

Mathematical methods and protection of privacy

Milan Todorović, Silvia Ghilezan, Zoran Ognjanović
Mathematical institute SASA



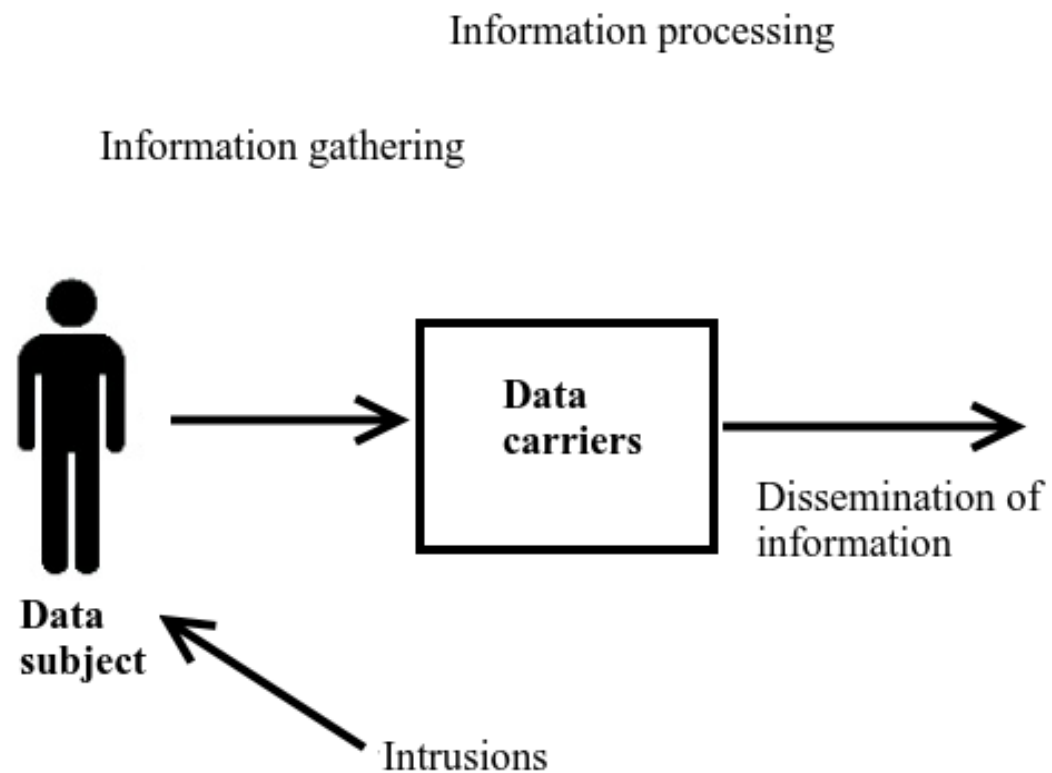
Information technologies and privacy

- Development of new information technologies and privacy
- Availability and usage of information
- Aspects of privacy

Privacy is ability and possibility of controlling both access to information and to whom this information is transmitted.



Four types of invasion of privacy (Solove's taxonomy)



Information age

Present age can be called *information age*

- Digital trace
 - Interests
 - Characteristics
 - Beliefs
 - Personal data (phone number, address, medical data)

Digital trace is created by using different services that are now part of everyday life (social networks, search engines, e-mail,...)



Information age



Internet of things

Internet of things

- Large number of sensors – data collection
- Wireless network – data transmission

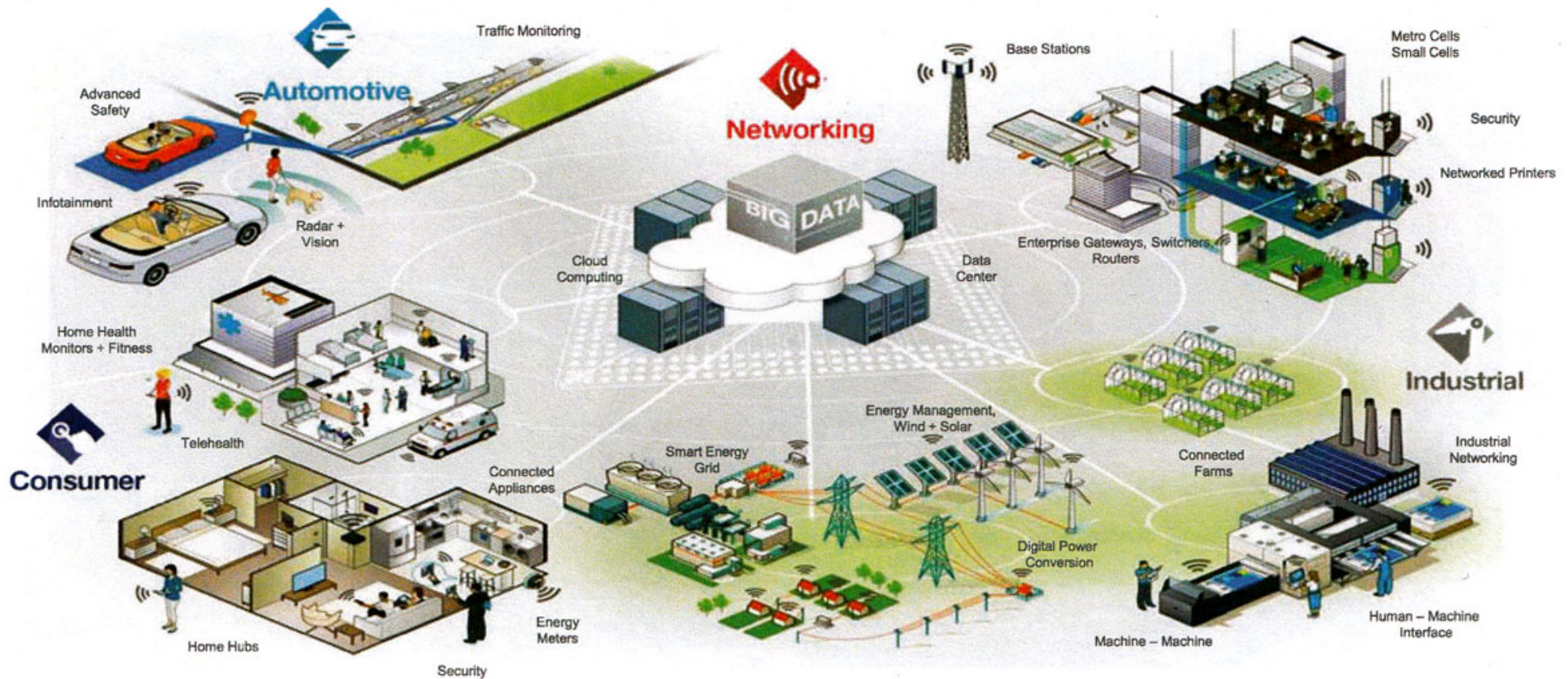
The data is the most diverse:

- Temperature
- Energy consumption
- Different medical data (monitoring of patients' condition)



Internet of things

The Internet of Things

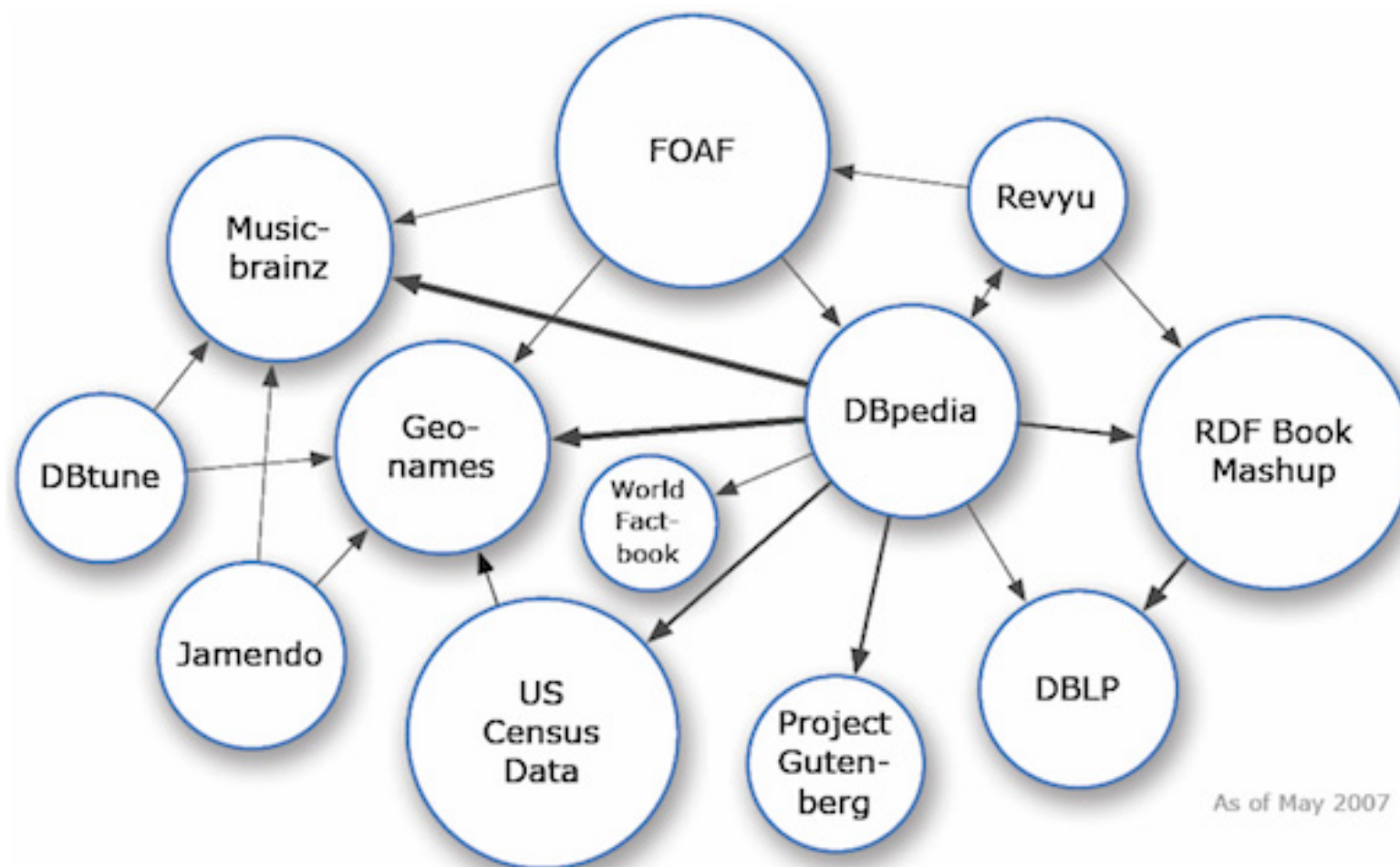


Cloud computing

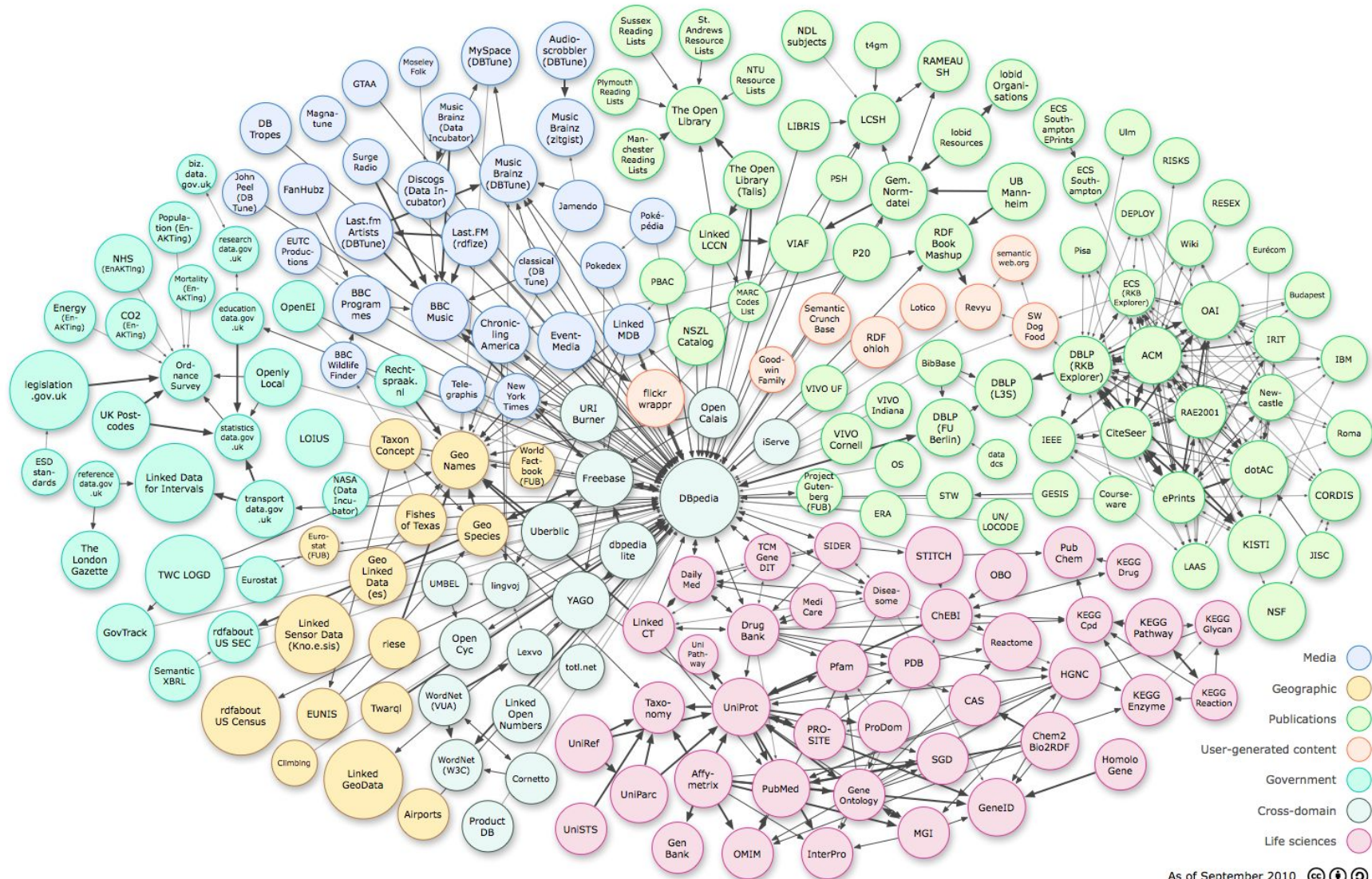
Cloud computing




- Computer infrastructure
- Access to remote set of resources
- Data resides on remote location
- Multiple users share resources
- Cloud providers

Cloud computing



Cloud computing



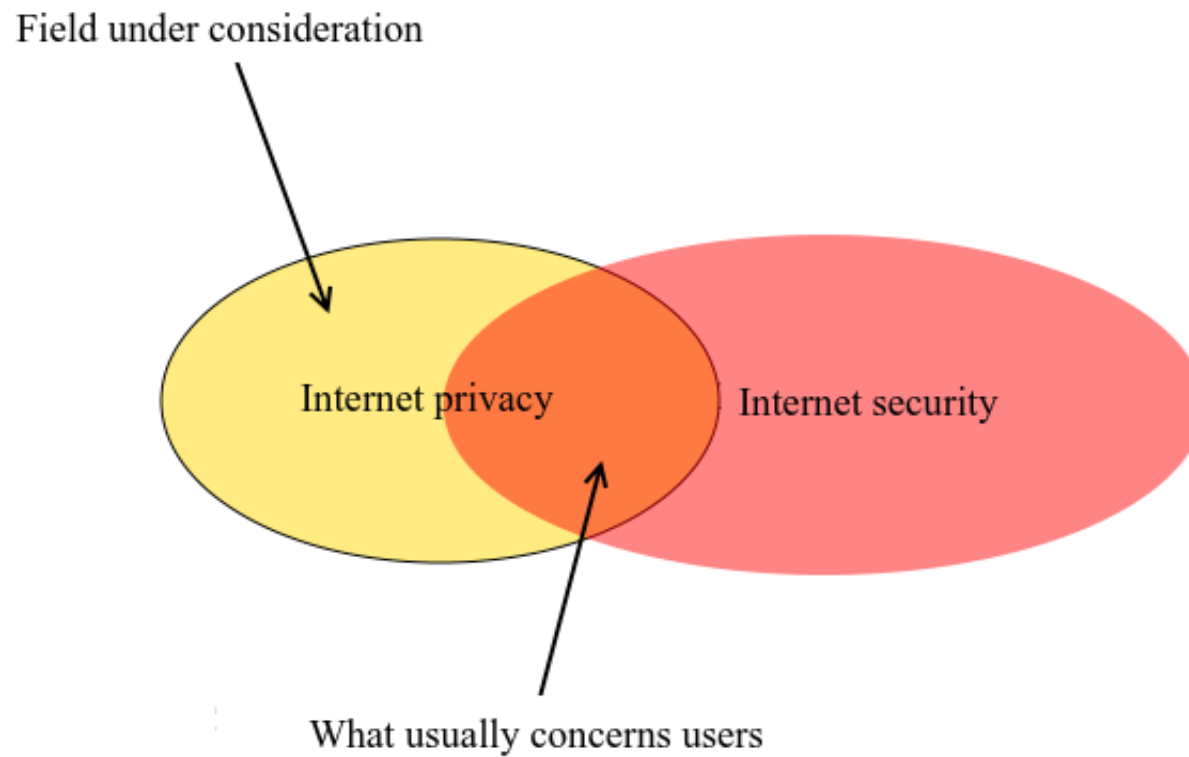
As of September 2010   

General Data Protection Regulation

Represents EU law on data protection that was implemented on 25. May 2018. Some important points from the law:

- Responsibility and accountability
- Data protection by design and by default
- Pseudonymisation
- Right of access
- Right to erasure
- Records of processing activities

What worries users the most?



Mathematical models and formal methods

Mathematical models and formal methods have become basic tool for development of reliable software and hardware.

Directions for applying mathematical models to privacy protection:

- Computational models for privacy

Turing machine, formal calculi, distributed and concurrent systems,

Access control, logic systems, type systems

S.G. "Types and Privacy" - Conference Formal Methods on Privacy 2016

- Formal methods for privacy

Model checking

Automated provers



Mathematical models and formal methods

- Differential privacy and probabilistic methods of reasoning

Zoran Ognjanović, Miodrag Rašković, Zoran Marković: *Probability Logics, Probability-Based Formalization of Uncertain Reasoning*, Springer, 2016.

- Cryptographic methods for privacy

Miodrag J. Mihaljević and Hideki Imai: *Privacy Preserving Light-Weight Authentication Based on a Variant of Niederreiter Public-Key Encryption*, Symposium on Cryptology and Information Security - SCIS 2014.

Mathematical models and formal methods

- Application in social networks, databases, medical data, linked data

Svetlana Jakšić, Jovanka Pantović, Silvia Ghilezan: *Privacy for Linked Data*, Mathematical Structures in Computer Science 27(1): 33-53 (2017).

- Open data

BE-OPEN Portal of open science

- Legal aspects of privacy in information systems
- Examples of good practice:

Greece: *The Transposition of European Union Open Data/Public Sector Information Policies in Greece: A Critical Analysis*, Prodromos Tsiavos, Petros Stefaneas, and Theodoros Karounos

USA: Adam Barth, Anupam Datta, John C. Mitchell, and Hellen Nissenbaum: *Privacy and contextual integrity: Framework and applications*. IEEE Symposium on Security and Privacy: 184–198 (2006).

Conclusion

Multidisciplinary teams: mathematicians, computer scientists, lawyers, sociologists and psychologists

Encouraging mathematical and multidisciplinary research, concerning privacy protection

