Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Mirko Zichichi

[1]Ontology Engineering Group,
Universidad Politécnica de Madrid
[2]Department of Computer Science and Engineering,
University of Bologna
[3]Department of Law,
University of Turin

Location Privacy and Inference in Online Social Networks

State of the Art

Online Social Networks (OSNs)

OSNs broke the boundaries between **authorship** and **readership**:

users produce the data that is consumed by other users

Location Data

"*Geoprivacy manifesto*" [Keßler and McKenzie, 2018] - **Location data**:

- is substantially **different** from the rest of personal data *(Thesis 1)*
- is **easy to capture** thanks to mobile devices and easy-to use APIs *(Thesis 2)*
- is more **useful when shared**, since it can improve the quality of services *(Thesis 3)*
- allows to **infer individuals activities** *(Thesis 5)*
  that they **never intended or agreed to share** with a service (Thesis 6)

Location Privacy and Inference

Spatial-Temporal Cloaking, **Obfuscation** → data can still be **de-anonymized** and used for **inferences**:

- **background knowledge** + anonymous OSNs data → can lead to **identify** individuals and to discover their **private attributes** [Qian et al., 2016]
- **social structures** information →
  - **friendships** links
  - fine-grained **users' position**, even when they **keep their data private** but their friends do not [Sadilek et al., 2012, Jurgens, 2013]
- "**co-location**" information from privacy sensitive user' friends [Olteanu et al., 2014]
  - pictures and **messages** [Ajao et al., 2015]
  - **spatiotemporal correlations** [Yamaguchi et al., 2014]

Economics of Location Information

- "**Digital twin**" → sold in the **adtech industry**.
- ↑ understanding **activity** and **lifestyle** patterns ⇒ ↑ intrusive **recommendations**.

Consumers Privacy Paradox [Norberg et al., 2007]

attitude: profess their need for privacy (general)

behavior: remain user of the tech that track and share their data (contextual)

- "**Privacy Calculus**" [Laufer and Wolfe, 1977]:

$$\text{perceived value of disclosure utility} = \frac{\mathit{privacy\ risk}}{\mathit{benefits}}$$

- Correct estimation undermined by **asymmetric information** or **unawareness of possible alternative solutions** [Acquisti et al., 2016].

Research Questions, Objectives, Methods

General Objective

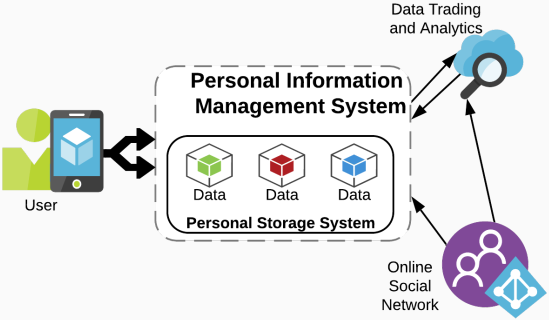
To design methodologies and systems that direct the **control** of the **flow** of **personal data** towards **individuals**.

"*privacy is not the opposite of sharing– rather, it is control over sharing*"
[Acquisti et al., 2016]
(Westin's and the IAPP's view)

Q1. Are distributed technologies and semantic web standards able to optimally support data protection and interoperability following the IoP paradigm?

Internet of Persons (IoP) is emerging as a paradigm that places individuals and their personal devices at the heart of the data management design.

O1. Design of a Personal Information Management System (PIMS)


Data Trading and Analytics
Personal Information Management System
Data
Data
Data
Personal Storage System
User
Online Social Network

Q1. Are distributed technologies and semantic web standards able to optimally support data protection and interoperability following the IoP paradigm?

O2. Specify languages and protocols that favour personal data interoperability and prevent interdependent privacy infringements

- **Semantic Web technologies**
- **Interdependent privacy infringements**: access to a user personal data without his consent through another user that has legitimate access
- **Linked Data + PIMS**: link interdependent data → confine this information and limit others' personal data disclosure

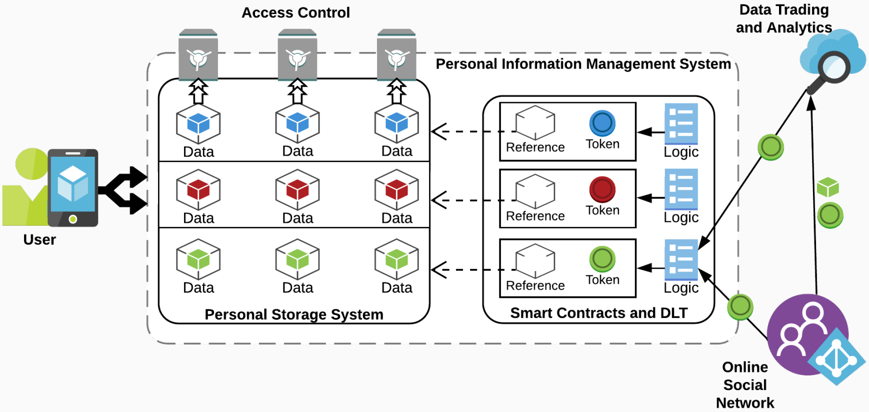
Q2. Can smart contracts represent and reason with policies to regulate the transmission and processing of personal data?

GDPR principles:

- **informed explanation**, by giving notice of use
- **specificity**, by providing the exact terms of the processing activity
- **consent**, by obtaining the free and unequivocal consent of the individual

Q2. Can smart contracts represent and reason with policies to regulate the transmission and processing of personal data?

O3. Specify the languages and algorithms to control the flow of personal data extending the private property paradigm



Q2. Can smart contracts represent and reason with policies to regulate the transmission and processing of personal data?

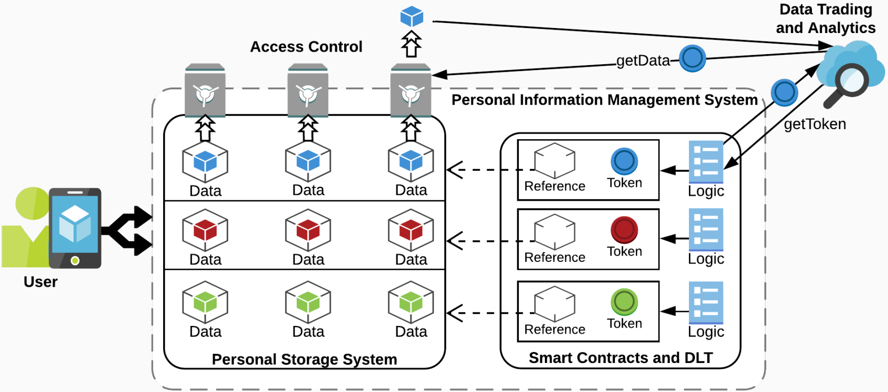
- Transactions recorded in smart contracts
  → **proof** of the **granting** of the use of the data and their **conditions** of use.

- The user can invoke this information in the event of a **dispute**.

- This proof can increase in **value** and thus take the form of an **exchanged asset**

Q3. Can PIMS ad SC allow the user to trade privacy for benefits, once the perceived utility value has been assessed with the help of a technology assistant?

“*My data are mine*” [Isabelle et al., 2018, Bock, 2018].



Q3. Can PIMS ad SC allow the user to trade privacy for benefits, once the perceived utility value has been assessed with the help of a technology assistant?

O4. Provide means to inform users about the inferences that can be performed on their location data

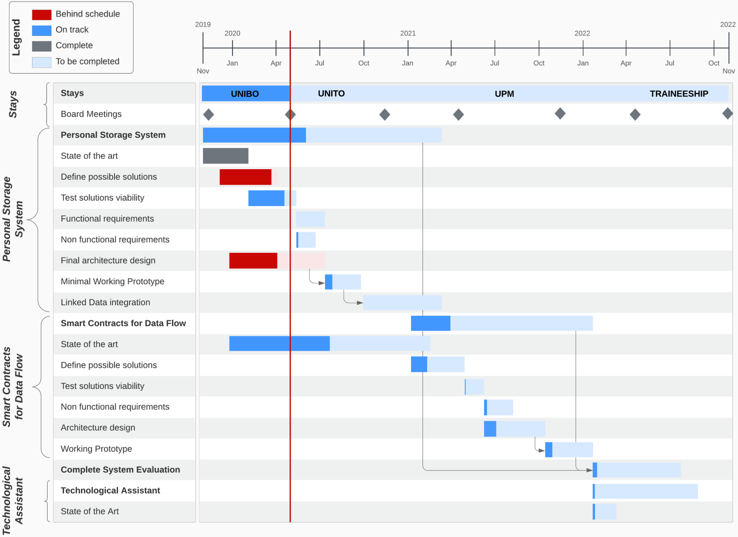
- A **technology assistant** →
  - provide all the information necessary for **consent** to be given
  - produce possible **inferences** to show to the user
  - help **trade-off** between privacy and utility ⇒ **privacy levels**

Conclusion

Related Works

- **My related works**
  Personal storage system & Personal Data Market Place
- **Similar approaches**
  Solid, Decode, MyHealthMyData
- **PIMS companies**
  Truonomi, digi.me, UBDI, Kork, BurstIQ

Workplan


Legend
Behind schedule
On track
Complete
To be completed
2019
2020
2021
2022
2022
Nov
Jan
Apr
Jul
Oct
Jan
Apr
Jul
Oct
Jan
Apr
Jul
Oct
Nov
Stays
Stays
UNIBO
UNITO
UPM
TRAINEESHIP
Board Meetings
Personal Storage System
Personal Storage System
State of the art
Define possible solutions
Test solutions viability
Functional requirements
Non functional requirements
Final architecture design
Minimal Working Prototype
Linked Data integration
Smart Contracts for Data Flow
Smart Contracts for Data Flow
State of the art
Define possible solutions
Test solutions viability
Non functional requirements
Architecture design
Working Prototype
Complete System Evaluation
Technological Assistant
Technological Assistant
State of the Art

Communication Results to Non-Expert Audience

- People need to understand their location data **real value**
- Control by **Disintermediation**
- **COVID-19** - PEPP-PT, DP-3T,...

Thanks for your attention!

Bibliography i

- Acquisti, A., Taylor, C., and Wagman, L. (2016).
  The economics of privacy.
  Journal of economic Literature, 54(2):442–92.
- Ajao, O., Hong, J., and Liu, W. (2015).
  A survey of location inference techniques on twitter.
  Journal of Information Science, 41(6):855–864.
- Bock, S. (2018).
  My data is mine-users' handling of personal data in everyday life.
  SICHERHEIT 2018.
- Isabelle, L., Pelics, G., Binctin, N., and Pez-Pérard, V. (2018).
  My data are mine: Why we should have ownership rights on our personal data.

Bibliography ii

- Jurgens, D. (2013).
  That's what friends are for: Inferring location in online social media platforms based on social relationships.
  In *Seventh International AAAI Conference on Weblogs and Social Media.*
- Keßler, C. and McKenzie, G. (2018).
  A geoprivacy manifesto.
  Transactions in GIS, 22(1):3–19.
- Laufer, R. S. and Wolfe, M. (1977).
  Privacy as a concept and a social issue: A multidimensional developmental theory.
  Journal of social Issues, 33(3):22–42.

Bibliography iii

- Norberg, P. A., Horne, D. R., and Horne, D. A. (2007).
  The privacy paradox: Personal information disclosure intentions versus behaviors.
  Journal of consumer affairs, 41(1):100–126.

- Olteanu, A.-M., Huguenin, K., Shokri, R., and Hubaux, J.-P. (2014).
  Quantifying the effect of co-location information on location privacy.
  In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 184–203. Springer.

Bibliography iv

Qian, J., Li, X.-Y., Zhang, C., and Chen, L. (2016).
De-anonymizing social networks and inferring private attributes using knowledge graphs.
In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9. IEEE.

Sadilek, A., Kautz, H., and Bigham, J. P. (2012).
Finding your friends and following them to where you are.
In *Proceedings of the fifth ACM international conference on Web search and data mining*, pages 723–732.

Bibliography v

Yamaguchi, Y., Amagasa, T., Kitagawa, H., and Ikawa, Y. (2014).
Online user location inference exploiting spatiotemporal correlations in social streams.
In *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management*, pages 1139–1148.