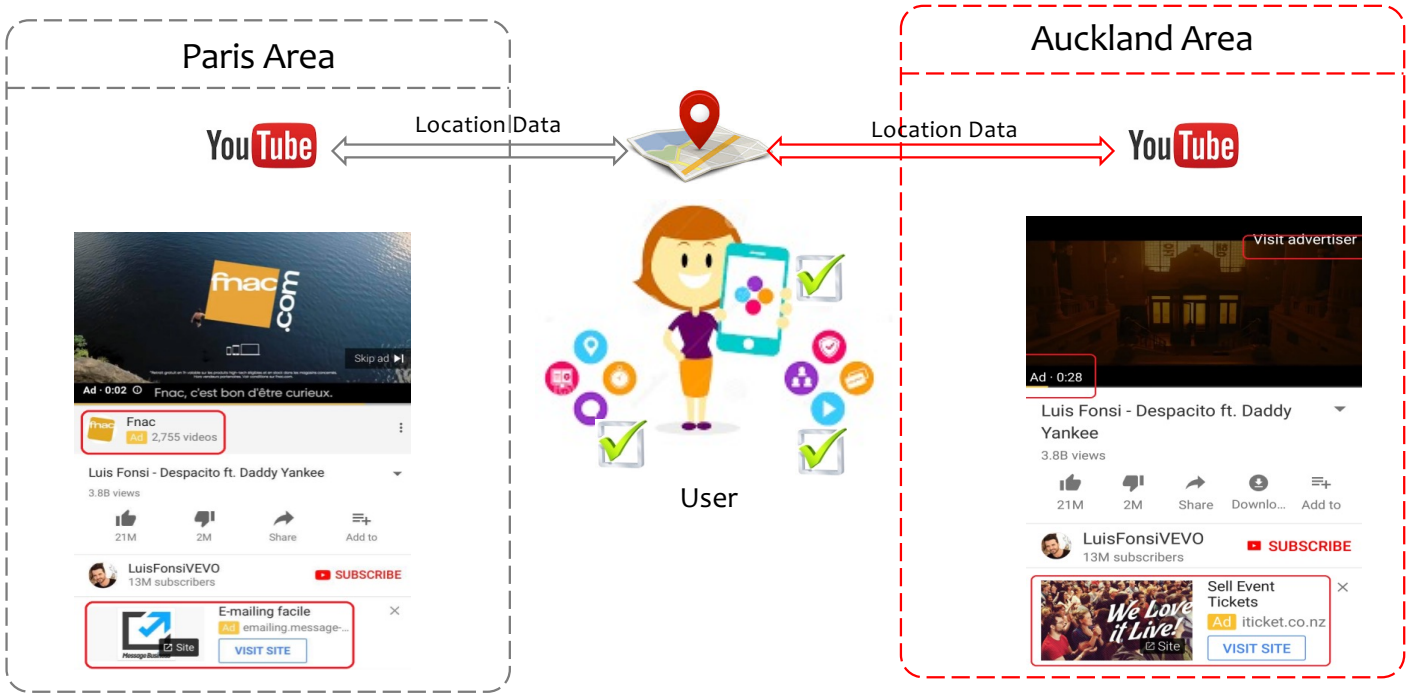
9th December 2021

**Nesrine Kaaniche and Joaquin Garcia Alfaro**

**Télécom SudParis, Institut Polytechnique de Paris, France**

# PRIVACY-PRESERVING CHALLENGES FOR URBAN SAFETY

General Context: What do they know about us?



# General Context: Who control our data in urban spaces?

Amazon Echo's privacy issues way beyond voice recordings

20 janvier 2020, 16:36 CET  Mis à jour le 21 janvier 2020, 09:56 CET

Amazon Echo and the Alexa voice assistant have publicised issues with privacy. Whether it is the they collect or the fact that they reportedly pay at times, external contractors from all over the recordings to improve accuracy, the potential is sensitive personal information to be leaked thro devices.

But the risks extend not just to our relationship with Amazon. Major privacy concerns are starting to emerge in the way Alexa devices interact with other services – risking a dystopian spiral of

Equifax Data Breach Affects Millions of Consumers. Here's What to Do.

By Steve Symanovich  October 12, 2017  Share

Related Articles

10 Warning Signs of Identity Theft

Fraud: What You Need to Know



Forbes  Billionaires  Innovation  Leadership  Money  Business  Small Business  Lifestyle  Lists  Advisor

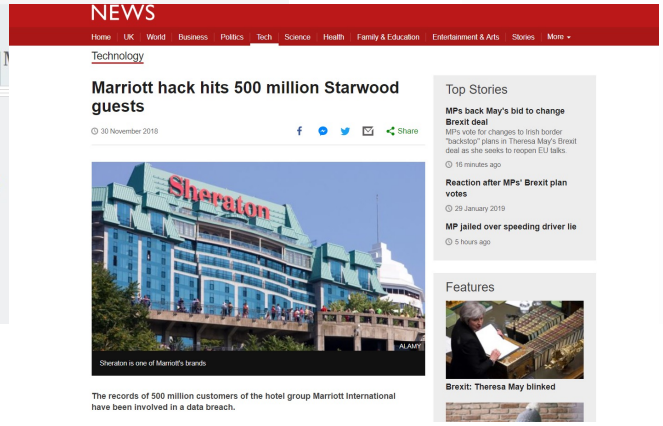
Support The Guardian  Subscribe  Find a job  Sign in  Search

News  Opinion  Sport  Culture  Lifestyle

Cambridge Analytica  The Cambridge Analytica Files

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters



NEWS

Home  UK  World  Business  Politics  Tech  Science  Health  Family & Education  Entertainment & Arts  Stories  More

Technology

Marriott hack hits 500 million Starwood guests

30 November 2018  Share

Sheraton

Sheraton is one of Marriott's brands

The records of 500 million customers of the hotel group Marriott International have been involved in a data breach.

Top Stories

MPs back May's bid to change Brexit deal

MPs vote for changes to Irish border "backstop" plans in Theresa May's Brexit deal as she seeks to reopen EU talks.

16 minutes ago

Reaction after MPs' Brexit plan votes

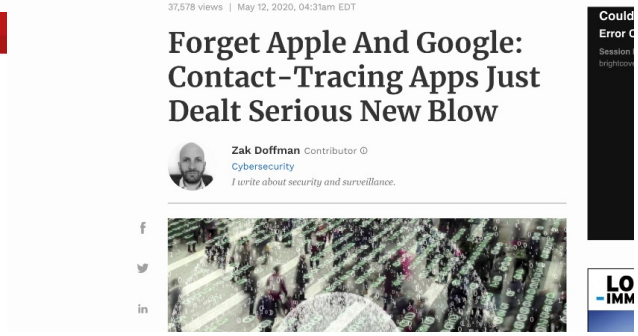
29 January 2019

MP jailed over speeding driver lie

5 hours ago

Features

Brexit: Theresa May blinked



37,578 views | May 12, 2020, 04:31am EDT

Forget Apple And Google: Contact-Tracing Apps Just Dealt Serious New Blow

Zak Doffman Contributor

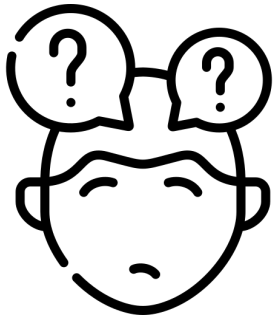
Cybersecurity

*I write about security and surveillance.*

# General context: How to deal with?

- Privacy is not only being anonymous. It is beyond that!

**Privacy is not for criminals only! But, It is Hard to achieve!**



## Privacy Enhancing Technologies (PET) can Help!

Needed

Fast enough to be useful


Not ***«generally usable»*** yet

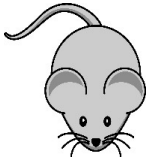
# Agenda

- General context
- Use case scenario
- PET categorization
- Discussion
- Conclusion

# Use case scenario

- Computer Science Student at IMT
- Living in Paris

**Alice**



Alice wants to buy a mouse (Grey Mouse)

Response: a list of websites selling mouses

Alice Profile:
- Computer Scientist
- Paris

**WSE**

Looking for a pleasant area

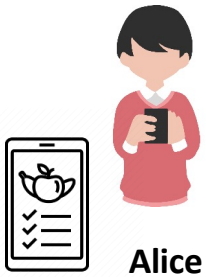
Response: Destinations around Paris
Ads related to mouses

Alice Profile:
- Computer Scientist
- Paris
- mouse

**Web search queries/recommandations**
**May be relevant/sometimes NOT!**

# Use case scenario

-Alice goes to the gym
- She uses a wellbeing mobile application



**Alice**

Sensitive data (wellbeing/health data): weight, height, nutrition, walking distances, activities, …

Personalised actions/recommendations

Sensitive data massively collected

**WSE**

**Pervasive Applications**

**Fun vs Inconvenience: What is the right Balance?**

**Health Insurance**

**Employer**

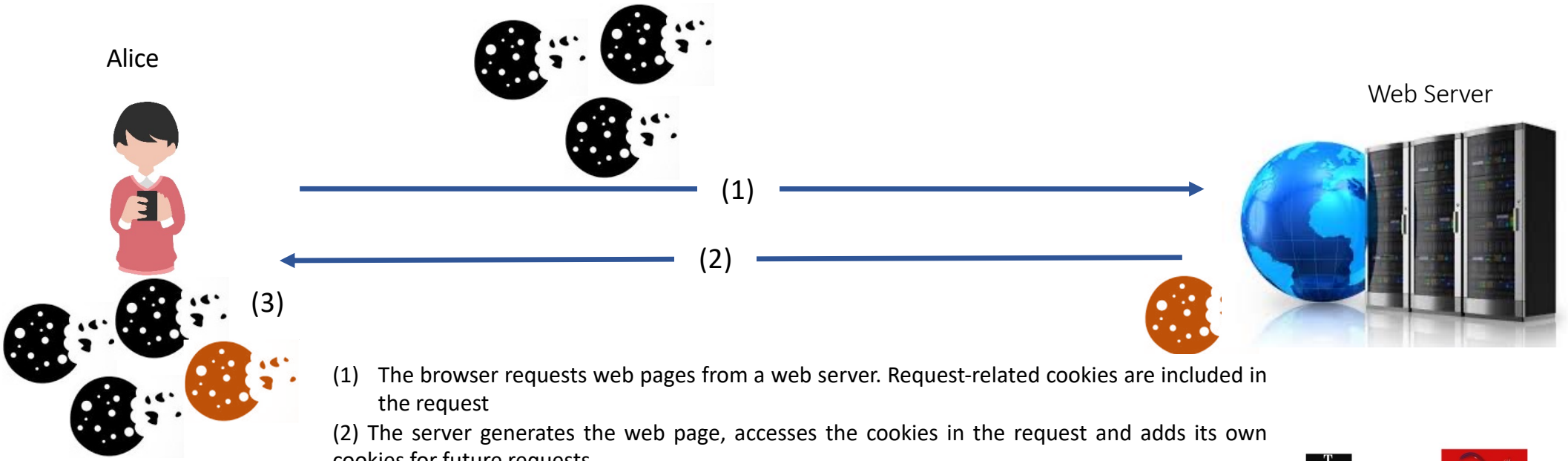
# PETs: A novel Taxonomy

| PET groups | Categories | Approaches | Trust Model | Architectural Model | Drawbacks | Adapted to Personalized Services | Use-Cases |
|---|---|---|---|---|---|---|---|
| User Side | anti tracking | application level | semi-trusted | client-server | non-personalized services<br>traffic overhead (TOR)<br>activity identification by provider (VPN) | × | web services |
| | | network level | untrusted | distributed (TOR) | | | |
| | | | trusted | client-server (VPN) | | | |
| | privacy preserving certification | anonymous credentials<br>group based signature<br>attribute based signature | semi-trusted | client-server | computational overhead<br>infrastructure requirements | ✓ | e-health applications<br>e-voting<br>smart-cities applications<br>e-banking |
| | obfuscation | data perturbation | untrusted | distributed | traffic overhead<br>privacy-utility trade-offs | ✓ | pervasive applications<br>recommendation services |
| | privacy preserving computation | SMC | untrusted | distributed | several users must collaborate<br>all participants need to be present<br>collusion attacks | ✓ | pervasive applications<br>web search<br>smart-cities applications |
| Server Side | Statistical Disclosure Control | anonymization<br>Differential Privacy | semi-trusted | client-server | privacy-utility trade-offs | ✓ | vehicular applications<br>well-being applications<br>geo-social applications<br>intelligent transport |
| | self-destructing data systems | | semi-trusted | distributed | Sybil attacks | × | web search |
| | obfuscation | PIR | semi-trusted | client-server | non-personalized services<br>computational overhead | × | web search |
| | privacy preserving computation | homomorphic encryption | semi-trusted | client-server, distributed | computational overhead | ✓ | recommendation services<br>pervasive applications |
| Channel Side | secure communications | C-S communications | trusted | client-server | key management (e.g. PKI) | ✓ | web search |
| | | end-to-end | untrusted | distributed | | × | messaging applications |
| | TTP | high anonymous proxy<br>anonymous proxy | trusted | TTP | users must trust an external entity<br>collusion attacks<br>infrastructure requirements | ✓ | web search<br>recommendation services<br>pervasive applications |

# Example of user side techniques: anti-tracking

**Main goal of anti-tracking tools:**

Prevent the server provider to trace Alice Interactions (using cookies or fingerprintings)




(1) The browser requests web pages from a web server. Request-related cookies are included in the request

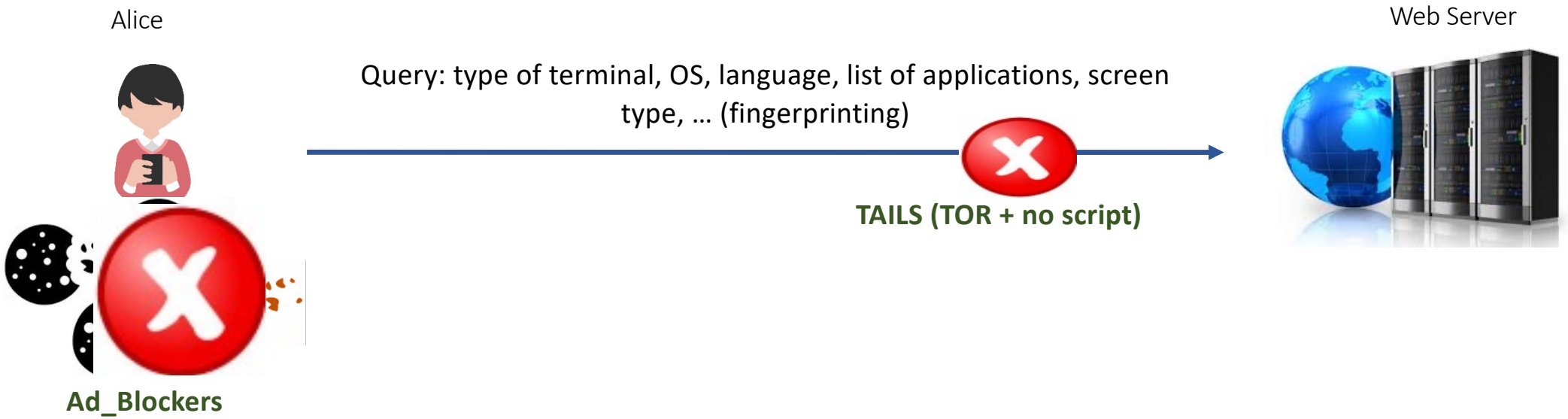
(2) The server generates the web page, accesses the cookies in the request and adds its own cookies for future requests

(3) The page loads in the browser using the existent cookies plus any new cookies received from the web server.

# Example of user side techniques: anti-tracking

**Main goal of anti-tracking tools:**

Prevent the server provider to trace Alice Interactions (using cookies or fingerprintings)



# Example of server side techniques: Statistical Data Disclosure

**Main goal of database anonymisation (Statistical Disclosure):**

- Enable companies/enterprises to use/process anonymised data (indenpendently from GDPR requirements)

Original dataset

| | Age | Disease |
|---|---|---|
| 1 | 22 | lung cancer |
| 2 | 22 | lung cancer |
| 3 | 22 | lung cancer |
| 4 | 45 | stomach cancer |
| 5 | 63 | diabetes |
| 6 | 40 | aids |
| 7 | 35 | aids |
| 8 | 35 | flu |
| 9 | 32 | diabetes |

Generalized dataset

| | Age | Age* |
|---|---|---|
| 1 | 22 | 2* |
| 2 | 22 | 2* |
| 3 | 22 | 2* |
| 4 | 45 | $\geq 40$ |
| 5 | 63 | $\geq 40$ |
| 6 | 40 | $\geq 40$ |
| 7 | 35 | 3* |
| 8 | 35 | 3* |
| 9 | 32 | 3* |

3-anonymity dataset

| | Age* | Disease |
|---|---|---|
| 1 | 2* | lung cancer |
| 2 | 2* | lung cancer |
| 3 | 2* | lung cancer |
| 4 | $\geq 40$ | stomach cancer |
| 5 | $\geq 40$ | diabetes |
| 6 | $\geq 40$ | flu |
| 7 | 3* | aids |
| 8 | 3* | aids |
| 9 | 3* | diabetes |

# Example of server side techniques: Statistical Data Disclosure

**Main goal of database anonymisation (Statistical Disclosure):**

- Enable companies/enterprises to use/process anonymised data (indenpendently from GDPR requirements)

**Drawbacks:**

- Complexity (Privacy-utility trade-offs)
- Inference Attacks
- Full Trust on the remote server (server provider)

# Discussion: technical challenges to implement PET in urban spaces

- **Privacy preserving auditing tools**
  - Transparency and auditing concerns have been addressed by a minority of works ➔ Need to address these requirements which have been emphasized by recent regulations.
  - *Examples of recent works: Intel-SGX provenance systems, informed consent for e-health applications, transactional privacy in blockchain-based systems*

- **Privacy preserving data collection techniques**
  - Massive collection of sensitive data, by AI-based systems, in emerging pervasive applications ➔ Need for privacy preserving data collection processes,
  - *Recent works: privacy-enhancing cryptographic methods (i.e., homomorphic encryption on encrypted users' data) to meet an agreement between privacy, efficiency and quality of experience.*

- **Privacy sensitive processing for ubiquitous environments**
  - Need for lightweight security/privacy solutions adapted to resource-constrained devices (mobile devices).
  - *Examples of recent solutions: Intel-SGX based solutions for pervasive/ubiquitous applications.*

# Discussion: legal, social and econmic challenges to implement PET in urban spaces

- **Legal challenges**
  - Several regulations and laws regarding data protection
  - *Research works: translations laws/texts into efficient technical solutions, namely for users' consent collection and data transfers between several service providers*

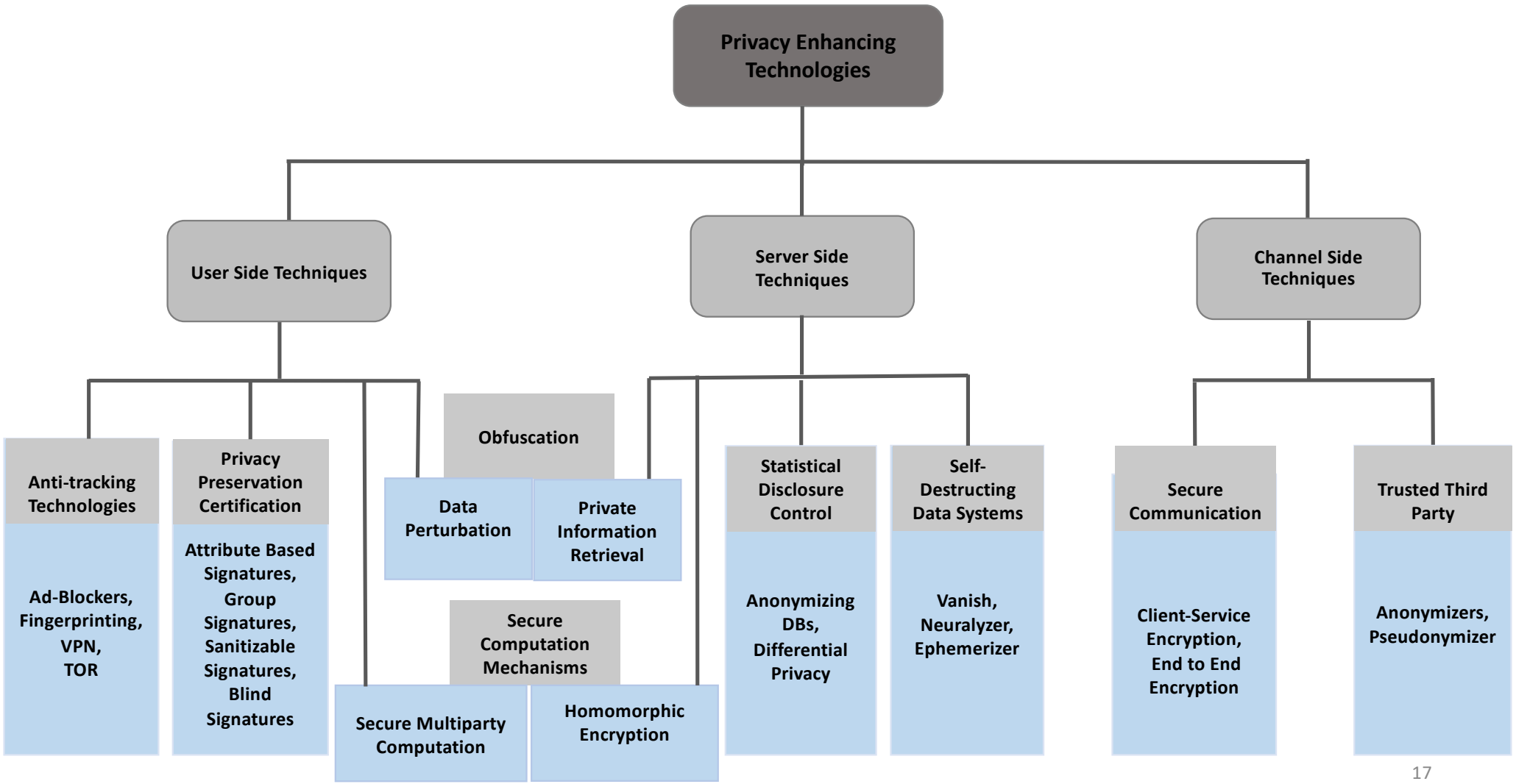
- **Social and economic challenges**
  - User-experience is the main pillar to define the perimeter of private information and the utility over the adoptions of PETs
  - Several mediated cases: Kodak cameras, Google glasses, LG-TV..
  - Trade-off between protection strategies and economic activities
  - *Recent works: user empowerment approaches, the impact of data collection abuse practices on consumers' attitudes…*

# Conclusion

- It is important to emphasize that due to the diversity of smart applications, different privacy technologies need to be combined to ensure an acceptable level of privacy.
  - Smart cities combine so many technological components that it is not enough to simply apply privacy technologies to each component.
  - The interactions between technologies and data have to be considered to design *"joint privacy technologies."*

- Several solutions can be deployed at different levels, the main challenge consist on the resolving the hard equation between privacy, utility and fairness emphasized by the usage of AI algorithms in urban spaces.

Any questions?


Privacy Enhancing Technologies
User Side Techniques
Server Side Techniques
Channel Side Techniques
Anti-tracking Technologies
Ad-Blockers, Fingerprinting, VPN, TOR
Privacy Preservation Certification
Attribute Based Signatures, Group Signatures, Sanitizable Signatures, Blind Signatures
Obfuscation
Data Perturbation
Private Information Retrieval
Secure Computation Mechanisms
Secure Multiparty Computation
Homomorphic Encryption
Statistical Disclosure Control
Anonymizing DBs, Differential Privacy
Self-Destructing Data Systems
Vanish, Neuralyzer, Ephemerizer
Secure Communication
Client-Service Encryption, End to End Encryption
Trusted Third Party
Anonymizers, Pseudonymizer