D2.1 – Orientation camp

Grant Agreement nº:	MSCA ITN EJD n. 814177
Project Acronym:	LAST-JD-RIoE
Project Title:	Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything (LAST-JD-RIoE)
Website:	https://www.last-jd-rioe.eu/
Contractual delivery date:	30/11/2019
Actual delivery date:	03/12/2019
Contributing WP	WP2
Dissemination level:	Public
Deliverable leader:	UNIBO
Contributors:	all beneficiaries

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177

Document History

Version	Date	Author	Partner	Description
1.0	03/09/2019	Monica Palmirani	UNIBO	First draft
2.0	10/10/2019	Monica Palmirani	UNIBO	Contribution of Paragraphs
3.0	10/11/2019	Monica Palmirani	UNIBO	Second draft
4.0	03/12/2019	Monica Palmirani	UNIBO	Final version

Contributors

Partner	Name	Role	Contribution
All			

Table of Contents

Executive Summary

This document presents the Deliverable D2.1, which reports of the Welcome Camp of Law, Science and Technology-RIoE.

The Welcome Camp was organized jointly with the Erasmus Mundus Law, Science, and Technology board. We have three different "Law, Science and Technology" PhD cohorts: Erasmus Mundus project in the last cycle (2016-2017); two national-funded cycles (2017-2018 and 2018-2019); MSCA-ITN cycle (2019-2020), four PhD students funded by national funds and one PhD student funded by University of Luxembourg. In total we have 37 PhD students.

The Welcome Camp is organized for all those students in order to create a large community considering that in this moment we have about 60 PhD researcher affiliate to the brand "Law, Science and Technology". Some of them already work as lecture or associate professors of ICT and Law or Legal informatics disciplines in European Universities (e.g., University of Luxembourg, Uppsala University, Leiden University, etc.) or in extra-European Universities (e.g., Shahid Beheshti University, University of New York of Tirana, University of Dhaka).

MSCA-ITN Law, Science and Technology-RIoE (Rights of Internet of Everything) is a continuation of this success in order to consolidate the community started at 2012.

The Welcome Camp included five main activities:

1. supervisory board and scientific committee in order to assess the status of the MSCA-ITN project and the research of each PhD candidate;
2. presentation of the MSCA-ITN organization, goals, deliverables, workpackages, rules;
3. presentation of the PhD candidates to the others;
4. presentation of the researches and discussion with the scientific committee;
5. lectures by experts and debate.

.

1 Welcome Camp

The Welcome Camp was held in Bologna at 18-19-20 November. It was organized jointly with the Erasmus Mundus Law, Science, and Technology board. We have three different “Law, Science and Technology” PhD cohorts: i) Erasmus Mundus project in the last cycle (2016-2017); ii) two national-funded cycles (2017-2018 and 2018-2019); MSCA-ITN cycle (2019-2020), four PhD students funded by national funds and one PhD student funded by University of Luxembourg. In total we have 37 PhD students.

The “Welcome Camp” was organized for all those students in order to create a large community considering that in this moment we have about 60 PhD researcher affiliate to the brand “Law, Science and Technology”. Some of them already work as lecture or associate professors of ICT and Law or Legal informatics disciplines in European Universities (e.g., University of Luxembourg, Uppsala University, Leiden University, etc.) or in extra-European Universities (e.g., Shahid Beheshti University, University of New York of Tirana, University of Dhaka).

MSCA-ITN Law, Science and Technology-RIoE (Rights of Internet of Everything) is a continuation of this success in order to consolidate the community started at 2012.

In this light the “Welcome Camp” included all the PhD students (any cohorts), the supervisory board, the scientific committee and the experts of the domain.

We have organized the Welcome Camp as an event where the new PhD candidates of MSCA-ITN can participate to the presentation of the research projects of the others, where they can take inspiration from the common methodology that is based on interdisciplinarity, investigation, and comparative law method. The new PhD candidates also had the occasion to take advantages from the existing state of the art presented by the colleagues and to listen the comments and the debate with the professors present in the room.

The Welcome Camp included five main activities:

1. supervisory board and scientific committee in order to assess the status of the MSCA-ITN project and the research of each PhD candidate. In this section we dedicated a slot to listen the MSCA-ITN PhD candidate and to collect their requests;
2. presentation of the MSCA-ITN organization, goals, deliverables, workpackage, rules;
3. presentation of the PhD candidate to the others;
4. presentation of the researches and discussion with the scientific committee;
5. lectures by experts and debate. In this context we have organized four lectures from experts: Prof. G. Sartor on AI and Law risks and opportunities, Prof. A. Vedder on the Ethics aspect of AI, Prof. M. Theobald on the technical aspect of the big data, Prof. V. Manes on AI in the eJustice field with particular regard to the Criminal domain.

The attendees to the Welcome Camp was about 60 participants coming also from the Law School, Computer Science and Engineering Department, Economic Department of University of Bologna. This participation was really appreciated in order to improve the feedbacks to the PhD candidates on their researches, to enhance the interdisciplinarity, to support multi-level approach in the methodology.

You can see in the annexes the following information:

1. Annex A: Agenda of the Welcome Camp;
2. Annex B: presentation of the MSCA-ITN;
3. Annex C: presentations of the experts;

4. Annex D: presentation of the PhD candidates.

Annex A – Agenda of the Welcome Camp

Joint International Doctoral Degree in Law, Science and technology

MARIE CURIE ACTIONS

Erasmus Mundus

Rights of Internet of Everything

International Joint Doctorate in Law, Science and Technology Rights of Internet of Everything

Welcome Camp Event

jointly with Supervisory Board Scientific Committee A. A. 2019-2020

Bologna, 18-19-20 Nov. 2019

CIRSFID, via Galliera 3.
Sala Kelsen

18TH NOVEMBER 2019

RESTRICTED TO THE SUPERVISORY BOARD AND THE SCIENTIFIC COMMITTEE

9.30 Welcome with breakfast

10.00-13.00	LAST-JD-RIoE (Law, Science and Technology, Rights of Internet of Everything) MSCA ITN EJD (Marie Skłodowska-Curie actions European Joint Doctorates) Horizon 2020 EU project 814177
	1. Contract and financial issues 2. Amendment, ESR and mobility plans 3. ESR Career Development Plan 4. Industrial partners involvement 5. PhD regulations, Ethical code 6. Supervisioning rules and methods: assignment of the supervisors 7. Quality check of the activities, monitoring method and thesis criteria 8. WPs and leaders: Milestones and Deliverables, Timetable and deadlines 9. Courses and training: Moodle platform 10. Next Meetings 11. Open data and open access policies and policy for the reference/affiliation/citations 12. Dissemination event: Annual Conference and other events 13. Portal and marketing strategy 14. Social media policy

13.00-14.00 Lunch

14.00-15.00	Report of the administrative staff work to the doctoral board and academic committee and vice versa
	Discussion on the doctoral candidates progresses and outcomes A.A 2016-2017 (32° cycle) and A.A. 2017-2018 (33° cycle) A.A. 2018-2019 (34° cycle). 1. Passing of the term 2. Ratification of some changes of research topic or supervisorships 3. Evaluation and quality of the results: elaboration of the judgment for each student 4. Mobility plan 5. Conference and courses 6. Doctorate Training and Supervision Plan 7. Deliberation of costs 10% for conferences, workshops abroad
15.00-15.30	Meeting with the MSCA-ITN PhD candidates for questions and answers.

15.30-16.00 Coffee break

Doctoral Board open to all

16.00-16.30 Opening session by Prof. Monica Palmirani, coordinator of LAST-JD – RioE, Introduction of LAST-JD-RIoE (Law, Science and Technology, Rights of Internet of Everything) MSCA ITN EJD (Marie Skłodowska-Curie actions European Joint Doctorates) Horizon 2020 EU project 814177

16.30–18.30 Presentation

- Presentation of the doctoral candidates A.A. 2016-2017 (each student presents his/her research) - 5 students – 25 minutes each (125 minutes): Konaschevick Oleksii, Zavaleta Salinas Daniel, Alunge Rogers, Urbano Reviglio, Dameski Andrej - cycle 32°

18.35 – Closing

18.35-19.30 [Supervisor meetings - slot where PhD Candidates and supervisors can meet each others]

19th November 2019

Doctoral Board open to all

9.00 Welcome from pro-rector Antonino Rotolo and Giovanni Sartor

9.10-10.30 Presentation

- Presentation of the doctoral candidates A.A. 2018-2019 (each student presents his/her research) - 2 students – 20 minutes each (60 minutes): Ilaria Amantea, Ludovica Paseri,– cycle 34°

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) - 1 student – 15 minutes each (15 minutes): Varga Stephan - cycle 35°

10.30-11.00 Coffee Break

11.00-13.00 Invited talk and discussion

- Giovanni Sartor, EUI, *Artificial Intelligence: Challenges and Opportunities*
- Anton Vedder, KUL, *Ethics principles for AI in the IoT light*
- Martin Theobald, University of Luxembourg, *From Big Data to Big Knowledge*

13.00-14.00 Lunch

[Supervisor meetings - slot where PhD Candidates and supervisors can meet each others]

14.00-16.00 Presentation

- Presentation of the doctoral candidates A.A. 2017-2018 (each student presents his/her research) - 6 students – 20 minutes each (120 minutes): Giorgia Bincoletto, Chantal Bomprezzi, Salvatore Sapienza, Federico Galli, Valentina Leone, Davide Liga - cycle 33°

16.00-16.30 Coffee Break

16.30-18.30 Presentation

- Presentation of the doctoral candidates A.A. 2018-2019 (each student presents his/her research) - 4 students – 20 minutes each (80 minutes): Sofia Iacomussi, Claudio Novelli, Ingrad Alvarado Lopez, Abiodun Abdullahi Solanke - cycle 34°

18.30 – Closing

18.30-19.30 [Supervisor meetings - slot where PhD Candidates and supervisors can meet each others]

20.00 – Social Dinner

20th November 2019

DOCTORAL BOARD OPEN TO ALL

9.00 – Welcome
9.10-10.30 Presentation
Big Data and AI

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) - 5 students – 15 minutes each (75 minutes): Yacin Orhan Gazi, Podda Emaunela, Gartner Maximilian, Derutigliano, Jacopo Menghini - cycle 35°

10.30-11.00 Coffee Break
11.00-13.00 Presentation
IoT

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) - 4 students – 15 minutes each (60 minutes): Gennari Francesca, Neroni Isadora, Vogel Yannick, Lisha Qiao - cycle 35°

Health

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) - 4 students – 15 minutes each (60 minutes): Francesco Vigna, Aiste Gerybaite, Richard Rak, Bresic Daniela - cycle 35°

13.00-14.00 Lunch

[Supervisor meetings - slot where PhD Candidates and supervisors can meet each others]

14.00-15.00 Invited talk and discussion

- Vittorio Manes, University of Bologna, *Artificial Intelligence and eJustice*

15.00-16.00 Presentation

eJustice

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) – 1 student – 15 minutes each (15 minutes): Olimpia Barresi - cycle 35°

Security

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) – 2 students – 15 minutes each (30 minutes): Pier Giorgio Chiara, Liuwen Yu – cycle, - cycle 35°

16.00-16.30 Coffee Break

16.30-17.30 Presentation
Blockchain

- Presentation of the doctoral candidates A.A. 2019-2020 (each student presents his/her research) – 3 students – 15 minutes each (45 minutes): Pocher Nadia, Mirko Zichichi, Biagio Distefano - cycle 35°

17.30 -18.00 – Conclusions

- Assessment of the passage of the term for the doctoral candidates A.A. 2016-2017, A.A. 2017-2018, A.A. 2018-2019.

Annex B – MSCA-ITN LAST-JD-RIoE main tasks

Rights of Internet of Everything

MARIE CURIE ACTIONS

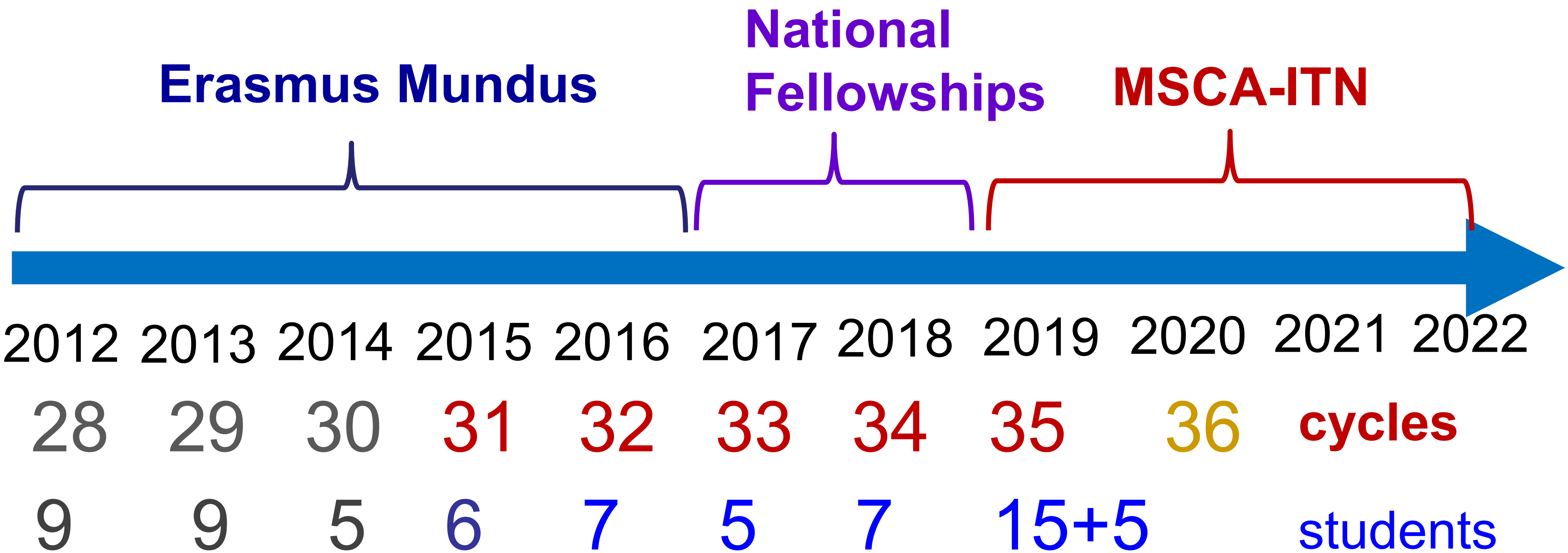
Law, Science and Technology
MSCA ITN EJD n. 814177

Erasmus+

Law, Science and Technology

Bologna ***November, 18-19-20 - 2019***

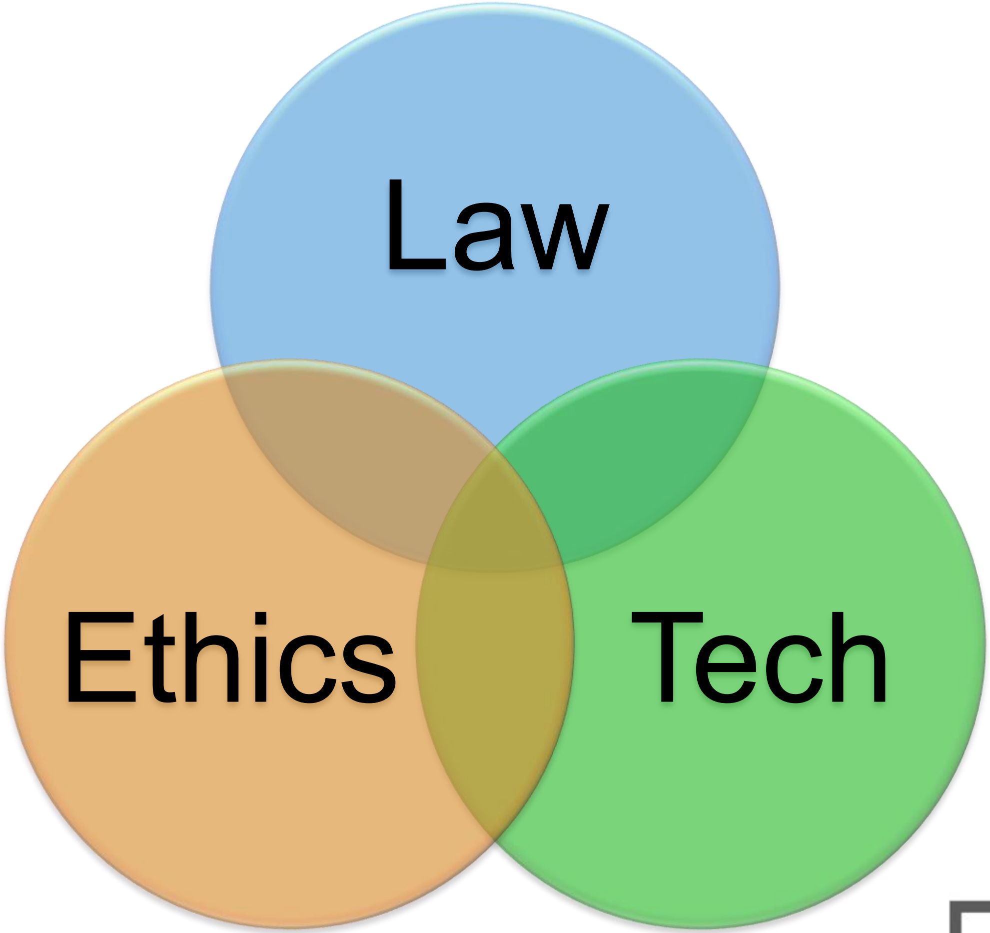
Law, Science and Technology



Why “Law, Science and Technology”

- The Joint International Doctoral Degree in “Law, Science and Technology” is an **interdisciplinary** integrated doctorate designed to address new challenges in **legal, socio-ethical and technical domains** arising from the information society and newly emerging technologies.
- New opportunities and risks for the society
- New professional operators for growth and job

Interdisciplinary approach



9 Beneficiaries, 7 countries

- UNIBO – Law School
- UNITO – Computer science and Law School
- UAB – Law School
- UL – Computer science and Law School
- MRU – Law School
- KUL – Law School
- LUH – Law School
- UNIVIE – Law School
- UPM – Computer science

6 Associate Partners

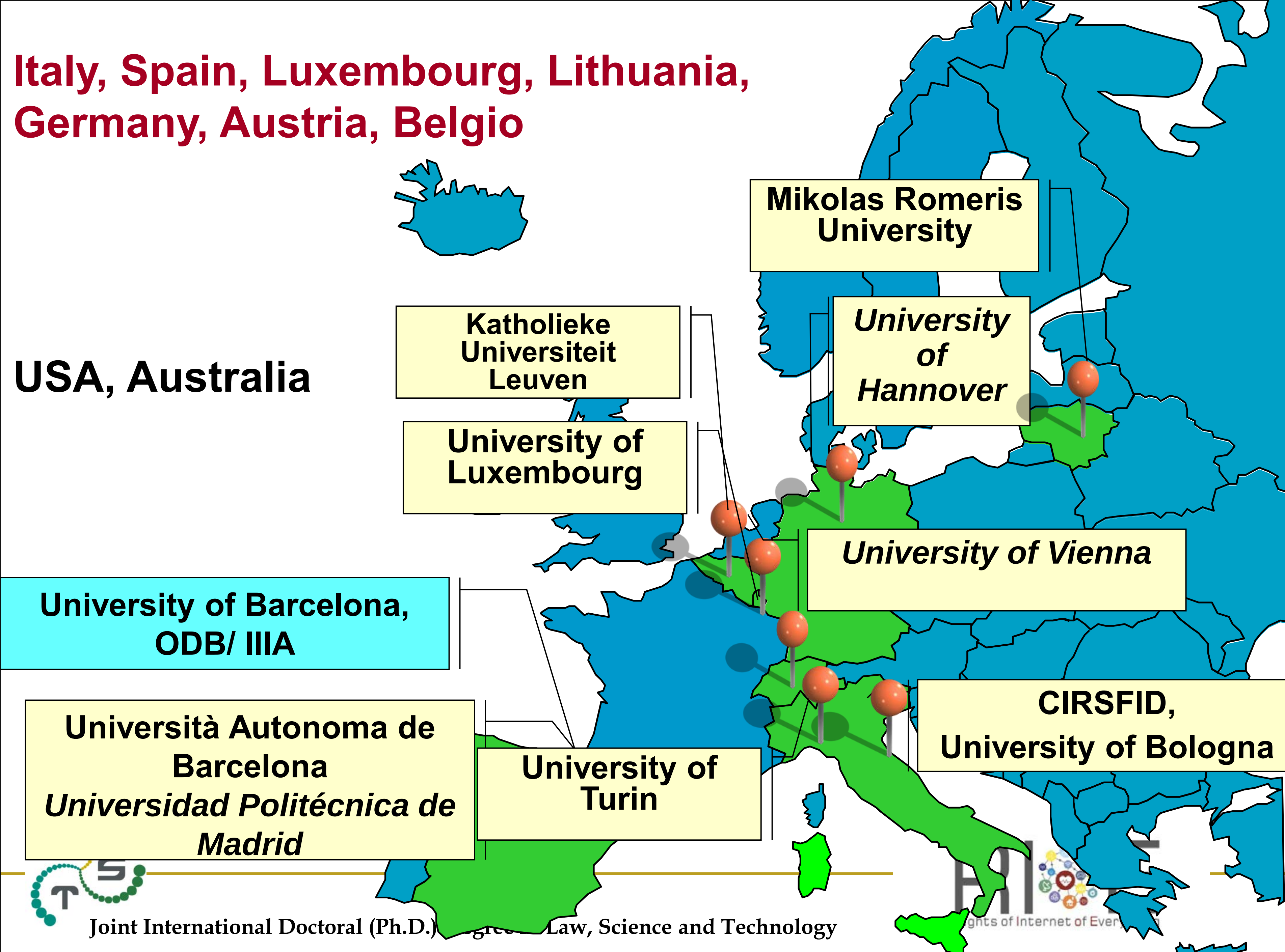
1. OBD, University of Barcellona
2. PITTS, University of Pittsburgh
3. Data61, CSIRO
4. CNR-ITTIG
5. La Trobe University, Australia
6. Università Piemonte Orientale

12 Industrial partners

1. APIS Europe A.D.
2. CELI S.r.l.
3. LIC
4. Nomotika
5. IoooTa S.r.l.
6. UAB Bioseka
7. tuOtempO
8. CARETEK
9. Consoft
10. AGILE LAB S.r.l.
11. BitNomos
12. Augeos

Italy, Spain, Luxembourg, Lithuania, Germany, Austria, Belgio

USA, Australia



Mobility Plan: 3 years, 3 mobiliy, 3 titles

First term:
1Nov-30 April2020

UNIBO

Second term:
1May-30Oct

UNITO UAB MRU

UL LUH UNIVIE UPM KUL

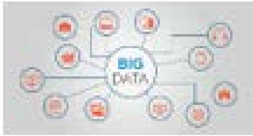
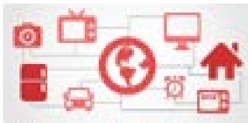
Third term: 1Nov2020-30April2021

CELI S.r.l. LIC IoooTa S.r.l. UAB Bioseka tuOtempO CARETEK Consoft AGILE LAB S.r.l. BitNomos Augeos

Six term: 1May-30Oct 2022

The remaining time you are located in the beneficiary premises

$\sum$

WP	Computer Science	Law	Ethical/Social
 Internet of Data	Governing algorithms in Big Data era balancing the new digital rights (UNIBO)	Big data analysis systems in IoE environment for managing privacy and digital identity: pseudonymity, deanonymization, right to be forgotten issues. (UNIBO)	Fundamental Rights in the IoE and Big Data New Digital Era. (LUH)
 Internet of Things	Security and privacy of resource constrained devices (UL)	Legal issues of IoT devices in home scenario: from data ownership to competition law (MRU)	Surveillance risk in IoT applied in Smart Cities (UAB)
 Internet of Persons	Location privacy and inference in online social networks (MUP)	Neo-commodification of persons: how their personal data are exploited and what is the impact on the shared economy (UNITO)	Influentiable Autonomy and Predictable Freedom in the IoE: beyond the automatic algorithm decisions (UNIBO)
 Internet of Healthcare	Big Data for Health in IoE in emergency situations (UNITO)	Privacy and Data Protection Aspects in IoH and Impact Assessment for minimizing the Digital Risk and guarantee the dignity of the person (UNIVIE)	Ethical, Legal and Social issues of eHealth for sharing personal sensitive data in IoE platform (KUL)
 Internet of Money	Risk analysis of distributed ledger technologies for transaction and management of securities (LUX)	Distributed ledger technologies between anonymity and publicity (UAB)	Distributed ledger technologies beyond financial applications: eDemocracy and new form of Governance (UNIVIE)

=IoE

ESRs

1, 2, 3

4, 5, 6

7, 8, 9

10, 11, 12

13, 14, 15

WP N.	WP Title	Beneficiary No.	Start Month	End Month	Activity Type	Beneficiary Short Name	ESR involvement
1	Recruitment	1	M1	M7-included	Management	UNIBO	
2	Training	8	M8	M43-included	Training	UNIVIE	1-15
3	Internet of Data	3	M8	M48	Research	UL	1,2,3
4	Internet of Things	4	M8	M48	Research	UAB	4,5,6
5	Internet of Persons	2	M8	M48	Research	UNITO	7,8,9
6	Internet of Healthcare	6	M8	M48	Research	KUL	10,11,12
7	Internet of Money	9	M8	M48	Research	UPM	13,14,15
8	Evaluation	5	M8	M48	Management	MRU	1-15
9	Dissemination / engagement	7	M1	M48	Dissemination	LUH	1-15
10	Management	1	M1	M48	Management	UNIBO	(representative)

31/03/2021 - DELIVERABLES

Dissemination Events

- April 1-2-3 2020 next Board - fixed
- Annual network wide event + mid-term audit July 2-3 2020 - fixed
- Annual conference 9-10-11 Nov. 2020 – Bologna (Board also included)
- Annual network wide event (mid May 2021 SPAIN)
- 2 Webinar per year, blog, papers, newsletter, web site, social

Deadline and *modality* of the final defence

Bologna ***November, 18-19-20 - 2019***

Criteria for passing the term

- Full time PhD programme
- Respect the milestones and the substantial evidence of progresses
- Attending the 70% of lectures proposed by the host with active attitude
- Pass the assignments (papers, comment of case-law, etc.) - recommendation
- Positive evaluation from the supervisor (MAIN first) and the others recommended, in case of strong disagreement the Board will decide
- Progresses in the thesis
- Linguistic course (desirable not mandatory)

Passing the Ph.D. defense

- Thesis (70.000 words monograph – guidelines - or a 4 – including the rewording of the material coming from two papers
- Template “4 papers-based” – option recommended only to the computer science students with codification and programming part
  - 4 papers – 6.000 to 10.000 [recommended] words
  - Chapter of introduction 10.000 words
  - Chapter of conclusions 10.000 words
  - 60.000 words
- papers with co-authorships but we need authorisation and the contribution from the student
- Two papers for publication (or accepted for publication):
  - Conferences papers
  - Journal with peer reviews (also in Web)
  - Chapter of book (no peers!! but editorial board that evaluates the product
- Make at least one presentation in International Conference during the three years (mandatory)

- Criteria of quality of thesis: argumentation, state of the art, research questions, innovation and original outcomes, methodology/formal

From cycle XXXII– DEADLINE

DEADLINE	WHO	WHAT
15/9	BOARD	Passing/not passing the third year; Nomination of 2 external evaluators + 2 substitutes (possibly for each candidates); Nomination of the defence committee (possibly for each candidates)
30/09	Phd candidates	Fill in the request for the admission at the final defence at the PhD office (with the stamp)
31/10	**Phd candidates**	**Upload of the thesis by the PhD candidates who are admitted to the final defence, in the dedicated Unibo website (https://phdthesisreview.unibo.it).**
15/12	evaluators	fill in the judgment in the dedicated Unibo website (https://phdthesisreview.unibo.it) and admit the candidate at the defence or proposed a deferreal for 6 months.
15/01	PhD Coordinator	send to the PhD office the list of the admitted candidates
15/02	Admitted Phd candidates	The Admitted candidates have to: upload the thesis, send the signed declaration to the PhD office, complete the IRIS catalouge (publications), send the thesis the the defence committee members.

DEFENCE PERIOD: 15/03 – 15/04
MARCH 2020→2023

From cycle XXXII – DEADLINE - REFERRAL

DEADLINE	WHO	WHAT
15/6	Phd candidates	Upload of the thesis by the PhD candidates who after the deferral, are admitted to the final defence, in the dedicated Unibo website (https://phdthesisreview.unibo.it).
31/7	evaluators	fill in the judgment in the dedicated Unibo website (https://phdthesisreview.unibo.it) and admit the candidate at the defence or proposed a deferreal for 6 months.
10/9	PhD Coordinator	send to the PhD office the list of the admitted candidates
30/9	Admitted Phd candidates	The Admitted candidates have to: upload the thesis, send the signed declaration to the PhD office, complete the IRIS catalouge (publications), send the thesis the the defence committee members.

DEFENCE PERIOD: 15/10 – 15/11
October-November 2020→2023!!

MSCA-ITN

- Defense rules: depending to the co-tutelle
- We are collecting all the rules and we will provide a guideline

Supervisioning rules

- Main supervisor, co-supervisor
- One online/remote meeting each month with a little report in written by student

Affiliation rule:

“LAST-JD-RIoE MSCA-ITN EJD No 814177”

- **Beneficiary + mobility secondments**

Example: Mario Rossi, the beneficiary is UNIVIEN “PhD candidate of LAST-JD-RIoE, **University of Vienna (beneficiary)**, University of Bologna, University of Turin”

Open Access

- Papers should be produced in open access. Each university has an official repository and local rules. **D10.1 DMP data management plan**
- Each papers must be notified also to the coordinator of the MSCA-ITN (Foschi)
- Acknowledgement to the project:

“This project Law, Science and Technology Rights in xxxx has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177”

•

Financial and reimbursement rules

- All the conferences must be approved by the Board
- Financial reimbursement are eligible only if the Board already approved the conference
- Financial reimbursement rules depend to the beneficiary national regulation

Many thanks for the attention

Questions

last-jd@unibo.it

Annex C – Expert lectures

Rights of Internet of Everything

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Joint International Doctoral Degree in Law, Science and technology

INTERNATIONAL JOINT DOCTORATE IN LAW, SCIENCE AND TECHNOLOGY - RIGHTS OF INTERNET OF EVERYTHING

WELCOME CAMP

19 NOVEMBER - h. 11.00-13.00

- **GIOVANNI SARTOR, EUI,**
  Artificial Intelligence: Challenges and Opportunities
- **ANTON VEDDER, KUL,**
  Ethics principles for AI in the IoT light
- **MARTIN THEOBALD, UL,**
  From Big Data to Big Knowledge

20 NOVEMBER- h. 14.00-15.00

- **VITTORIO MANES, UNIBO,**
  Artificial Intelligence and eJustice

Kelsen Room

via Galliera, 3 - Bologna

INVITED LECTURERES WITH FINAL DISCUSSION

https://last-jd-rioe.eu/

Artificial Intelligence &
EU citizens/consumers

European University Institute

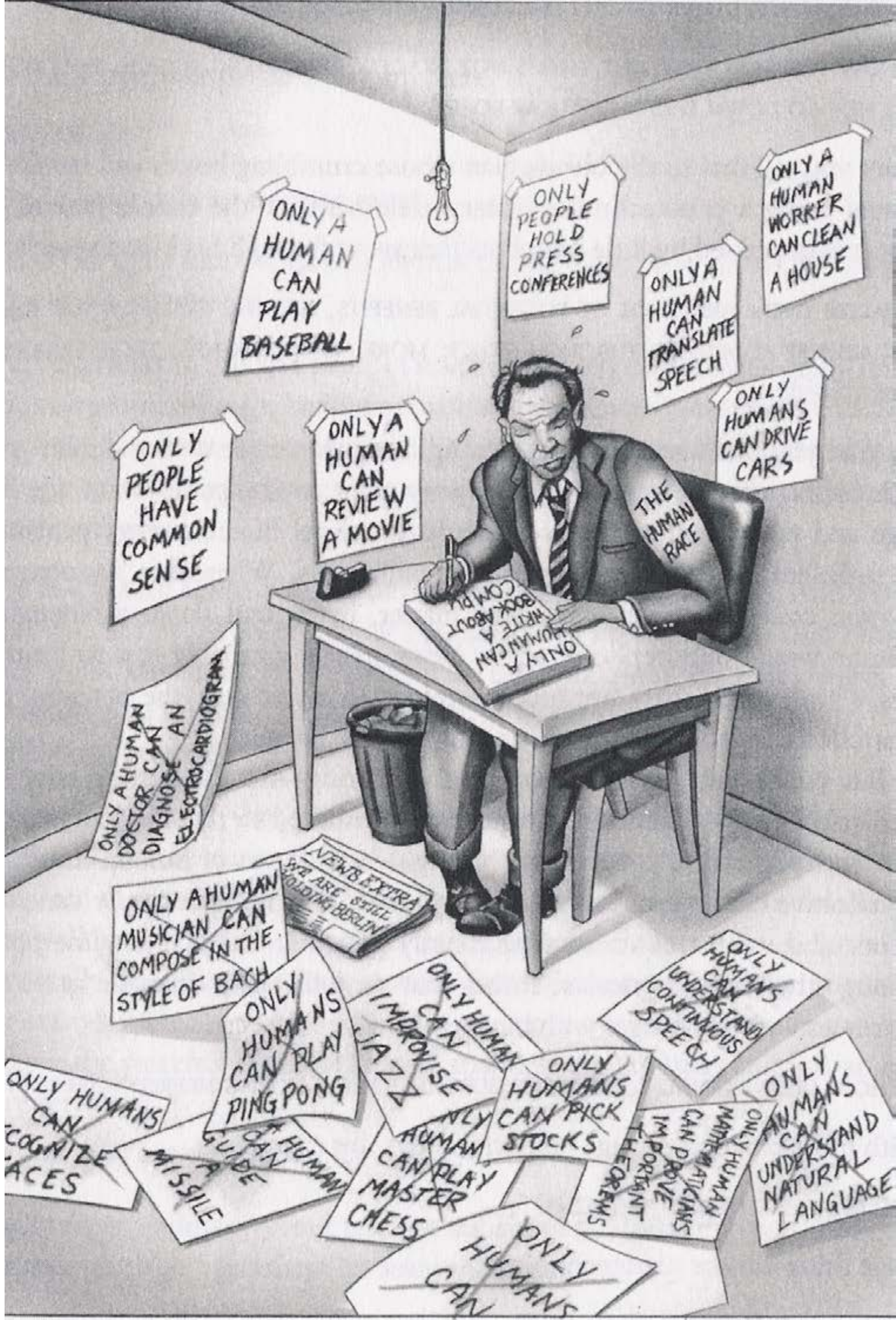
Giovanni Sartor

Cirsfid-University of Bologna, European University Institute,

The issue AI

- AI builds build machines that “perform functions that require intelligence when performed by people”

  - opportunities (development, sustainability, health, knowledge, etc.)
  - significant risks (unemployment, discrimination, exclusion, etc.).
- How to
  - support useful AI applications, and
  - Provide legal/ethical frameworks ensuring that AI contributes to the social good



Strong vs narrow AI

- Strong (general) AI:
  - System that exhibit most of the human cognitive skills, possibly at a superhuman level. A future existential risk?
- Narrow (specific) AI:
  - systems capable of satisfactorily carrying out single specific tasks requiring intelligence. Is is already with us and raises a number of legal and social issues

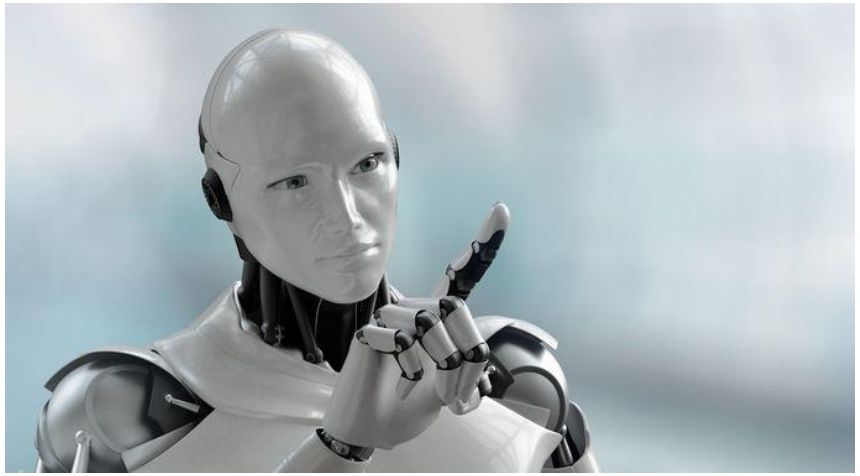
AI and the Internet: convergent evolutions

- Artificial intelligence reaches maturity
  - From human-made representations of knowledge and logical inference, to data-driven machine learning from examples and correlations
  - A unified paradigm: logic merges with statistics and neuro-science
- The Internet reaches maturity:
  - From an infrastructure for human communication to a global interconnected data infrastructure,
  - From access to passive information to active algorithmic intermediation

AI and the Internet: convergent successes

- AI: From toy examples to a host of real applications:
  - speech and image recognition, question-answering, recommendation, translation, planning, autonomous mobile robots, etc.
- The Internet: From message exchanges to the universal medium for any private and public services
  - shopping, banking, pay taxes, get benefits, information seeking, access to knowledge, social networking, etc.

What AI does and wants



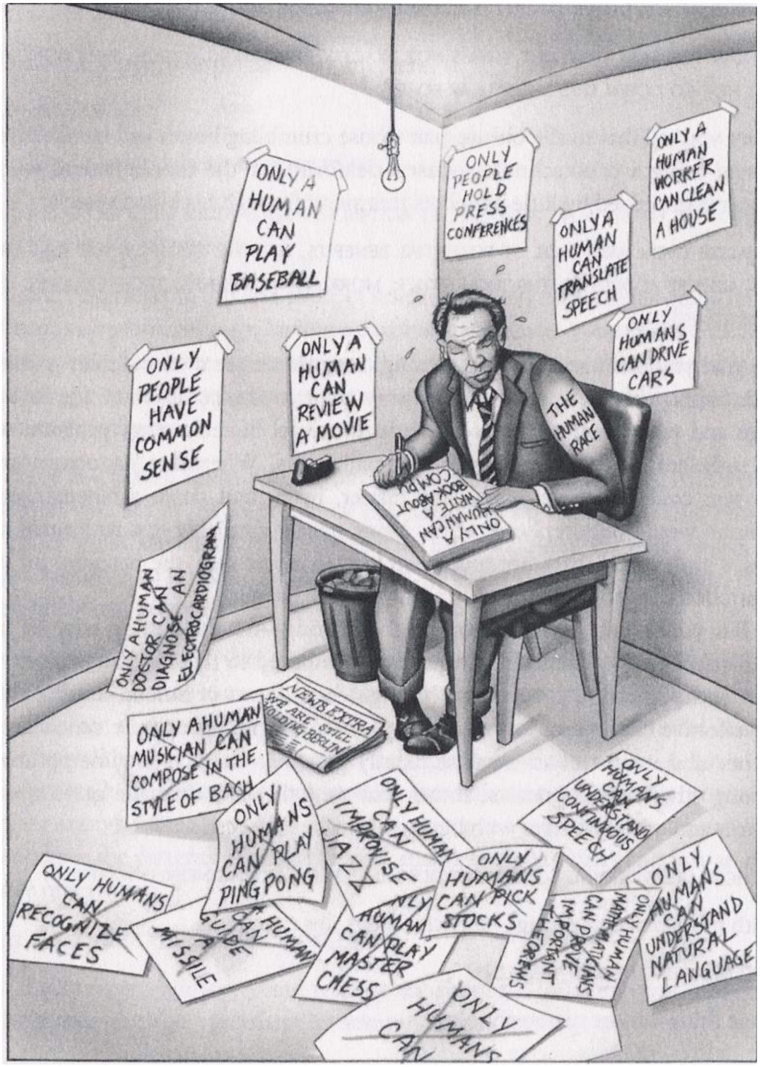
- What AI does
  - apply learning methods to vast sets of examples to discover correlations
  - make classifications and predictions based on correlations and data
  - learn from past successes and failures in classifying and predicting
- What AI wants
  - the largest sets of examples
  - Including as much data as possible to discover new correlations

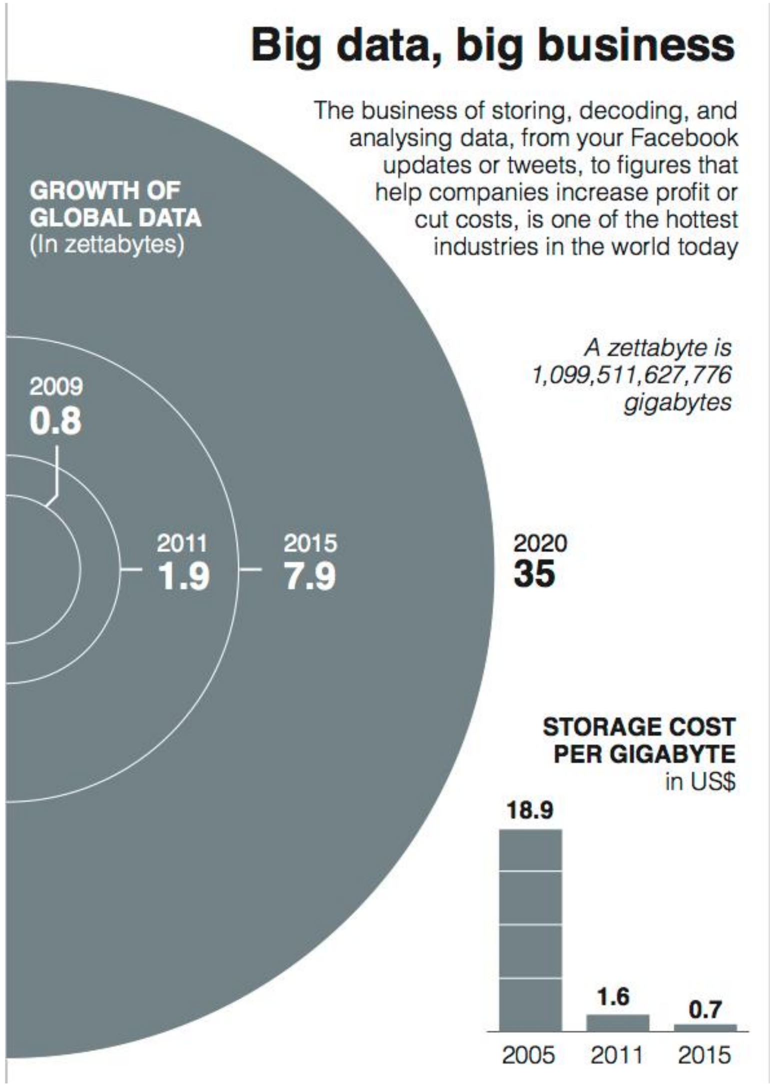
What the Internet does and want

- What the Internet does
  - enable human interaction
  - link billions of connected devices
  - collect all kind of data from physical and virtual environments
- What the Internet wants
  - services, providing intelligent and individualised solutions
  - the ability to extract useful knowledge from data

The great convergence

- The Internet provides AI with data
- AI enables the Internet to exploit the data



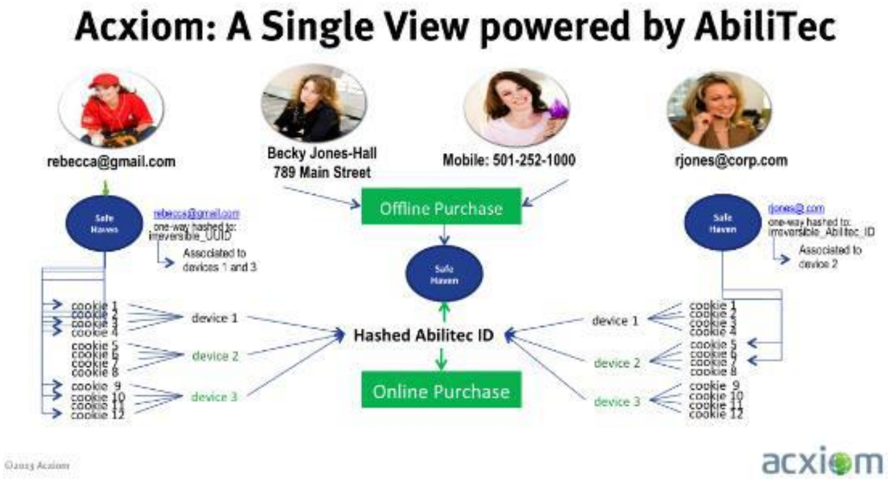


Data-hungry AI meets data-abundant Internet

- Pervasive data collection
- Learning from big data
- Ubiquitous algorithmic intelligence


Admiral to price car insurance based on Facebook posts

Insurer's algorithm analyses social media usage to identify safe drivers in unprecedented use of customer data

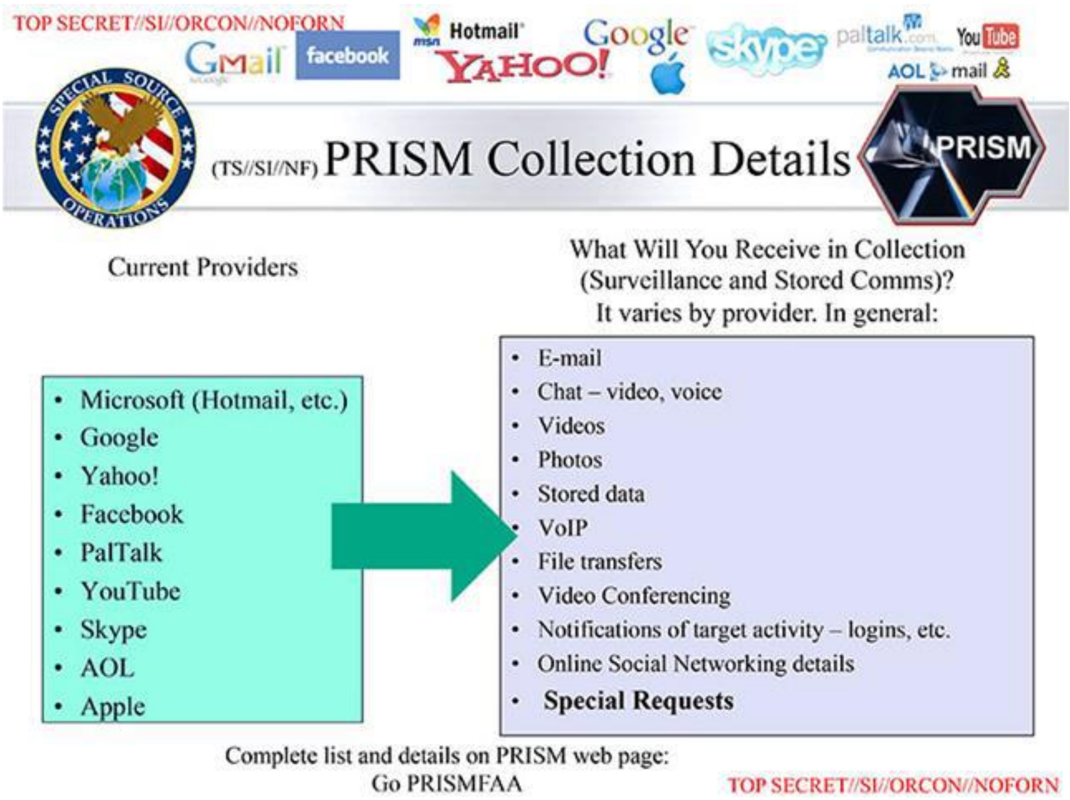


The Internet & AI: the promise

- overcome the information overload
- world-wide generation and distribution of knowledge and solutions
- economic efficiency, wealth creation
- cost-effective, individualised private and public services
- environmental-friendly management of utilities, traffic, logistics
- support for transparency, overcome bias and discrimination
- Etc.

The Internet + AI infrastructure: The catch

- Data collection/analysis/surveillance
- We cannot get out of the infrastructure
- We cannot effectively resist/contest influence and manipulation



Ethics and law violations by AI + Big Data

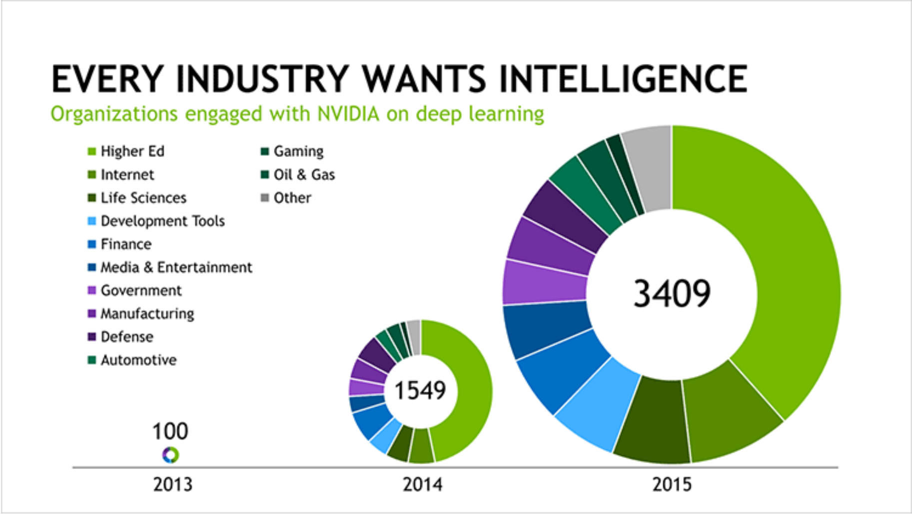
By 2018, 50% of violations of business ethics will be performed by algorithms

Gartner 2016

What drivers for AI

AI is in principle innocent, it only pursue the goals it is assigned

- By profit-making actors
  - Efficiency, cost reduction, better services
  - Anticipate/control/direct behaviour (to sell goods and services)
  - Two sided markets: capture user, to send them advertising, suggestions, and services, get revenue from advertisers-persuaders
- By governmental actors
  - Efficiency, costs reduction, better services
  - Anticipate/control/direct behaviour (for security and other purposes)



But impacts on individual and society are not always good!


BBC Sign in News Sport Weather iPlayer TV

NEWS

Home UK World Business Politics Tech Science Health Family & Education

Technology

Google searches expose racial bias, says study of names

4 February 2013 Technology

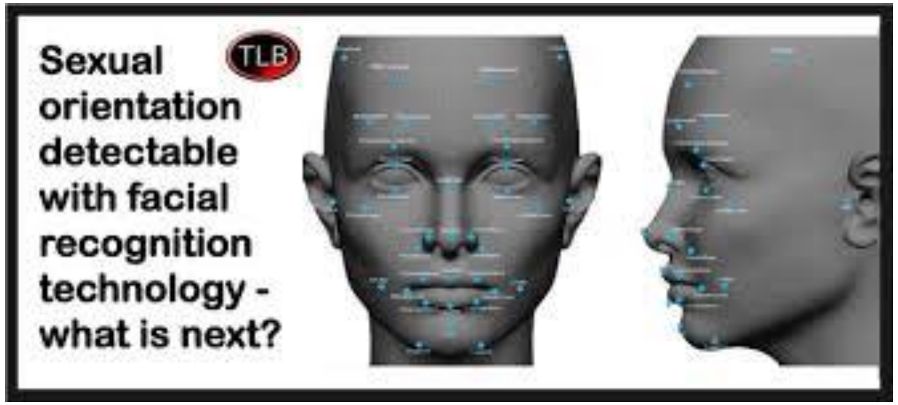
Share

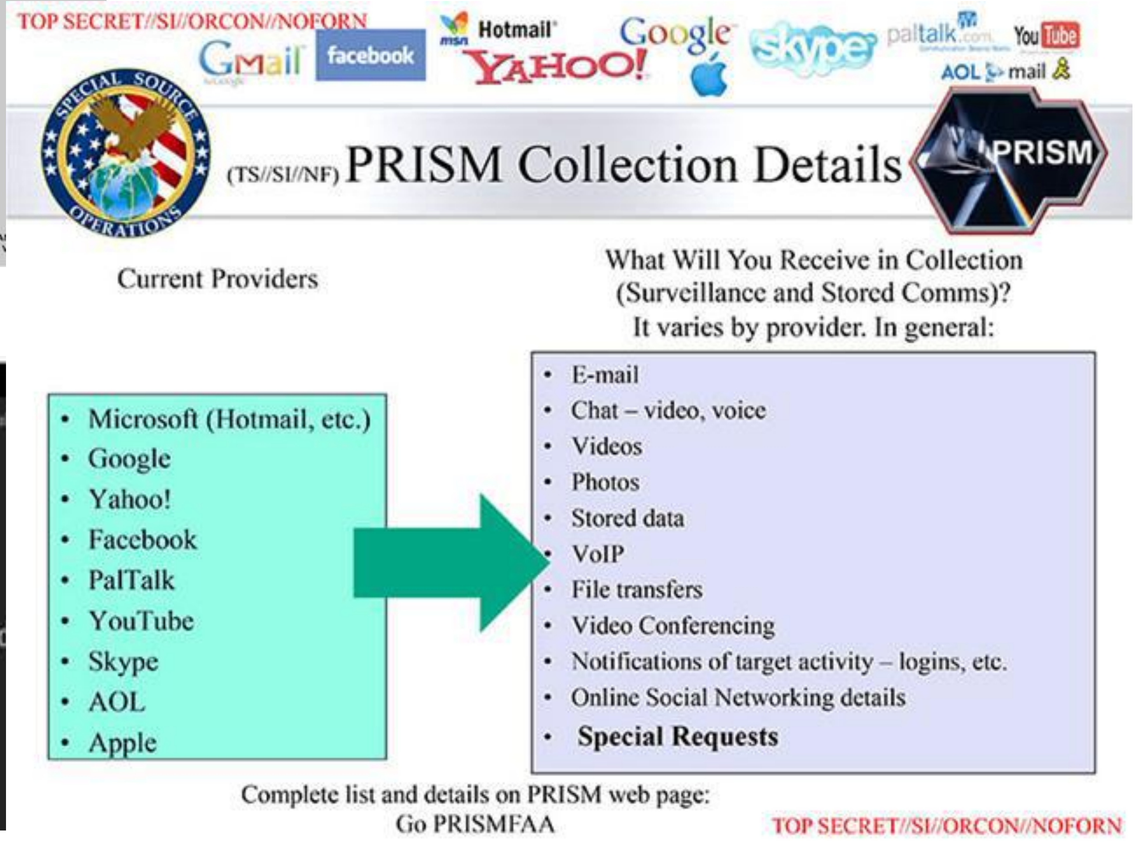
A study of Google searches has found "significant discrimination" in advert results depending on the perceived race of names searched for.

Harvard professor Latanya Sweeney said names typically associated with black people were more likely to produce ads related to criminal activity.

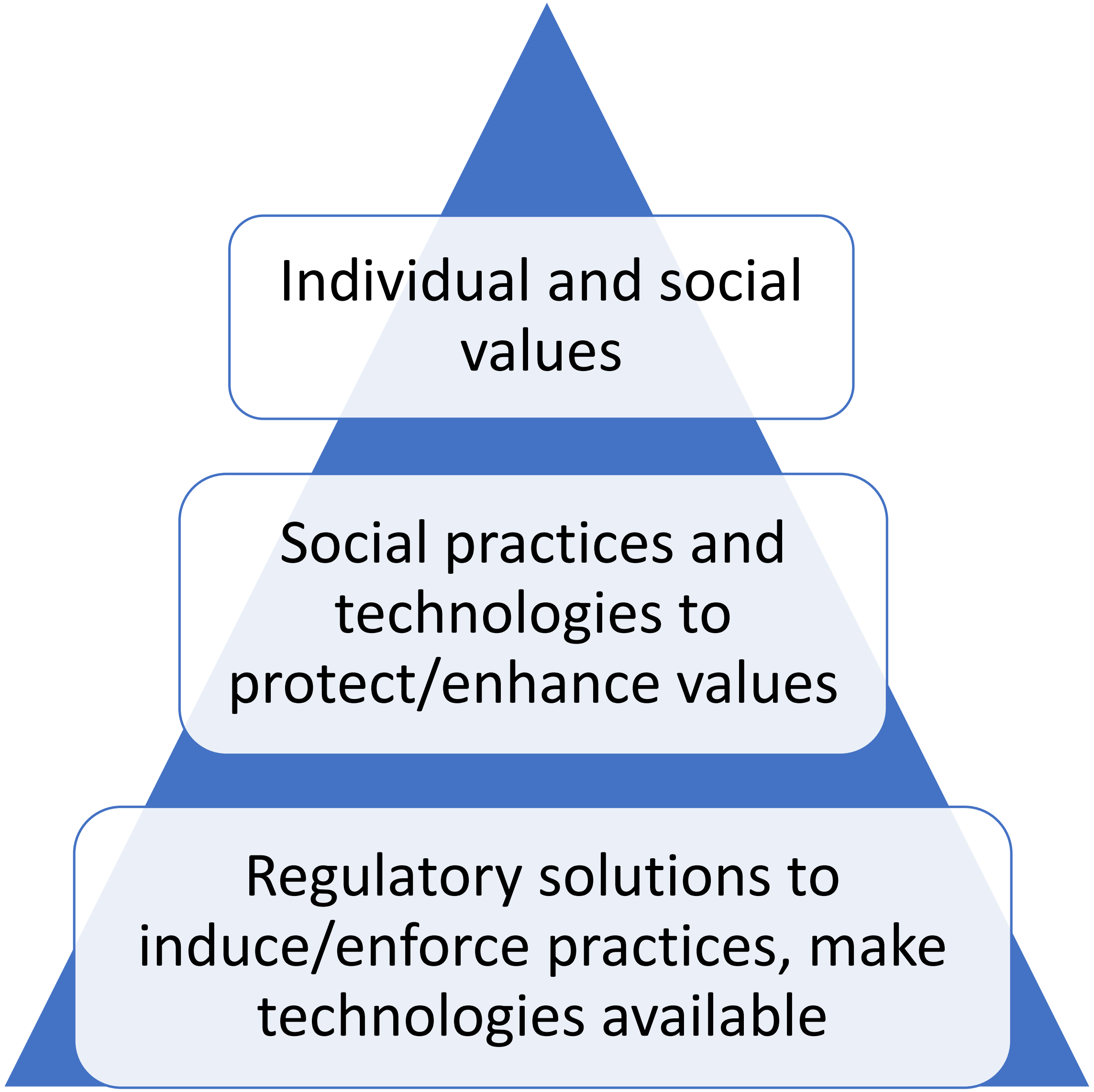
GETTY IMAGES

Prof Sweeney said technology could be used to counteract racial intolerance





A value-based approach to regulating AI



A disrupting flow of innovations, generates multiple and diverse legal/social issues

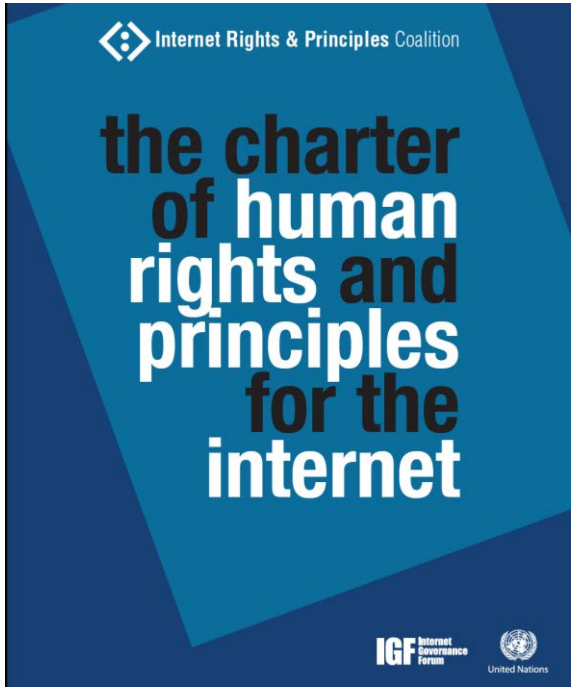
How to proceed:

- Start from first principles
- Promote valuable socio-technical practices through tailored regulations and technologies
- Adapt existing legal frameworks, multi-layered regulation

What answers?

- Regulation
  - Smart regulation to direct the use of AI by private and public organisations
    - https://artsy.eui.eu/
- Empowerment
  - Make the power of AI available to citizen and civil society
    - https://claudette.eui.eu/

The legal-ethical framework: rights and social values



- Human/fundamental rights:
  - privacy, data protection, dignity, autonomy, freedom of expression, non-discrimination, equality, participation
- Social/economic goals:
  - welfare, competition, efficiency, science, art and culture, cooperation, civic dialogue, democracy

The legal framework: Multiple sectorial legal regimes and principles

- Data protection law
  - Principles: lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; integrity and confidentiality; accountability; legitimate interest, data subject rights, etc.
- Consumer protection law
  - Principles: Protection of the weaker party, Regulated autonomy, Non-discrimination, etc.
- Competition law
  - Principles: fair competition, consumer welfare, etc.

Synergy and tensions: EDPS (Opinion 8/18)

- **Consumer** and **data protection law** share common goals of **redressing imbalances of informational and market power**
- Together with **competition law**, data protection and consumer protection need to work to ensure that people are **treated fairly**.

An issue: are personal data a tradable property?

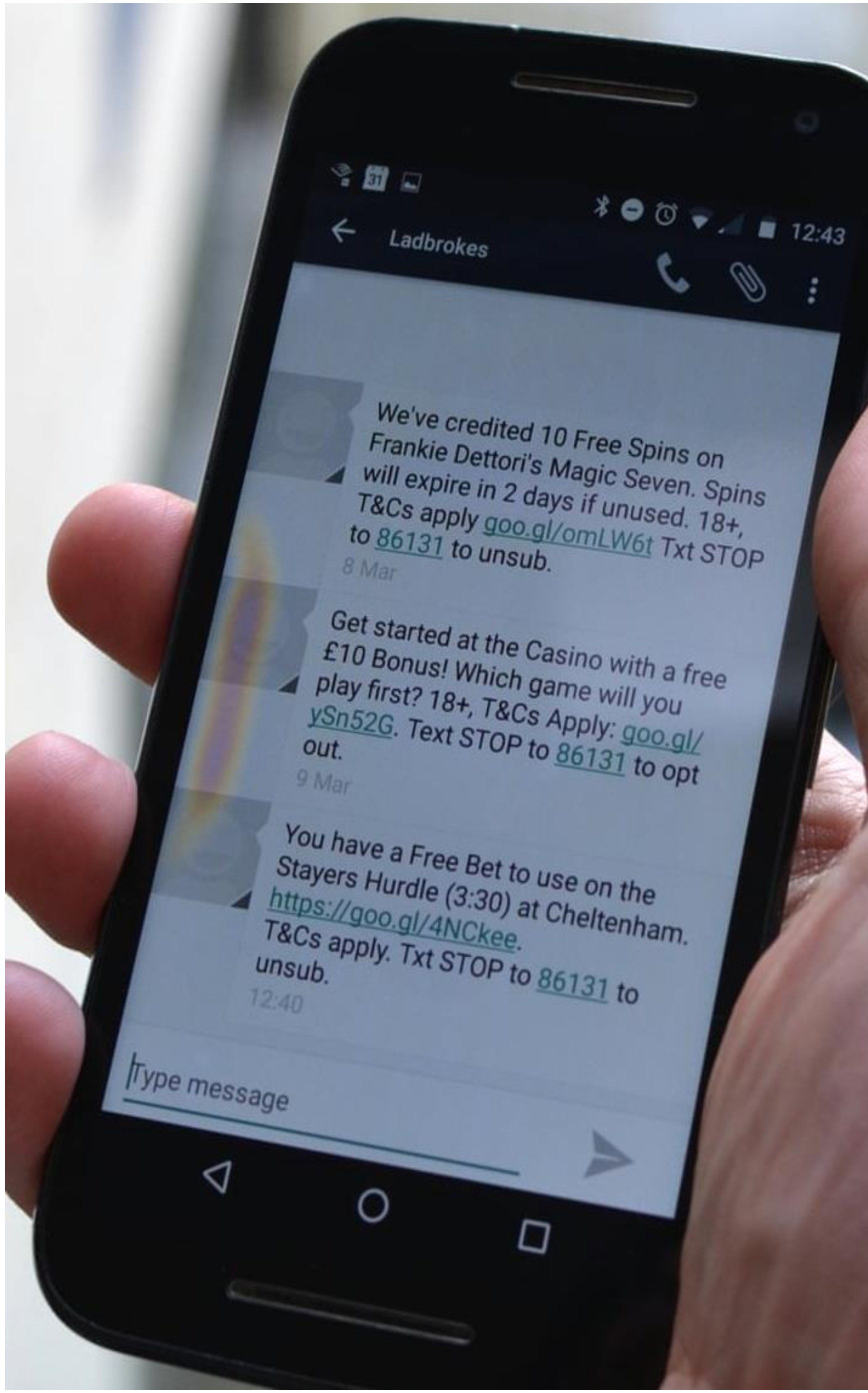
- Can a consumer pay with his or her data? What about revocable consent under GDPR? What about privacy as a fundamental right?

What interests/rights are at stake

- Privacy-data protection
  - to lawful and proportionate processing of personal data, to control processing
- Fair algorithmic treatment
  - not to be subject to unfair differentiated treatment
- Algorithmic transparency
  - to know why a certain algorithmic response or decision ha been given
- Interest in fair algorithmic interaction
  - not to be misled or manipulated
- Interest in fair algorithmic (cognitive) competition
  - Interest in accessing data sources and algorithms that are available to big players

Focus on risks for consumers

- Unfair algorithmic decisions
- Unfair, excessive data processing/profiling
- Limitations on consumers' autonomy
- Discriminatory/unfair/ aggressive/exploitative advertising
- Filter bubbles/echo chambers
- Information asymmetry; arbitrary power
- Exploitation of vulnerabilities
- Opacity, inability to contest
- Risk of erroneous diagnoses, suggestions



Issue: Price discrimination

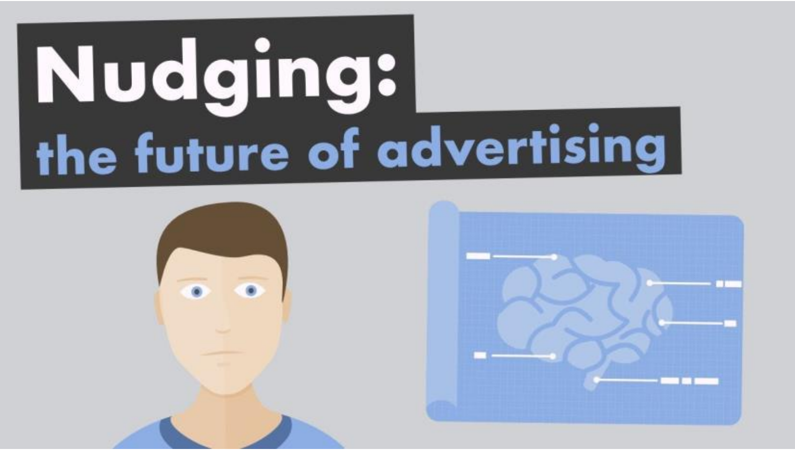
- AI enables sellers to figure out the highest price a client can pay
- Should there be price discrimination in consumer retail markets? For what good/service, on what grounds'?
  - cost structures, risks
  - spending capacity, needs, interests, vulnerabilities
- Normative standards:
  - Consumer protection law: is it unfair/discriminatory?
  - GDPR: is it an automated decision, is there a legitimate interest?
  - Competition law: does this affect competition?

Issue: Discrimination in algorithmic offers

- What if different people are offered different opportunities
  - Men getting better loans, women better insurance
  - People of certain ethnicity being more often refused opportunities
- What if the AI system has “innocently” learned to apply differential treatment
  - based on previous practice
  - to achieve a business purpose
- What legal solution
  - Data protection law: legitimate purpose, sensitive data, consent?
  - Consumer protection law/discrimination law: unacceptable discrimination?

Issue. Targeted advertising/malicious nudging

- AI can deliver each consumer the ads that most trigger purchasing, depending on:
    - how well they match consumer's needs and interest
    - how well they exploit consumer's vulnerabilities (e.g., predatory loans to people in difficulties, gambling offers to gambling addicts, drugs to depressed people)
- What legal solution?
  - When is it permissible? When a prevailing "legitimate interest"?
  - When does it "materially distort the economic behaviour of consumers"



Issue: Aggressive personalised advertising

- What if personalized advertising, to maximize clicks and revenues, exploit individual vulnerabilities (economic hardship, propensity to gambling, etc.)
  - This may be non-intentional, as the system may aim to use any factors correlated to clicks and purchases, regardless of the impact on consumer's interests
- Data protection law: Is exploiting vulnerabilities acceptable?
- Consumer protection law: does it count as "aggressive advertising"

Issue: Discrimination in Ad delivery

- Systems meant to address Ads and offers to those who are most probably interested in them may reproduce biases and discrimination
  - Offers for top jobs to male people
  - Offers for houses to those who match current ethnic ownership
- Maybe no data protection issue, But is there a discrimination issue?


theguardian

ort football opinion culture business lifestyle fashion environment tech

Women less likely to be shown ads for high-paid jobs on Google, study shows

Automated testing and analysis of company's advertising system reveals male job seekers are shown far more adverts for high-paying executive jobs

Issue: “Turn off” personalization?

- Personalised treatment of consumer can provide the with advantages, but also disadvantages
- Should the consumers know that they profiled, for what specific purposes?
- Should consumers be offered the option to trade and purchase anonymously?

- The GDPR allows consumer to withdraw consent and object to profiling. Is there a right to trade anonymously?

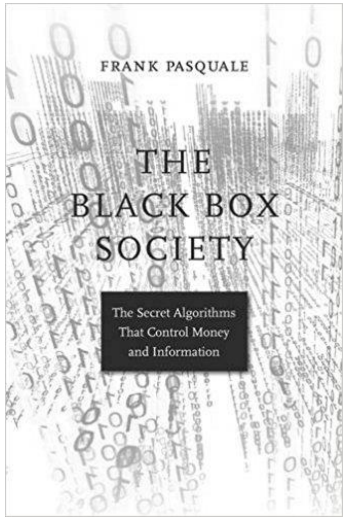
Issue. Rights to information/transparency

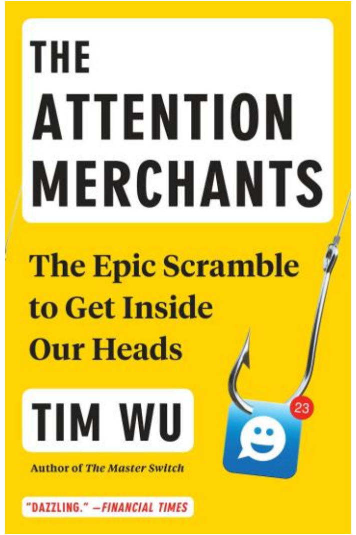
- Have (should have) consumers a right to know that they are offered personalised prices? Calculated in what way?
- Have (should have) consumers a right to know to know that their treatment is dependant on the tracking of their behaviour, and on consequent classifications/profiling? With what impacts?

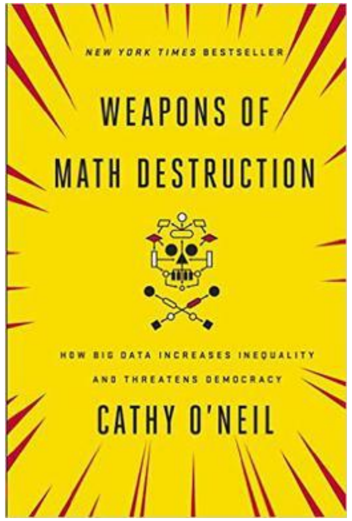
- Data protection law: information obligations on data controllers
- Consumer protection law: information obligations on suppliers
- What about platforms?

Other issues to be addressed

- Right to procedural regularity
- Right to substantive legality
- Right to explanation/justification
- Right to have a human answer
- Right to be protected from abusive manipulation
- Liabilities for mistaken decisions/advice







Empowering civil society?

- Remedy the imbalance for AI-powered platforms and suppliers through citizen and consumer-empowering AI
  - Protection against unwanted monitoring
  - Support in detecting unfair/unlawful use of AI
  - Control over fairness of commercial practices

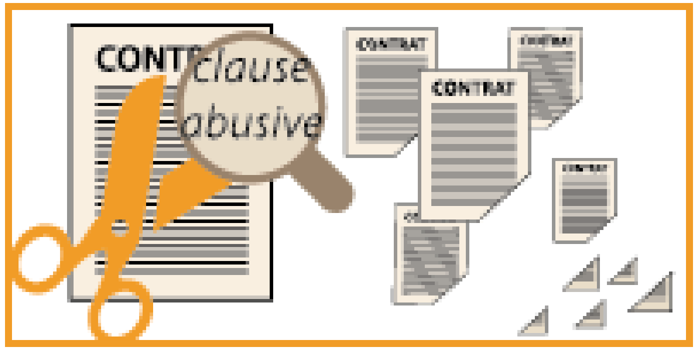
- Some examples:
  - Spam filters
  - Ad-blocking tools
  - Anti-tracking tools
  - Price comparison platforms
  - Detection of, and response to, violations of law and ethics
- Should consumer-empowering initiatives be supported and incentivised?

Detect, and respond to, violations of law and ethics

- AI can contribute to address online violations:
  - Unlawful and unethical behaviour on line is often unnoticed, rarely acted upon.
  - AI can facilitate cost-effective prevention/detection/reaction
- The AI-empowerment should be available to those who most need it:
  - Commercial actors, and resourceful individuals already use AI to apply the law
  - This opportunity should be open to citizens and civil society!

What about privacy policies and terms of service?

- Most online terms of service and privacy policies contain unlawful/unfair clauses, or miss relevant information:
  - Consumers agree but don’t read
  - NGOs (consumer organisations) lack resources



- AI can contribute:
  - AI support to citizens and civil society to detect and react
  - An example: An automatic detector of unfair clauses in online contracts and privacy policies: https://claudette.eui.eu/

CLAUDETTE GDPR

— Automatically Monitoring Privacy Policies —

Forgetting in the context of AI?

- What does it mean to forget in the context of AI
- There are two texts (Zuboff 2019): “The specific mechanisms of surveillance capitalism compel the production of two “electronic texts,”
  - When it comes to the public-facing text, we are its authors and readers.
  - The first text, full of promise, actually functions as the supply operation for the second text: the *shadow text*.
- Where does forgetting matter more?
  - How can we be forgotten relatively to the second text?

Thanks for your attention

Giovanni Sartor, European University Institute / University of Bologna

ETHICAL PRINCIPLES FOR ARTIFICIAL INTELLIGENCE IN LIGHT OF THE IoT/IoE

Prof.dr. Anton Vedder
Centre for IT and IP Law
KU Leuven

Intro

- AI: Preliminaries
- The “Fundamental Rights approach” (FRA) to AI
- The Pros and Cons in the current debate
- Some more Pros and Cons
  - FRA vis-a-vis under-articulated problems
  - FRA vis-a-vis impact on basic concepts and presuppositions

  Examples:
  - Machine Learning in a Big Data Context (MLBD)
  - Human enhancement through merges of AI and IoE

KU LEUVEN

Preliminary: AI def

- Intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and animals
- In particular, intelligence shown by machines, in the capacities to observe and analyse surroundings and to perform acts successfully instrumental to purposes

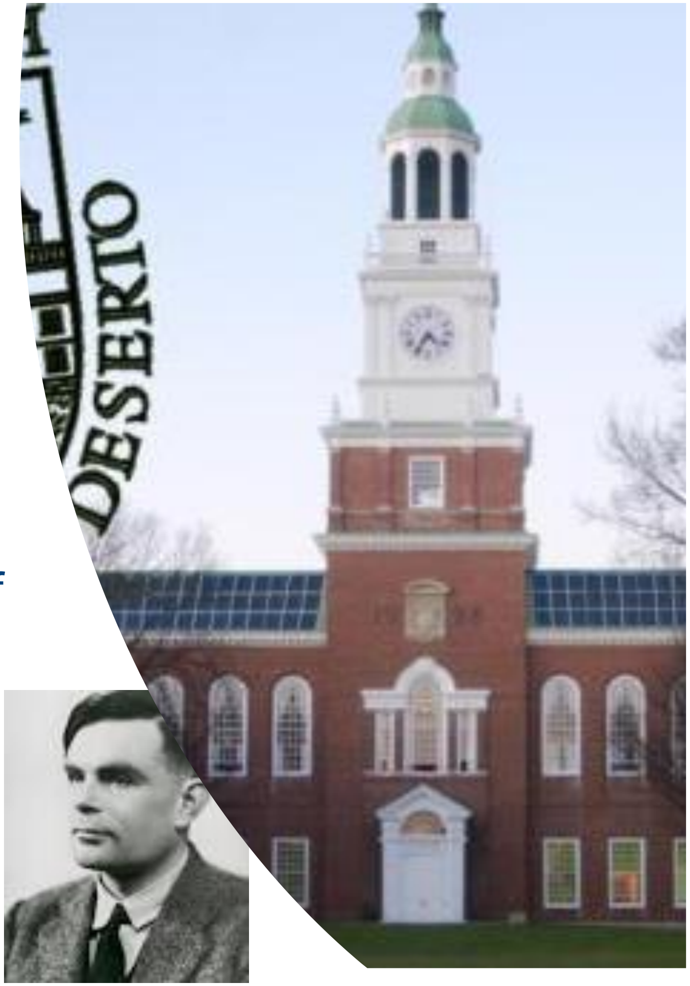
Preliminary: “AI” effect

“AI effect”: As soon as a computer application once referred to as AI becomes mainstream, it will soon no longer be referred to as AI

Currently: AI effect reversed? Awful lot goes under the label of AI: software, cars, drones, robots for whatever purpose

For Ethics and Law maybe more appropriate to specify, at least to the degree that different types of AI applications at least in part may raise different ethical issues (eg: weaponed robots – telemedical instruments – MLBD supported decision making in marketing)

Here: focus on Machine Learning in a Big Data context (MLBD)



High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (8 April 2019)

- Trustworthy AI: complying with applicable laws and regulations, in accordance with ethical principles and values, technically robust
- Ehical imperatives *based on fundamental rights enshrined in the EU Treaties, Charter and international human rights law*: Respect for human autonomy, prevention of harm, fairness, explicability
- Seven key requirements to be evaluated throughout the AI system's life cycle
  - Human agency and oversight
  - Technical robustness and safety
  - Privacy and data governance
  - Transparency
  - Diversity, non-discrimination and fairness
  - Environmental and societal well-being
  - Accountability
- Trustworthy AI Assessment: Impact for 7 Reqs + Fundamental Rights + accessibility, explainability and other values and principles

"Fundamental Rights Approach"

Status of the Ethics Guidelines – “Soft Regulation”

- Not binding
- Addressed to all possible stakeholders
- Wrt Trustworthy AI Assessment primarily the producers of AI seem to be addressed

- [Ms Von der Leyen, next president EC: legislative proposals!]

Actual opinions about the Ethics Guidelines as regulatory instrument

- Cons:
  - Vagueness: difficult to implement
  - Nonbinding
  - No (external) oversight
  - “Butchers inspecting and certifying their own meat”?
- Pros
  - Typically European: values first
  - To a degree, vagueness leaves room for openness to new developments

Second thoughts

- FRA suggests consistent, coherent approach. However: no clear internal logic: broad variety of “values”, e.g. FR Impact assessment, “explainability”, accessibility, robustness etc suddenly introduced – contentwise relationship with FR not clarified etc.
- Nonetheless:
  - Emphasis on procedural – non-substantial – principles, e.g. transparency, accountability, explainability, but fortunately combined with substantial principles (no matter how unclear the connections)
    - Example: MLBD and some of its consequences
  - AI will confront us with developments and new opportunities that affect the presupposed ontological basis and the key concepts of law and morality themselves. Will the key concepts of the “traditional” human rights and other normative starting points of the Guidelines be able to make sense of the developments that will transform themselves and their basis in reality?
    - Example: Human enhancement through merges of AI and IoT/IoE

Example 1: MLBD – good to have a mix of relatively open procedural and substantial principles

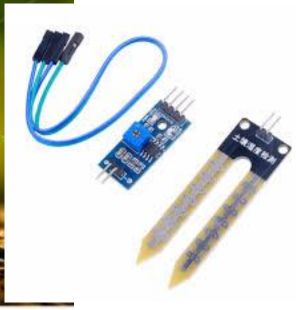
- Possible adverse impact of MLBD generally approached with combination of tranparency principle, P/DP, and recently fairness/non-discrimination
- What about under-articulated problems?

MLBD: Possible problems not necessarily involving data about humans1

Problems concerning access to information:

- Access to the technologies of MLBD incl its opportunities

- Relocation of info and expertise: power shifts, economic impact



MLBD: Possible problems involving data about humans (not necessarily qualifying as personal data)

Problems arising from group profiling:

- Distributive profiles (group characteristic shown by each group member, remaining with the individual also after leaving the group) and non-distributive profiles (group characteristic only shown by individual as member of the group)
  - possible adverse treatment and judgement based on traditional grounds for discrimination (e.g. when input data already biased);
  - possible adverse judgement and treatment based on non-distributive group characteristics that do *not* coincide with those traditional grounds for discrimination > NEW DISCRIMINATION GROUNDS
  - the confrontation with unwanted negative information about yourself.

KU LEUVEN

MLBD: Procedural principles, P/DP and traditional notions of fairness cannot be THE remedies to all problems

- Basic impediment for attempts to cope with MLBD complexity / opacity of technical basics and (business) secrecy. Simply requiring transparency probably will not help.
- More importantly: Transparency as a response only makes sense when

  (1) there are clearly designated addressees (a specific forum to which the system opens up) and

  (2) these addressees are provided with adequate rights to do something about possible problems.
- Not all input, nor all output data, causing problems, are about humans in general, or if about humans, not about individual persons

KU LEUVEN

Transparency may work as part of the regulatory framework for P/DP

- As that same framework is clear about the addressees (the legislator and the data subjects) and it provides the addressees of the transparency – i.e. primarily the data subjects – with rights and powers to (to a degree) effectively protect themselves.
- To the degree that MLBD's impact on human beings coincides with Data Protection problems, because personal data are involved, transparency is utterly important, although even here of course transparency of and in itself is not enough.

Transparency, P/DP, Fairness will not work wrt the many problems where

- There are no clearly designated addressees (such as data subjects)
  - E.g. In group profiles often no traditional individual data subjects, due to aggregate level + non-distributiveness of profile: Unclear which individuals affected
- It is not clear what parties should have which powers and rights
  - Due to the previously mentioned aspect +
  - In case of group profiles, individual discretionary powers might have consequences for the group
- (Most dramatically) where these are still in need of articulation, e.g. creation of new discriminatory grounds

The regulatory regime needed

- Facilitates deliberations about the possible impacts on humans of whatever MLBD applications in order to explore and identify the exact nature and significance of the possible problems.
- Will not obstruct from the outset all of the advantages that MLBD has to offer.
- Could stipulate mechanisms of for instance processing records, impact assessments, etc.
- Involves representatives from various possible stakeholders, but also ethicists, lawyers and policy makers in order to effectively identify possible infringements of rights, legitimate interests and values affected
- FRA is a step in the right direction where as yet inarticulate adverse impact is concerned
- This is not a plea for non-interference by the legislator and policy makers

Human enhancement: networked humans

- AI merged with IoT and IoE, e.g. with help of wearables and implants: networked humans for
  - Extended memory, brain functions
  - Online realtime coaching
  - Emotion management
  - Regulation by technology

- Individuality, autonomy endangered, or just changed? (Compare: education, psychopharmaca)
- What if the new “connected human” is morally, physically, emotionally and intellectually better than the good old autonomous individual? What if they agree to being enhanced in this way?

Conclusion: FRA

- Pro:
  - Typically European: values first
  - Vagueness leaves room for openness to assess and regulate new developments to a degree
  - Involvement of all stakeholders and non-bindingness may stimulate thorough debate and careful articulation of problems and relevant norms.
- Contra
  - Vagueness: difficult to implement
  - Nonbinding
  - No (external) oversight
  - “Butchers inspecting and certifying their own meat”?
  - Messy contentwise structure of guidelines
  - On a fundamental normative level not open to assess and regulate future technical developments

Sources

- Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*. European Commission, April 2019
- Vedder, Anton & Laurens Naudts, Accountability for the Use of Algorithms in a Big Data Environment. *International Review of Law, Computers & Technology* 2017; 31; 2: 206-224
- Vedder, Anton, An Obligation to Enhance? *Topoi* 2019; 38 (1) pp. 49-52
- Lucivero, Federica & Anton Vedder, *Beyond Therapy v. Enhancement: Multidisciplinary Analyses of a Heated Debate*. Pisa: Pisa University Press, 2013
- Vedder, Anton, KDD: The Challenge to individualism. *Ethics and Information Technology* 1999; 1: 4: 275-281

For comments upon reflection:

Anton.vedder@kuleuven.be

KU LEUVEN

From Big Data to Big Knowledge:

Large-Scale Information Extraction based on Statistical Methods

Martin Theobald

University of Luxembourg

Faculty of Science, Technology & Communication

Wikipedia

Angela Merkel

From Wikipedia, the free encyclopedia

"Merkel" redirects here. For other uses, see Merkel (disambiguation).

Categories

Categories: 1954 births | Angela Merkel | Chancellors of Germany | Christian Democratic Union (Germany) politicians | Environment ministers of Germany | Female heads of government | German Lutherans | German people of Polish descent | German physical chemists | German politicians | German women in politics | Grand Crosses of the Order of Merit of the Federal Republic of Germany | Jawaharlal Nehru Award laureates | Leaders of political parties in Germany | Leipzig University alumni | Living people | Members of the Bundestag | Ministers for children, young people and families | People from Hamburg | Presidential Medal of Freedom recipients | Presidents of the European Council | Recipients of the Order of the Sun of Peru | Women chemists | Women's ministers | Recipients of the Presidential Medal of Distinction of Israel

problems concerning future energy development have been major issues during her Chancellorship.

Assumed office
10 April 2000

Infoboxes

Personal details	
Born	Angela Dorothea Kasner 17 July 1954 (age 64) Hamburg, West Germany
cal party	Democratic Awakening (1989–1990) Christian Democratic Union (1990–present)
se(s)	Ulrich Merkel (m. 1977; div. 1982) Joachim Sauer (m. 1998)
mater	Leipzig University German Academy of Sciences at Berlin (Ph.D.)[1]
ature	

Information Extraction

Angela Merkel

From Wikipedia, the free encyclopedia

"Merkel" redirects here. For other uses, see Merkel (disambiguation).

Angela Dorothea Merkel[a] (née **Kasner**; born 17 July 1954) is a German politician and former research scientist who has been the Chancellor of Germany since 2005 and the Leader of the Christian Democratic Union (CDU) since 2000. She is the first woman to hold either office.[7]

Having earned a doctorate as a physical chemist, Merkel entered politics in the wake of the Revolutions of 1989, briefly serving as a deputy spokesperson for the first democratically elected East German Government in 1990. Following German reunification in 1990, she was elected to the Bundestag for Stralsund-Nordvorpommern-Rügen in the state of Mecklenburg-Vorpommern, a seat she has held ever since. She was later appointed as the Minister for Women and Youth in 1991 under Chancellor Helmut Kohl, later becoming the Minister for the Environment in 1994. After Kohl was defeated in 1998, she was elected Secretary-General of the CDU before becoming the party's first female leader two years later in the aftermath of a donations scandal that toppled Wolfgang Schäuble.

Following the 2005 federal election, she was appointed Germany's first female Chancellor at the head of a grand coalition consisting of the CDU, its Bavarian sister party, the Christian Social Union (CSU), and the Social Democratic Party of Germany (SPD). In the 2009 federal election, the CDU obtained the largest share of the vote and Merkel was able to form a coalition government with the support of the Free Democratic Party (FDP).[8] At the 2013 federal election, Merkel won a landslide victory with 41.5% of the vote, falling just short of an overall majority, and formed a second grand coalition with the SPD, after the FDP lost all of its representation in the Bundestag.[9]

In 2007, Merkel was President of the European Council and chaired the G8, the second woman to do so. She played a central role in the negotiation of the Treaty of Lisbon and the Berlin Declaration. One of her priorities was also to strengthen transatlantic economic relations by signing the agreement for the Transatlantic Economic Council on 30 April 2007. Merkel was seen as having played a crucial role in managing the financial crisis at the European and international level, and has been referred to as "the decider."[10] In domestic policy, health care reform and problems concerning future energy development have been major issues during her Chancellorship.

Merkel has been described as the *de facto* leader of the European Union, and was ranked as the world's second most powerful person by *Forbes* magazine in 2012, the highest ranking ever achieved by a woman; she is currently ranked fifth.[11][12][13][14][15][16] On 26 March 2014, she became the longest-serving incumbent head of government in the European Union. Merkel is currently the Senior G7 leader. In May 2015, she was named the most powerful woman in the world for a record ninth

Angela Merkel

Merkel in February 2015

Chancellor of Germany

Incumbent

Assumed office
22 November 2005

President	Horst Köhler Christian Wulff Joachim Gauck
Deputy	Franz Müntefering Frank-Walter Steinmeier Guido Westerwelle Philipp Rösler Sigmar Gabriel
Preceded by	Gerhard Schröder

Leader of the Christian Democratic Union of Germany

Incumbent

Assumed office
10 April 2000

Preceded by	Wolfgang Schäuble

Minister for the Environment

In office
17 November 1994 – 26 October 1998

Chancellor	Helmut Kohl
Preceded by	Klaus Töpfer

DBpedia/YAGO et al.

```
bornOn(Angela,17-07-1954)
bornIn(Angela,Hamburg)
hasBirthName(Angela,Kasner)
marriedTo(Angela,Ulrich)
marriedTo(Angela,Joachim)
graduatedFrom(Angela,U_Leipzig)
instanceOf(Angela,Politician)
instanceOf(Angela,Chemist)
instanceOf(Angela,Chancelor)
```

>120 M facts for YAGO3
(from Wikipedia infoboxes/categories)

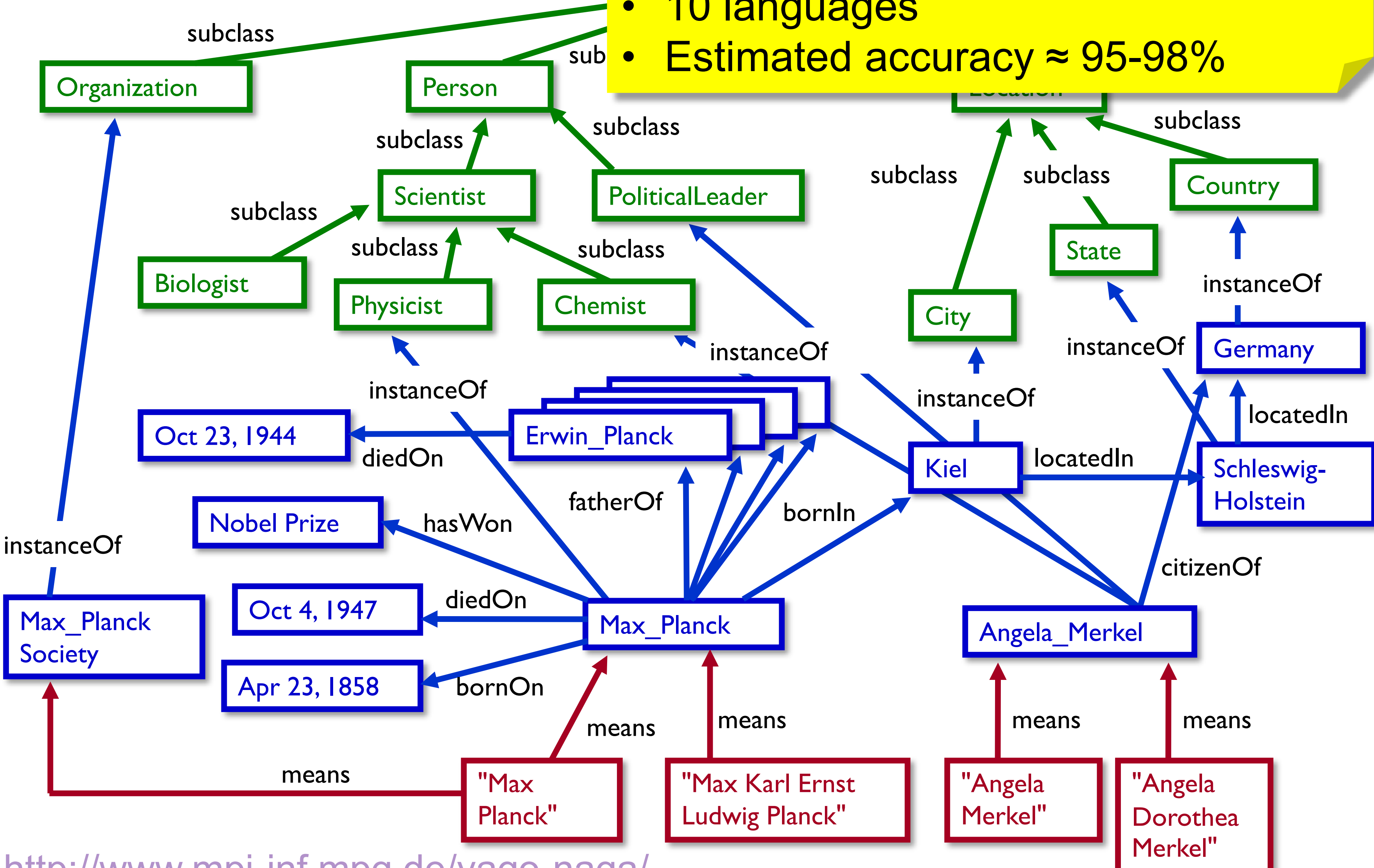
New fact candidates

```
leaderOf(Angela,CDU)[0.5]
hasPhDIn(Angela,Chemistry)[0.2]
elected(Angela,GDR_Government)[0.9]
elected(Angela,Bundestag)[0.8]
appointed(Angela,Minister)[0.2]
elected(Angela,SecrGeneral)[0.4]
appointed(Angela,Chancellor)[0.6]
president(Angela,EuroCouncil)[0.7]
chaired(Angela,G8)[0.9]
leader(Angela,EuroUnion)[0.2]
ranked(Angela,Forbes)[0.3]
```

100's M additional facts
from Wikipedia free-text!

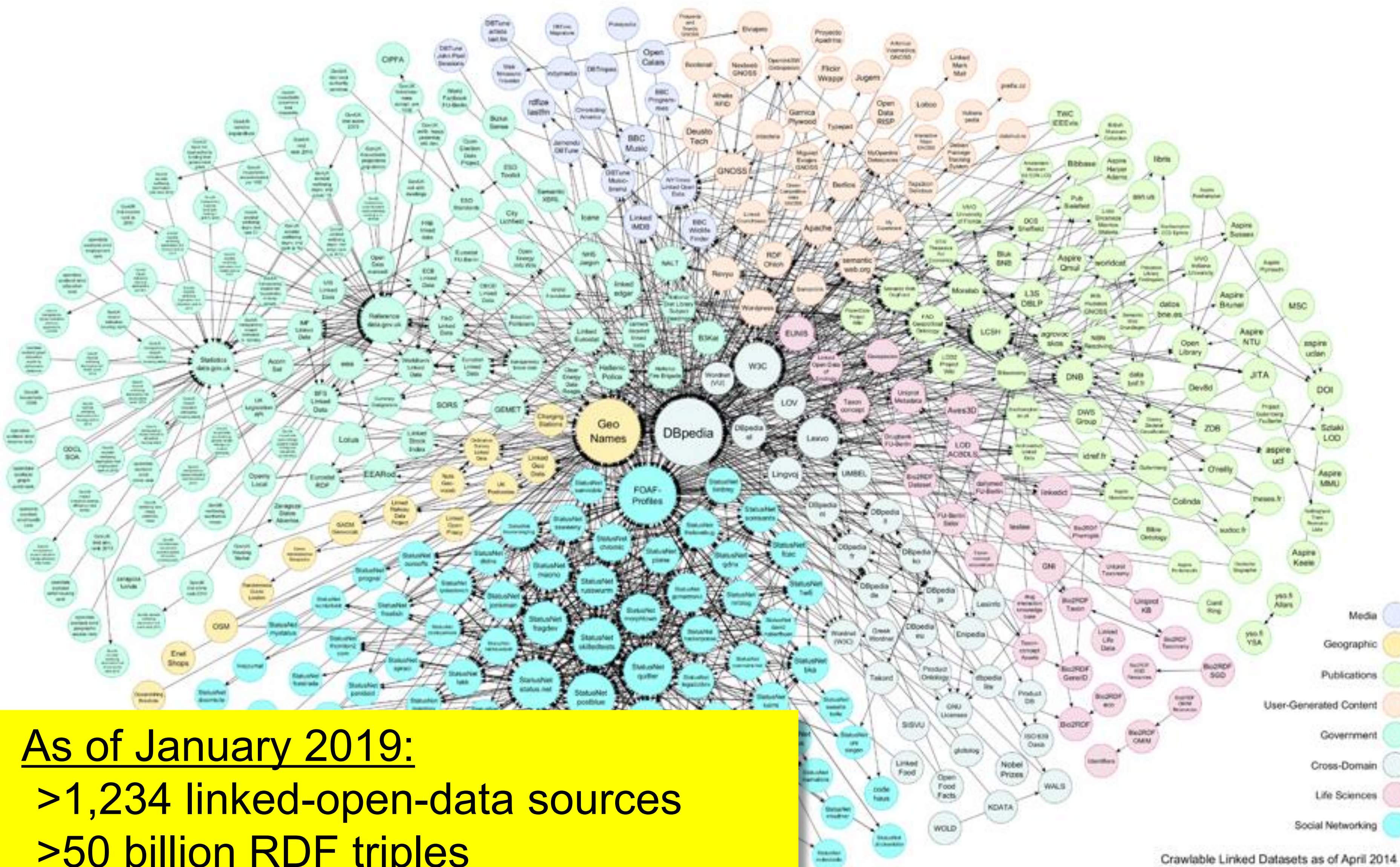
YAGO3 Knowledge

- 10 M entities, 120 M core facts
- 100 relations, 350 K classes
- 10 languages
- Estimated accuracy ≈ 95-98%



http://www.mpi-inf.mpg.de/yago-naga/

Linked-Open-Data Cloud



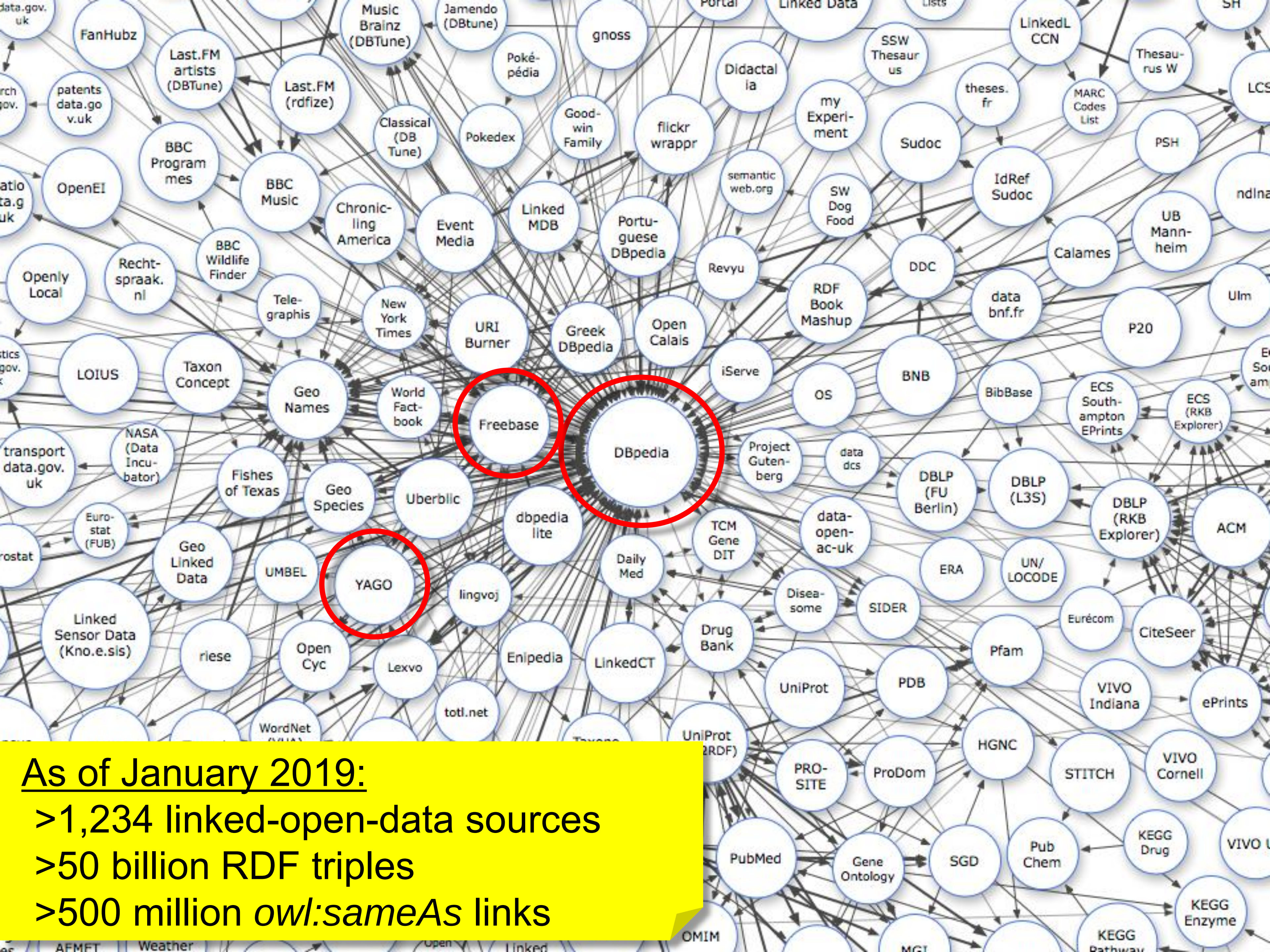
As of January 2019:

>1,234 linked-open-data sources

>50 billion RDF triples

>500 million *owl:sameAs* links

https://lod-cloud.net/



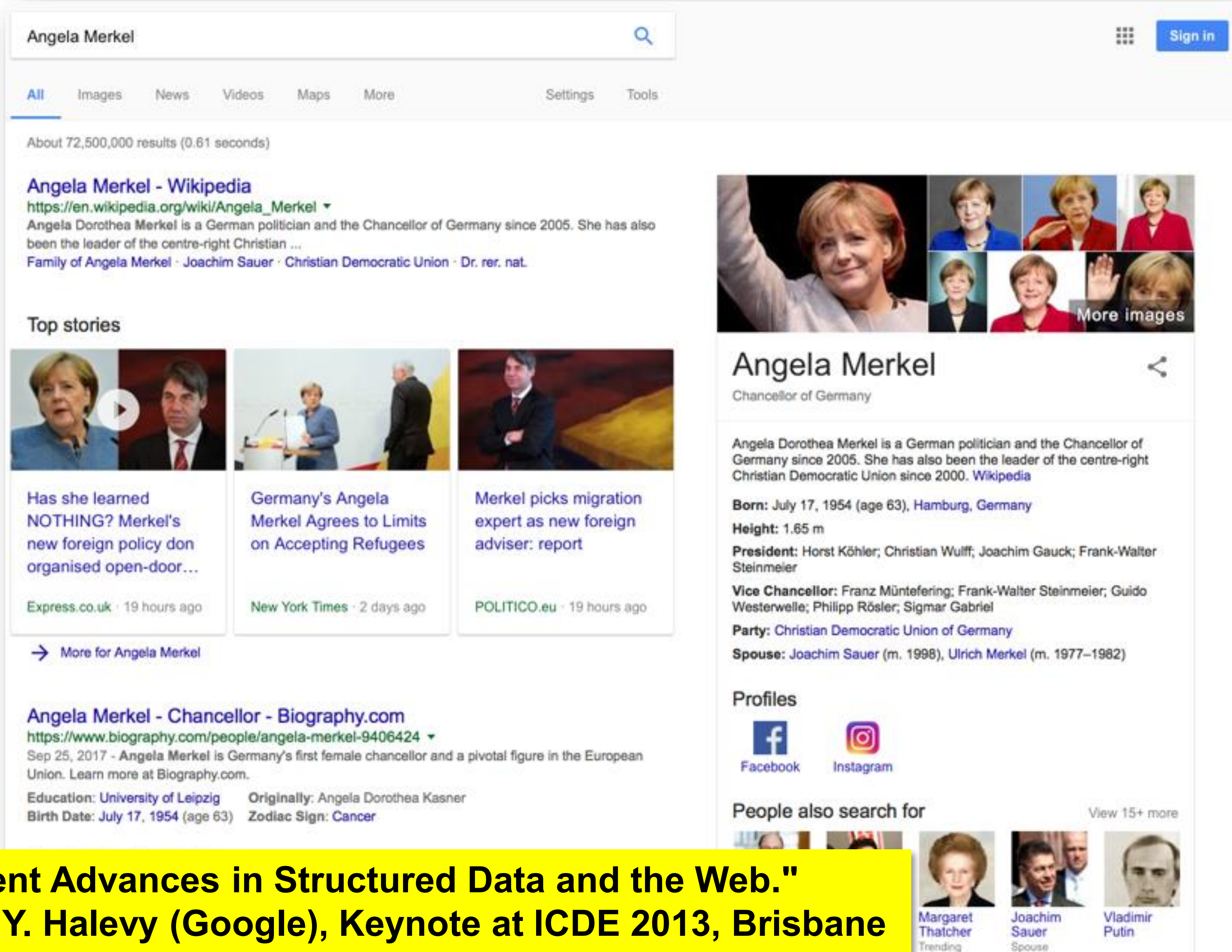
As of January 2019:

>1,234 linked-open-data sources

>50 billion RDF triples

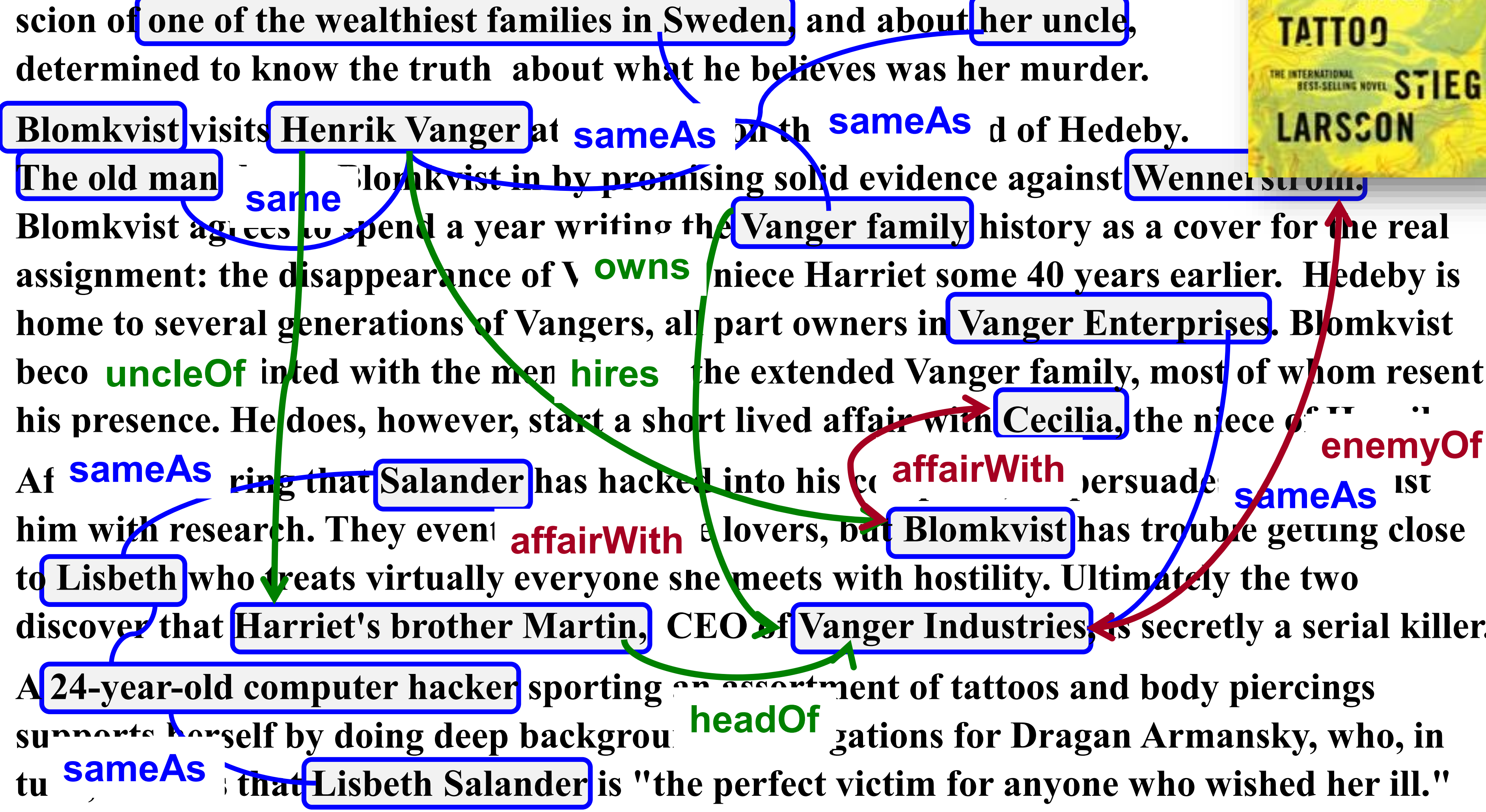
>500 million *owl:sameAs* links

Application I: Structured Search Results



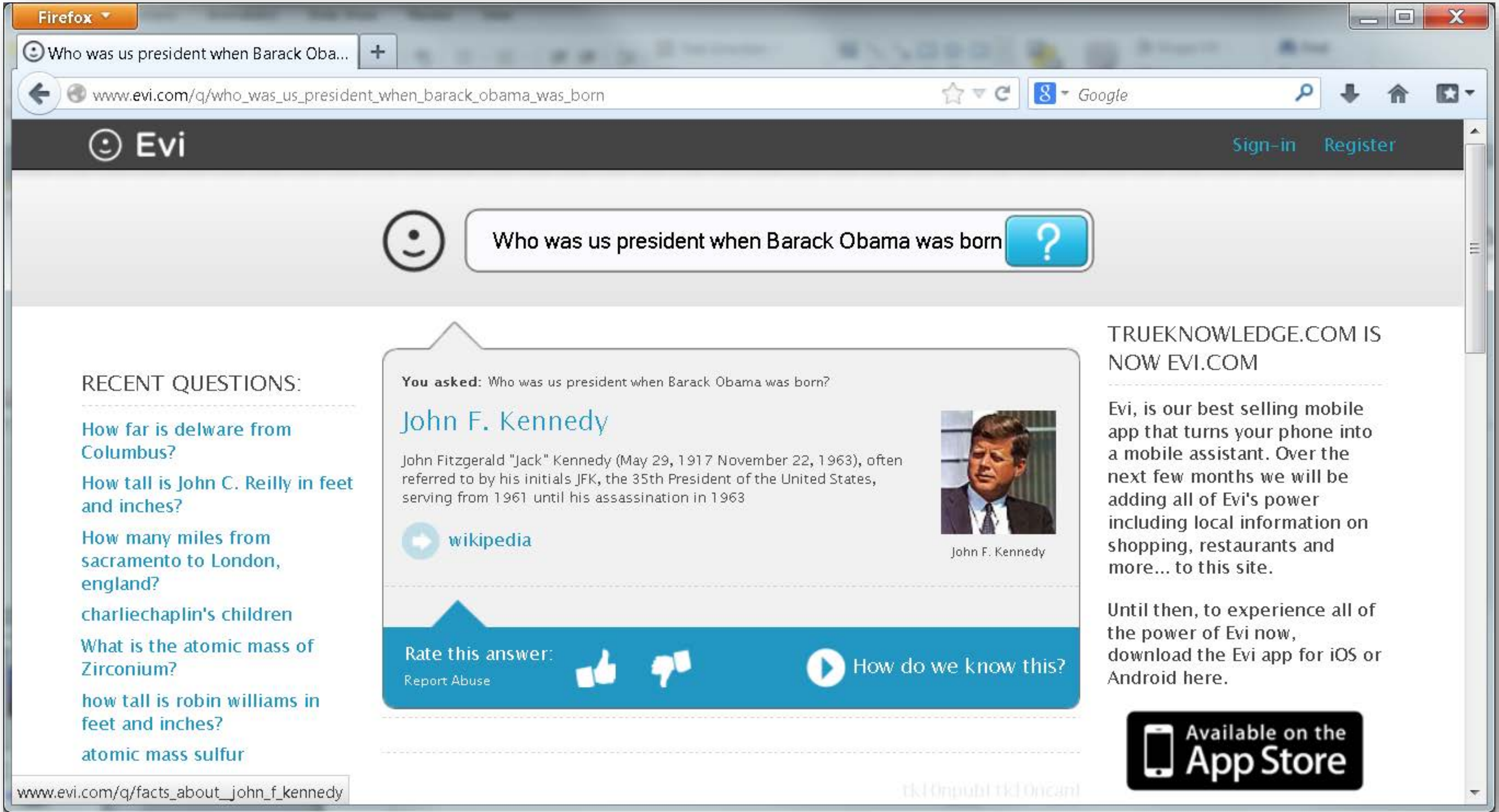
"Recent Advances in Structured Data and the Web."
Alon Y. Halevy (Google), Keynote at ICDE 2013, Brisbane

Application II: Machine Reading



Etzioni, Banko, Cafarella: Machine Reading. AAAI'06
Mitchell & Carlson: Toward an Architecture for Never-Ending Language Learning. AAAI'10

Application III:
Natural-Language Question Answering



evi.com (founded as trueknowledge.com in 2005, now Amazon Alexa)

IBM Watson: Deep Question Answering

- William Wilkinson's "An Account of the Principalities of Wallachia and Moldavia" inspired this author's most famous novel
- This town is known as "Sin City" & its downtown is "Glitter Gulch"
- As of 2010, this is the only former Yugoslav republic in the EU
- 99 cents got me a 4-pack of Ytterlig coasters from this Swedish chain
- U.S. City: largest airport is named for a World War II Hero; its second largest for a World War II Battle

WIKIPEDIA
The Free Encyclopedia

DBpedia

freebase™

Question classification & decomposition → **Knowledge back-ends**

yago
select knowledge

D. Ferrucci et al.: Building Watson: An Overview of the DeepQA Project. AI Magazine, 2010.

https://www.ibm.com/watson/

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

In other projects

Wikimedia Commons

Languages

University of Luxembourg

From Wikipedia, the free encyclopedia

Coordinates: 49.505031°N 5.948246°E

The **University of Luxembourg** (Luxembourgish: ***Universitéit vu Lëtzebuerg***; French: ***Université du Luxembourg***), is a public research university with a distinctly international, multilingual and interdisciplinary character, situated on Belval Campus and in Luxembourg City, Luxembourg.

Founded in 2003, the university has already built a reputation as being among the best young universities in the world. It was ranked 11th in the Times Higher Young University Rankings 2017, and 178th in the Times Higher World University Rankings 2016.

The University offers many bilingual and multilingual study programmes in French, English and German, as well as several master courses and doctoral schools entirely taught in English. With 6,200 students from 120 countries and 250 academics from all over the globe, the university provides a cosmopolitan learning experience. Moreover, all Bachelor's students have to spend a mandatory semester abroad, reflecting the importance attached to mobility. The University therefore cooperates with nearly 90 partner universities worldwide.

University of Luxembourg

UNIVERSITÉ DU LUXEMBOURG

Established	2003
Rector	Prof. Dr. Ludwig Neyses (Vice-President for Research, acting President)
Students	6,200 *(04. 2017)*
Location	Esch-sur-Alzette, Luxembourg
Colors	Red, white and light blue
Website	https://www.uni.lu/

Campus Limpertsberg

The University of Luxembourg has three faculties, including the **Faculty of Science, Technology and Communication**,[1] the **Faculty of Law, Economics and Finance**,[2] the **Faculty of Language and Literature, Humanities, Arts and Education**,[3] as well as three interdisciplinary research centres: the **Luxembourg Centre for Systems Biomedicine (LCSB)**[4], the **Interdisciplinary Centre for Security, Reliability and Trust (SnT)**[5] as well as the **Luxembourg Centre for Contemporary and Digital History (C^{2}DH)**.[6] Current research priorities are computational sciences and ICT, systems biomedicine, European law, international finance and educational sciences.

As one of the most international universities in Europe, the University of Luxembourg maintains close relations with EU institutions and participates in the debate on Europe's future. As a motor of the national research and innovation system, the University gives also strong support to entrepreneurial activities and is closely connected to Luxembourg's industry and the country's multicultural community, with an aim to support the creation of a knowledge-based society.

pha

nal
ne"
d in
atica

ns and
es
for
layouts
pecific
s

pha.com/

Outline

- Information Extraction

  [SIGMOD'09, WebDB'10, PODS'10, WSDM'11, CIKM'12, CLEF/INEX'11/'12, LDOW'14, TACL'16, CIKM'17, PVLDB'17]

- Probabilistic Databases

  [ICDE'08, VLDB-J'08, SSDBM'10, BTW'11, CIKM'11, ICDE'13, PVLDB'14, ICDE'18, StarAI'18, ICDE'19, SIGMOD'19]

- Distributed Indexing & Query Processing

  [SIGMOD'14, SWIM'14, SIGMOD'16]

Named-Entity Recognition & Disambiguation

"Merkel, Trump and May met at the G20 in Hamburg.
It was the first meeting between Trump and Putin."

- State-of-art approaches **recognize** named entities and then **disambiguate** these entities in two strictly separated phases.

Named-Entity Recognition & Disambiguation

"Merkel, Trump and May met at the G20 in Hamburg.
It was the first meeting between Trump and Putin."

- State-of-art approaches **recognize** named entities and then **disambiguate** these entities in two strictly separated phases.

Named-Entity Recognition & Disambiguation

"Merkel, Trump and May met at the G20 in Hamburg.
It was the first meeting between Trump and Putin."

?

- State-of-art approaches **recognize** named entities and then **disambiguate** these entities in two strictly separated phases.

Named-Entity Recognition & Disambiguation

“Merkel, Trump and May met at the G20 in Hamburg. It was the first meeting between Trump and Putin.”

?

- State-of-art approaches **recognize** named entities and then **disambiguate** these entities in two strictly separated phases.

Joint Named-Entity Recognition & Disambiguation

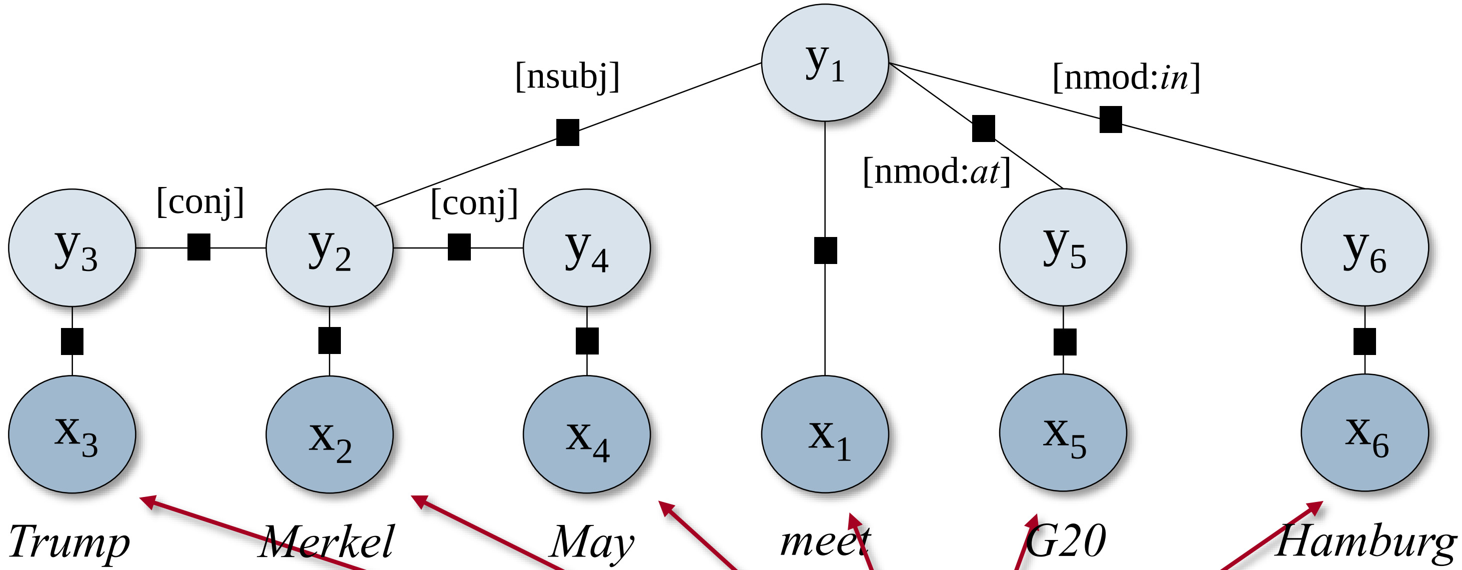
"Merkel, Trump and May met at the G20 in Hamburg.
It was the first meeting between Trump and Putin."

Images source: Wikipedia

- *J*-NERD *jointly* **recognizes** and **disambiguates** named entities with respect to a background knowledge base such as YAGO.

Conditional Random Field in *J*-NERD

[Nguyen et al.: LDOW'14,TACL'16,CIKM'17,PVLDB'17]

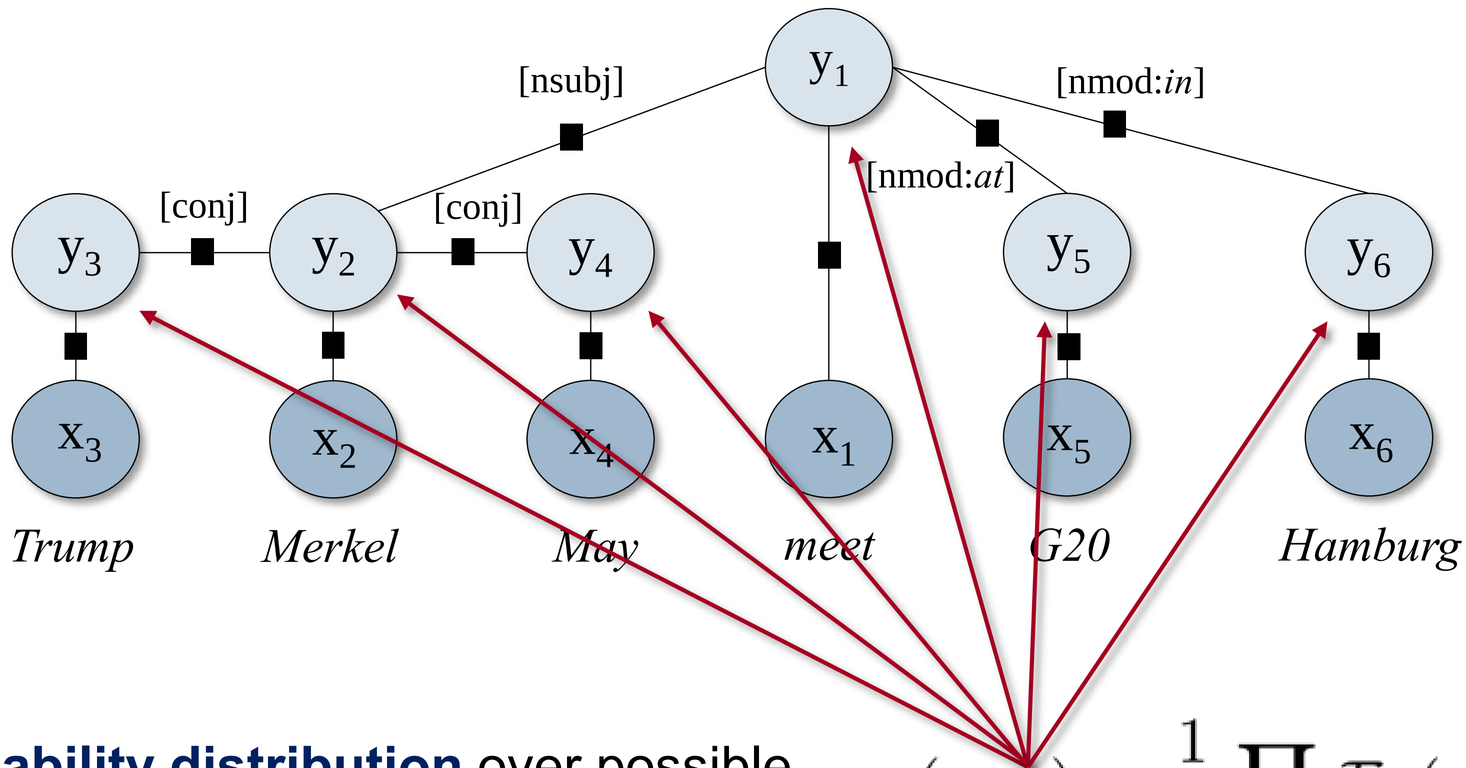


- **Probability distribution** over possible tokens *x* and combined NER/D labels *y*

$$p(\mathbf{x}, \mathbf{y}) = \frac{1}{Z} \prod_{A} \mathcal{F}_A(\mathbf{x}_A, \mathbf{y}_A)$$

Conditional Random Field in *J*-NERD

[Nguyen et al.: LDOW'14,TACL'16,CIKM'17,PVLDB'17]

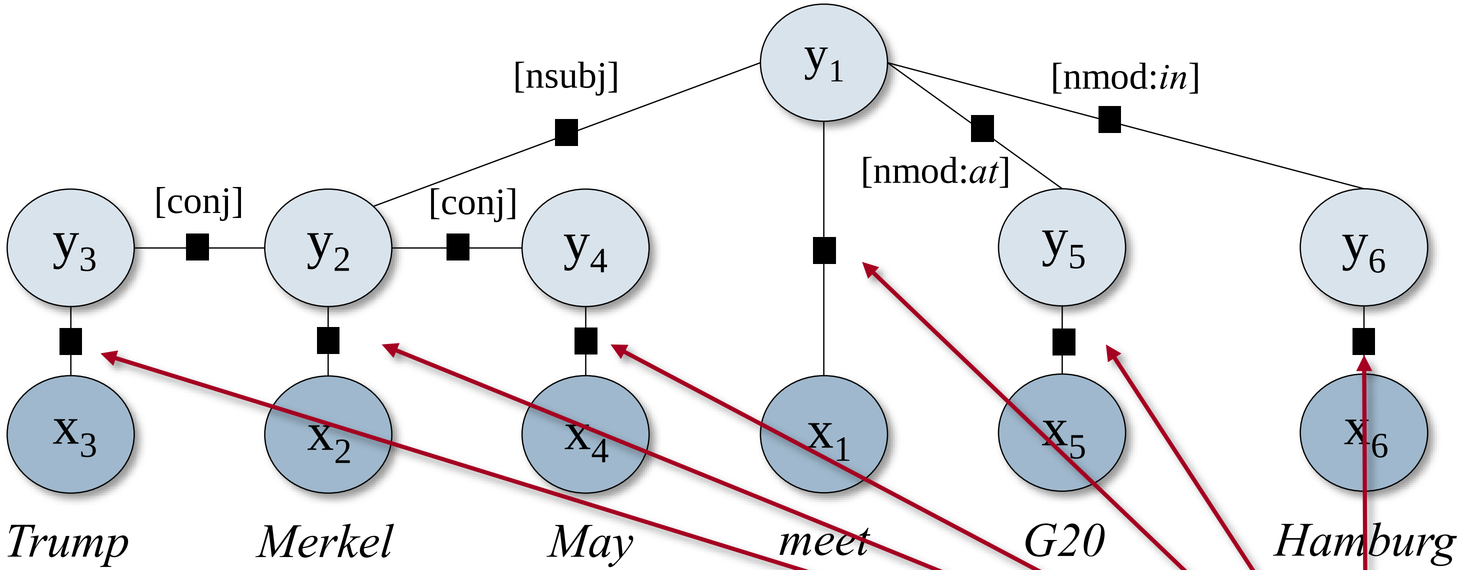


- **Probability distribution** over possible tokens *x* and combined NER/D labels *y*

$$p(\mathbf{x}, \mathbf{y}) = \frac{1}{Z} \prod_A \mathcal{F}_A(\mathbf{x}_A, \mathbf{y}_A)$$

Conditional Random Field in *J*-NERD

[Nguyen et al.: LDOW'14,TACL'16,CIKM'17,PVLDB'17]

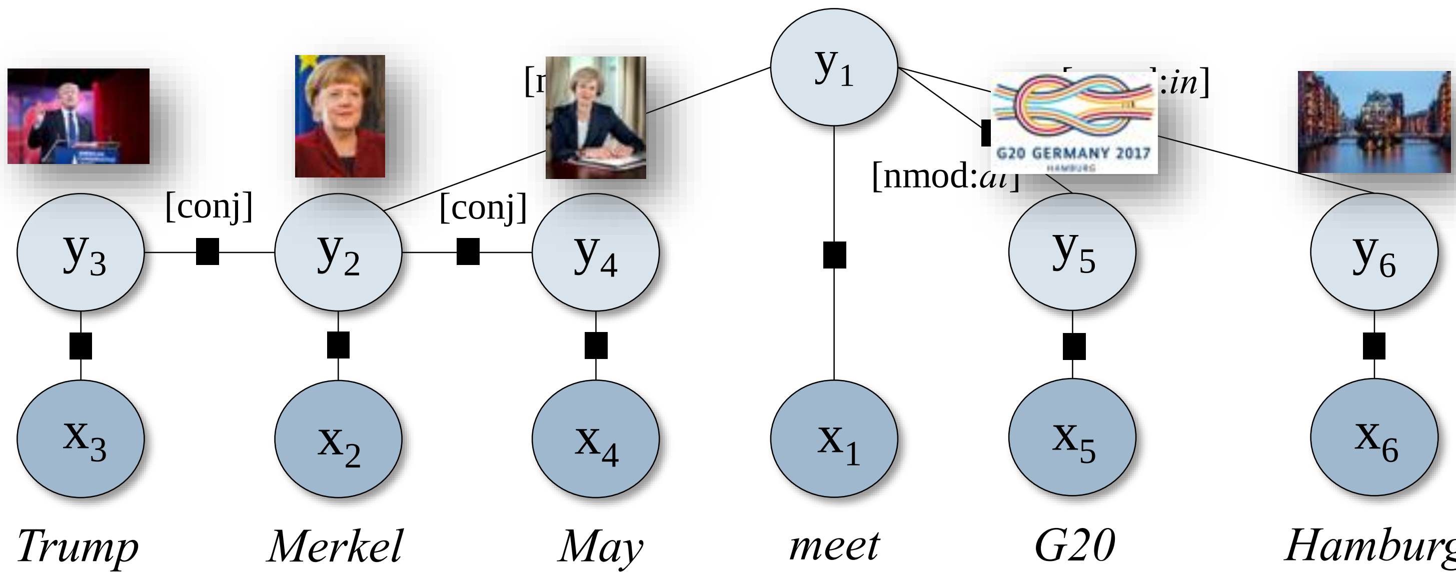


- **Probability distribution** over possible tokens *x* and combined NER/D labels *y*

$$p(\mathbf{x}, \mathbf{y}) = \frac{1}{Z} \prod_A \mathcal{F}_A(\mathbf{x}_A, \mathbf{y}_A)$$

Conditional Random Field in *J*-NERD

[Nguyen et al.: LDOW'14,TACL'16,CIKM'17,PVLDB'17]



- **Probability distribution** over possible tokens $\boldsymbol{x}$ and combined NER/D labels $\boldsymbol{y}$

$$p(\mathbf{x}, \mathbf{y}) = \frac{1}{Z} \prod_{A} \mathcal{F}_A(\mathbf{x}_A, \mathbf{y}_A)$$

- **Probabilistic inference**: find the *most likely* labels $\boldsymbol{y}$, given the observed tokens $\boldsymbol{x}$

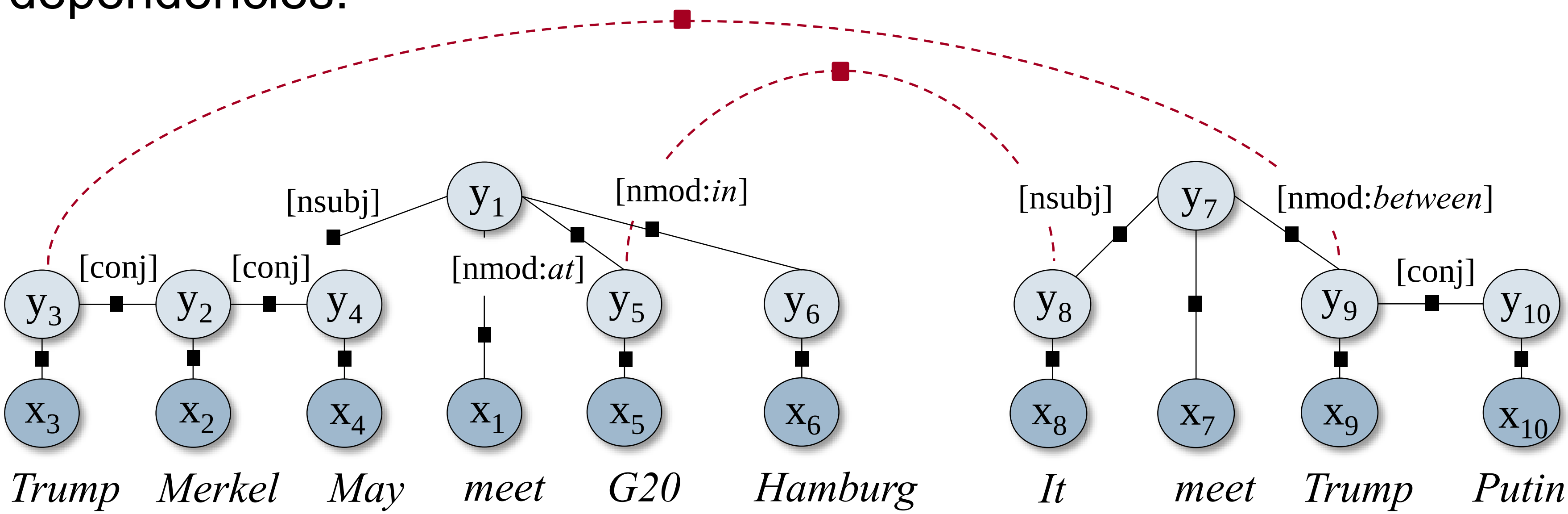
$$\mathbf{y}^* = \arg\max_{\mathbf{y}} p(\mathbf{y} \mid \mathbf{x})$$

- **Viterbi algorithm** (dynamic programming) for fast and exact inference

Conditional Random Field in *J*-NERD

[Nguyen et al.: LDOW'14,TACL'16,CIKM'17,PVLDB'17]

CRF with **cross-sentence** dependencies:



- **Probability distribution** over possible tokens x and combined NER/D labels y

$$p(\mathbf{x},\mathbf{y}) = \frac{1}{Z}\prod_{A} \mathcal{F}_A(\mathbf{x}_A,\mathbf{y}_A)$$

- **Probabilistic inference**: find the *most likely* labels y, given the observed tokens x

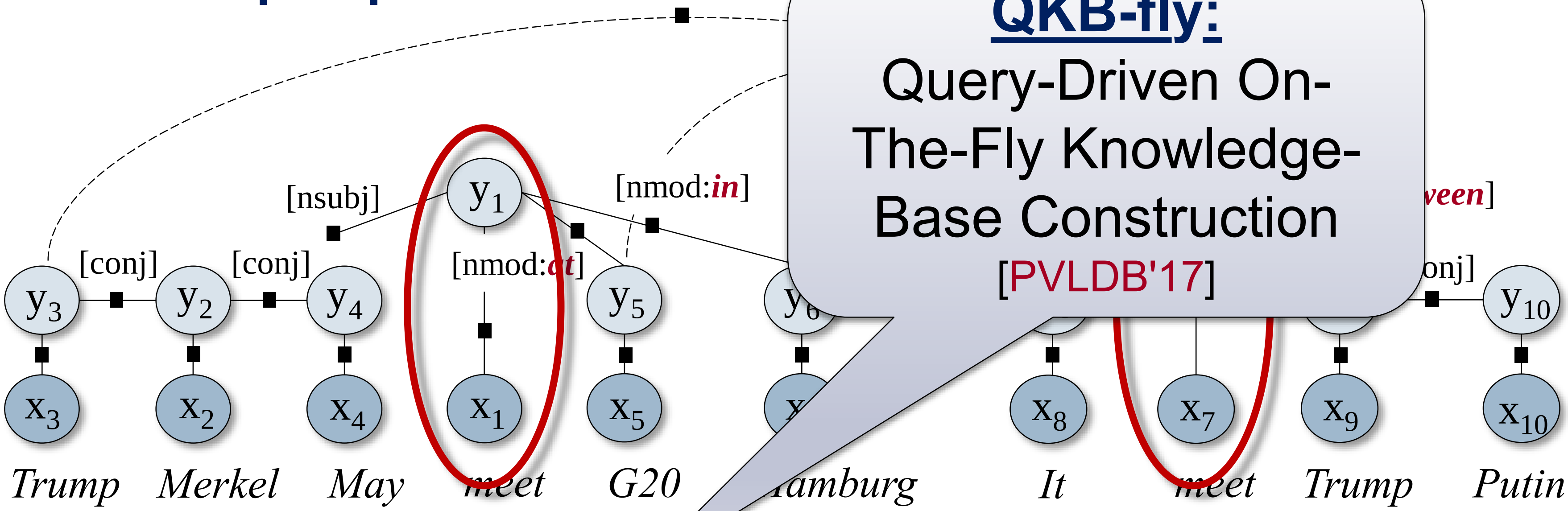
$$\mathbf{y}^* = \arg\max_{\mathbf{y}}\, p(\mathbf{y}\,|\,\mathbf{x})$$

- General factor graphs: **MCMC-style sampling** for approximate inference

J-REED: Joint Relation Extraction & Entity Disambiguation

[Nguyen et al.: CIKM'17,PVLDB'17]

Coupled with repository of 127K **relational paraphrases**:



Facts extracted:

```
meetAtIn(Angela_Merkel, Donald_Trump, 2017_G20_Hamburg_summit, Hamburg)
meetAtIn(Angela_Merkel, Theresa_May, 2017_G20_Hamburg_summit, Hamburg)
meetAtIn(Donald_Trump, Theresa_May, 2017_G20_Hamburg_summit, Hamburg)
meet(Donald_Trump, Validimir_Putin)
```

But not (yet):

```
meetAtIn(Donald_Trump, Vladimir_Putin, 2017_G20_Hamburg_summit, Hamburg)
```

Outline

- Information Extraction

  [SIGMOD'09, WebDB'10, PODS'10, WSDM'11, CIKM'12, CLEF/INEX'11/'12, LDOW'14, TACL'16, CIKM'17, PVLDB'17]

- Probabilistic Databases

  [ICDE'08, VLDB-J'08, SSDBM'10, BTW'11, CIKM'11, ICDE'13, PVLDB'14, ICDE'18, StarAI'18, ICDE'19, SIGMOD'19]

- Distributed Indexing & Query Processing

  [SIGMOD'14, SWIM'14, SIGMOD'16]

Probabilistic Database

A probabilistic database $\mathbf{D}^p$ (compactly) encodes a probability distribution over a finite set of deterministic database instances $\mathbf{D}_i$.

D_1: 0.42

worksAt(sub, obj)	
Lutz	TU_Chemnitz
Lutz	U_Leipzig

D_2: 0.18

worksAt(sub, obj)	
Lutz	TU_Chemnitz

D_3: 0.28

worksAt(sub, obj)	
Lutz	U_Leipzig

D_4: 0.12

worksAt(sub, obj)

- Special Cases:

(1) $\mathbf{D}^p$ tuple-independent

worksAt(sub, obj)		p
Lutz	TU_Chemnitz	0.6
Lutz	U_Leipzig	0.7

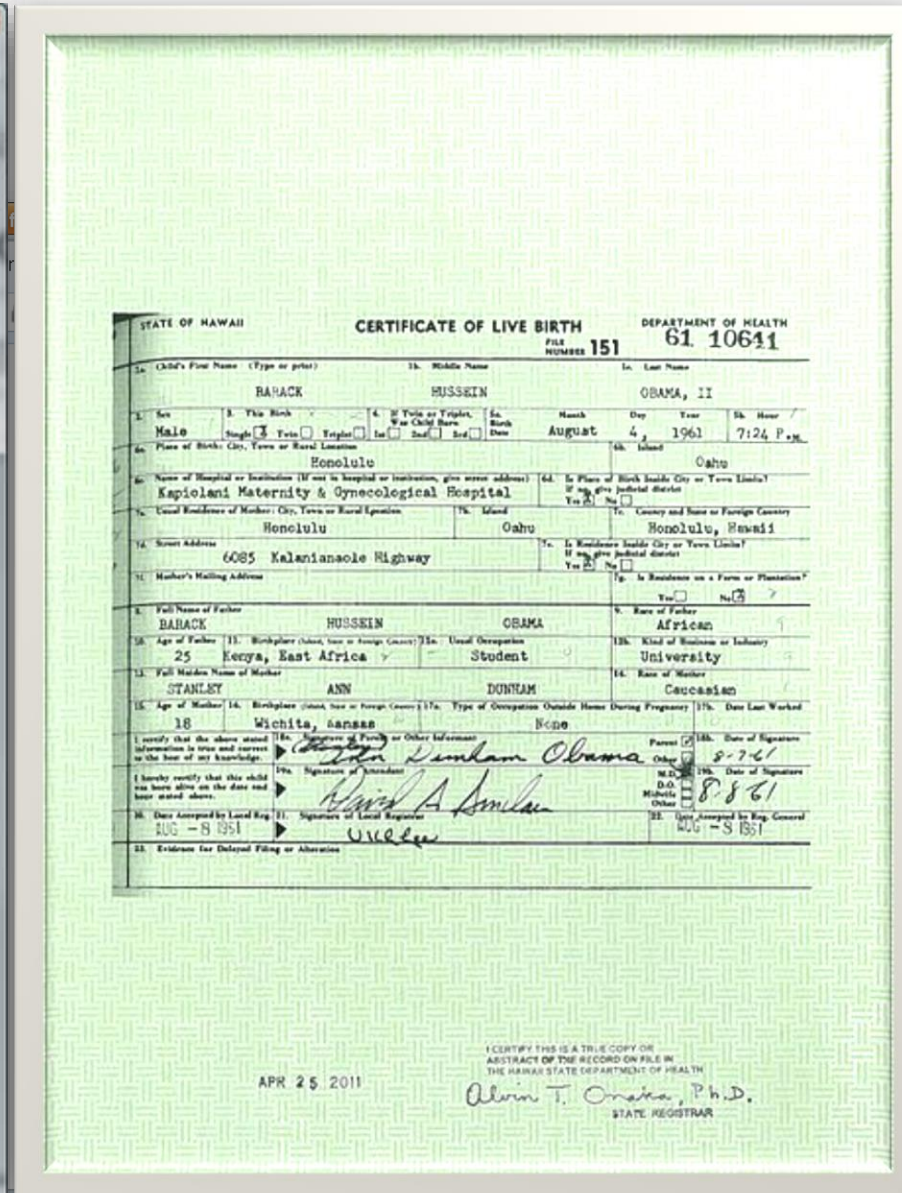
(II) $\mathbf{D}^p$ block-independent

worksAt(sub, obj)		p
Lutz	TU_Chemnitz	0.6
	U_Leipzig	0.4

Note:
(I) and (II) are not equivalent!

- **Query Answering Problem:** ("Marginal Probabilities" of Query Answers)

  Evaluate query **Q** over each instance $\mathbf{D}_i$; for each answer tuple t_j, $P(t_j)$ is the *sum* of the probabilities of all instances $\mathbf{D}_i$ where t_j exists.



bornIn(Barack, Hawaii)

~~**bornIn(Barack, Kenya)**~~

Soft Rules vs. Hard Rules

(**Soft**) Deduction Rules vs.
(**Hard**) Consistency Constraints

- People may **live in** more than one p

  $\texttt{livesIn(x,y)} \Leftarrow \texttt{marriedTo(x,z)} \wedge \texttt{lives}\ldots \texttt{,y)}\ [0.8]$

  $\texttt{livesIn(x,y)} \Leftarrow \texttt{hasChild(x,z)} \wedge \texttt{livesIn(z,y)}\ [0.5]$

- People are not **born in** different places/on different dates

  $\texttt{bornIn(x,y)} \wedge \texttt{bornIn(x,z)} \Rightarrow \texttt{y=z}$

  $\texttt{bornOn(x,y)} \wedge \texttt{bornOn(x,z)} \Rightarrow \texttt{y=z}$

- People are not **married to** more th

  (at the *same time*, in *most countries*?)

  $\texttt{marriedTo(x,y,}t_1\texttt{)} \wedge \texttt{marriedTo(x,z,}t_2\texttt{)} \wedge \texttt{y} \neq \texttt{z}$

  $\Rightarrow \texttt{disjoint(}t_1\texttt{,}t_2\texttt{)}$

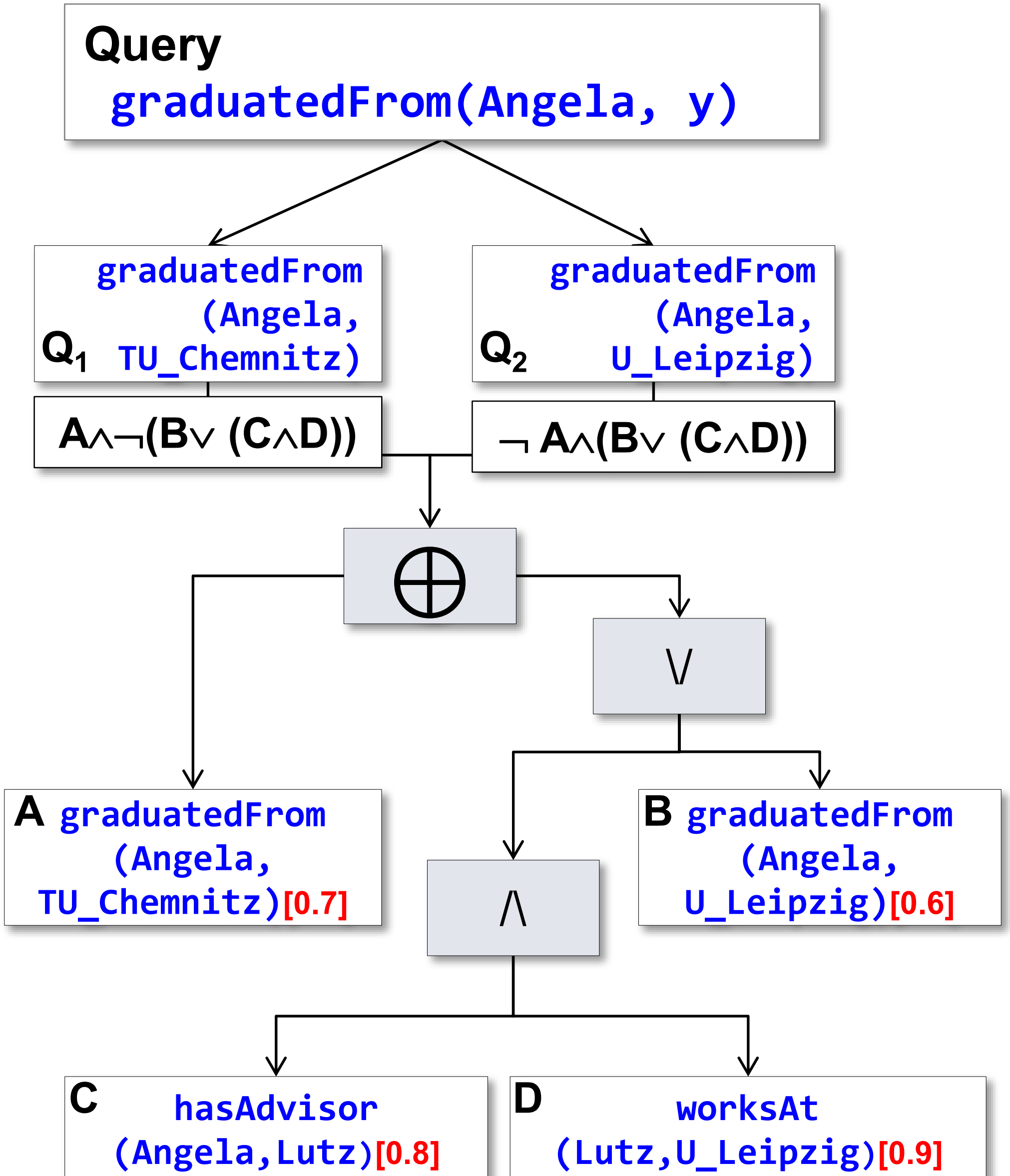
Deductive Database:
Datalog, Core of SQL & Relational Algebra, RDF/S, OWL2-RL, etc.

More General FOL Constraints:
Datalog plus constraints, Block-Indep. PDB's, *owl:FunctionalProperty*, *owl:disjointWith*, etc.

Deductive Grounding with Lineage

(SLD Resolution in Datalog/Prolog)

[Yahya,Theobald: RuleML'11; Dylla,Miliaraki,Theobald: ICDE'13]



Rules

hasAdvisor(x,y) ∧
worksAt(y,z)
⇒ graduatedFrom(x,z)

graduatedFrom(x,y) ∧
graduatedFrom(x,z)
⇒ y=z

Base Facts

graduatedFrom(Angela, TU_Chemnitz)[0.7]
graduatedFrom(Angela, U_Leipzig)[0.6]

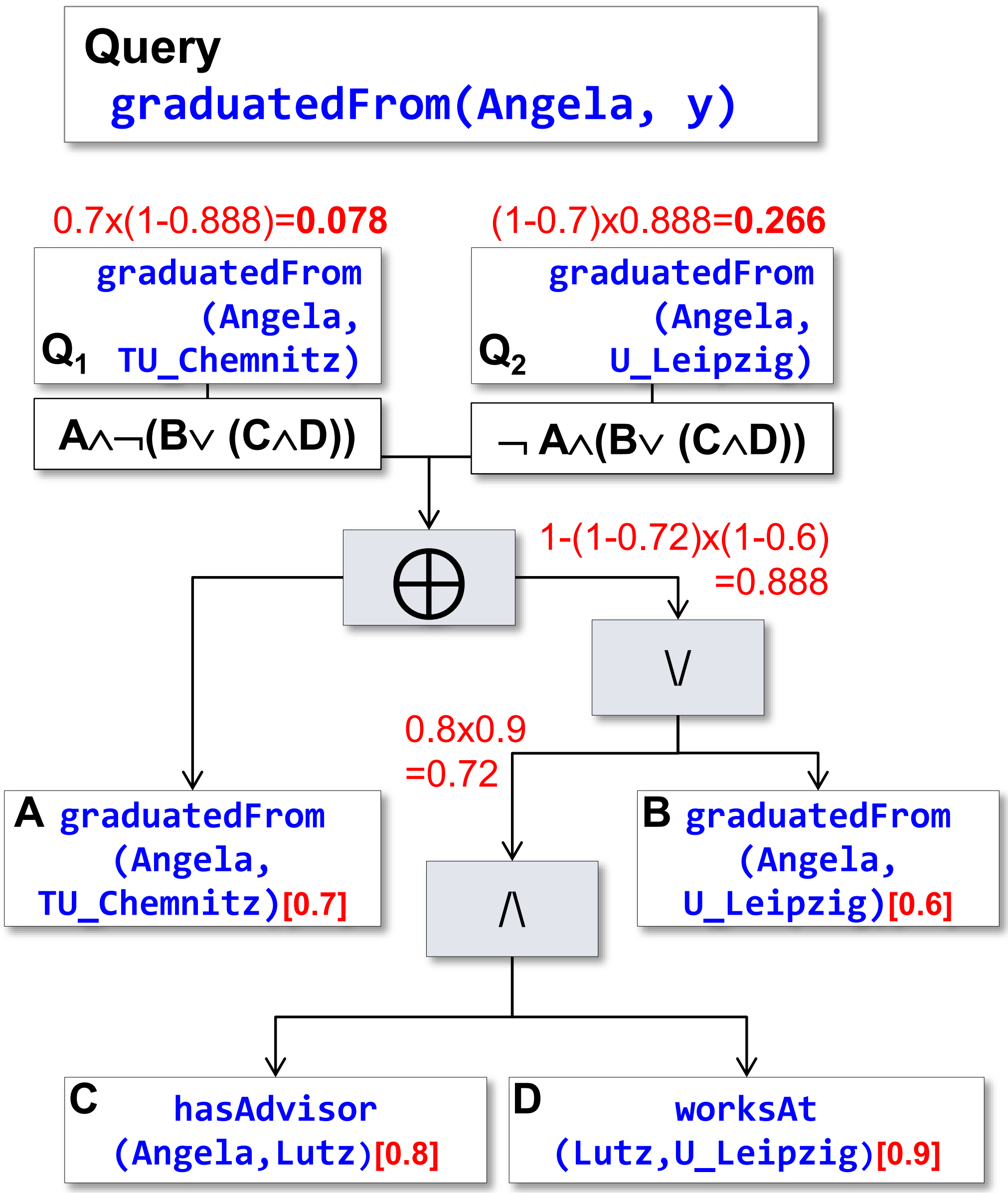
hasAdvisor(Angela, Lutz)[0.8]

worksAt(Lutz, U_Leipzig)[0.9]

instanceOf(Angela, Chemist)[0.5]
instanceOf(Lutz, Chemist)[0.6]
instanceOf(TU_Chemnitz, University)[1.0]
instanceOf(U_Leipzig, University)[1.0]

Lineage & Probabilistic Inference

[Das Sarma,Theobald,Widom: ICDE'08;
Dylla,Miliaraki,Theobald: ICDE'13]



1) Deductive Grounding

- Top-down Datalog evaluation
- Plus tracing the lineage of individual query answers

2) Lineage DAG

- Grounded soft & hard rules
- Base facts with confidences

3) Probabilistic Inference

→ **Compute marginals:**

P(Q): **sum up the probabilities of all possible worlds** that entail the query answers

P(Q|H): drop "impossible worlds"

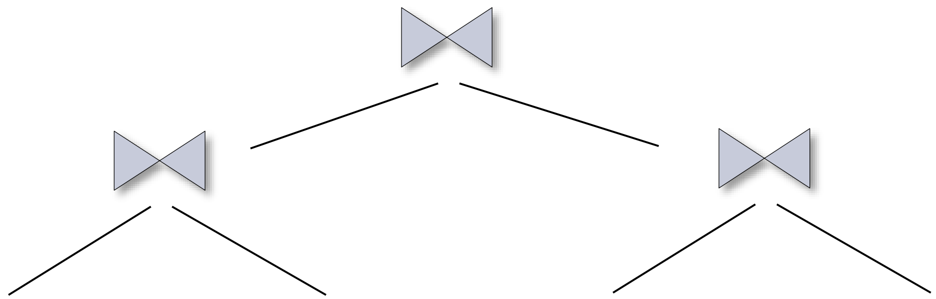
Dichotomy of Queries

[Suciu & Dalvi: SIGMOD'05 Tutorial on "Foundations of Probabilistic Answers to Queries"]

A probabilistic database $\mathbf{D}^p$ (compactly) encodes a probability distribution over a finite set of deterministic database instances $\mathbf{D}_i$.

Is there any professor who works at a university that is located in DE?

$$Q() \Leftarrow isProfessor(prof) \wedge worksAt(prof,uni) \wedge located(uni,DE)$$



isProfessor(prof)	p
Lutz	0.9

worksAt(prof, uni)		p
Lutz	U_Leipzig	0.9
Lutz	TU_Chemnitz	0.2

located(uni, ctry)		p
U_Leipzig	DE	0.8
TU_Chemnitz	DE	0.7

Theorem: The query answering problem for the above join query over a tuple-independent probabilistic database is **#P-hard**.

Outline

- Information Extraction

  [SIGMOD'09, WebDB'10, PODS'10, WSDM'11, CIKM'12, CLEF/INEX'11/'12, LDOW'14, TACL'16, CIKM'17, PVLDB'17]

- Probabilistic Databases

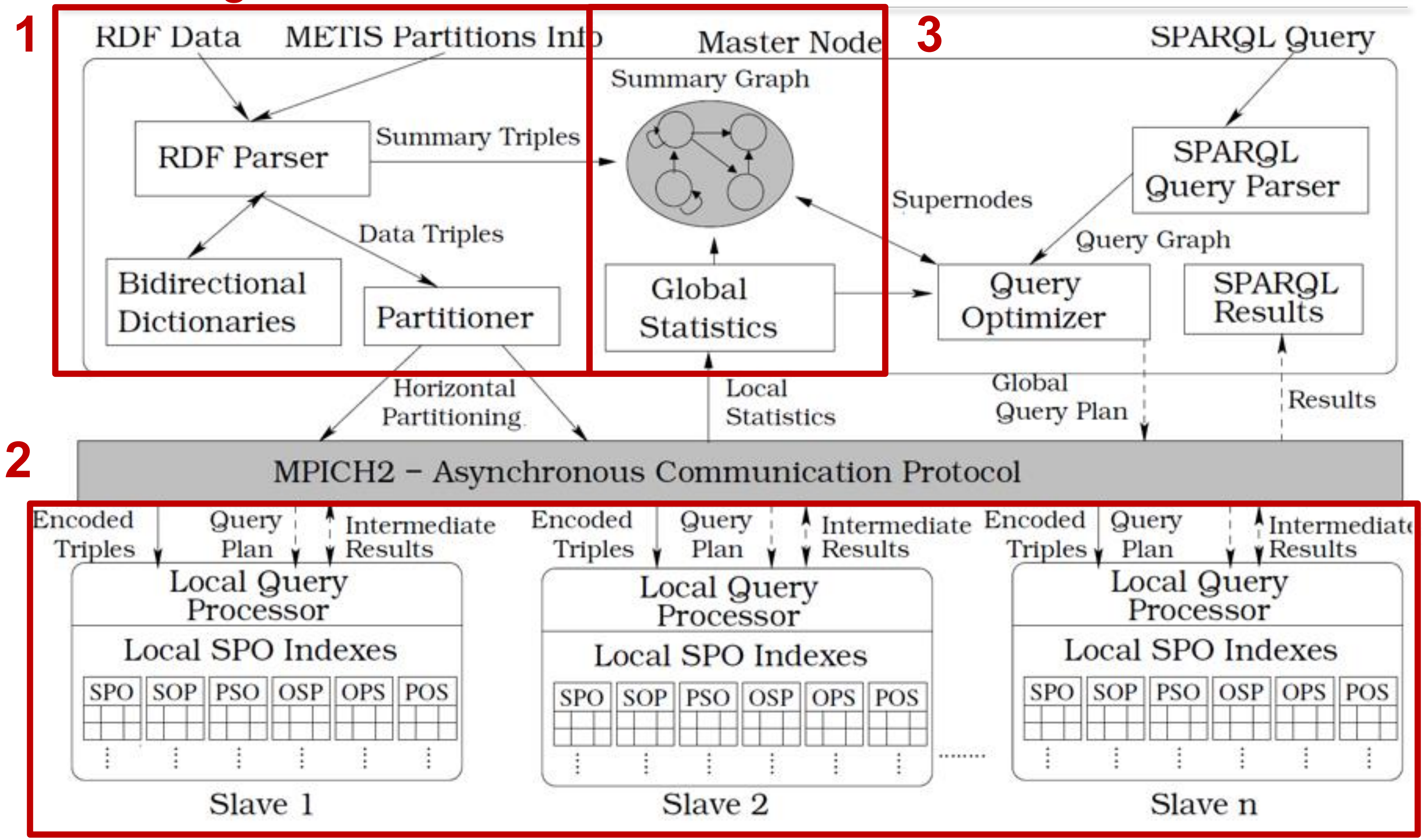
  [ICDE'08, VLDB-J'08, SSDBM'10, BTW'11, CIKM'11, ICDE'13, PVLDB'14, ICDE'18, StarAI'18, ICDE'19, SIGMOD'19]

- Distributed Indexing & Query Processing

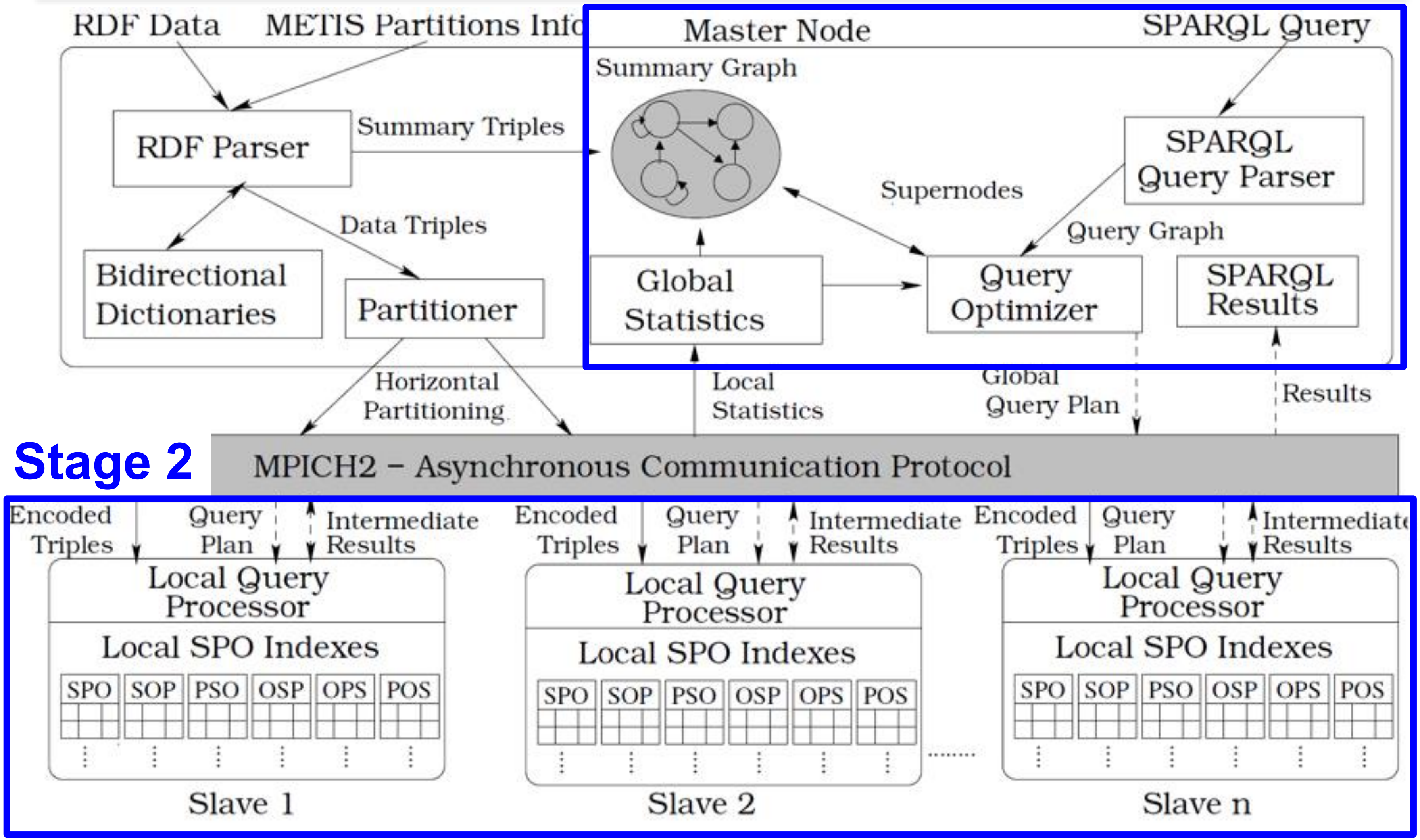
  [SIGMOD'14, SWIM'14, SIGMOD'16]

RDF Indexing

TriAD Graph Engine



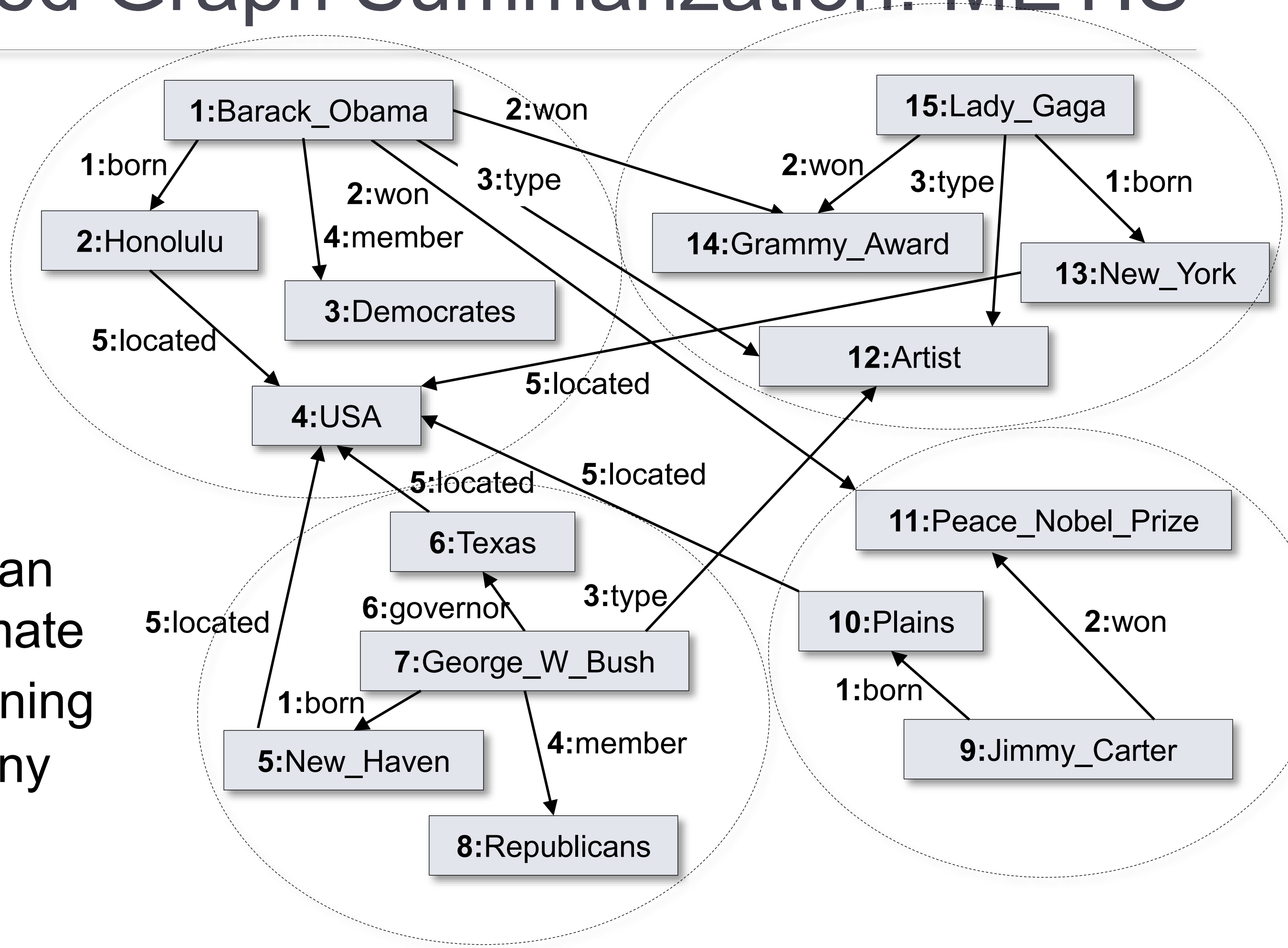
TriAD Graph Engine



→ TriAD follows a very **classical master-slave architecture**; however with a **direct (asynchronous) communication** among all slaves at query time.

Locality-Based Graph Summarization: METIS

$k = 4$



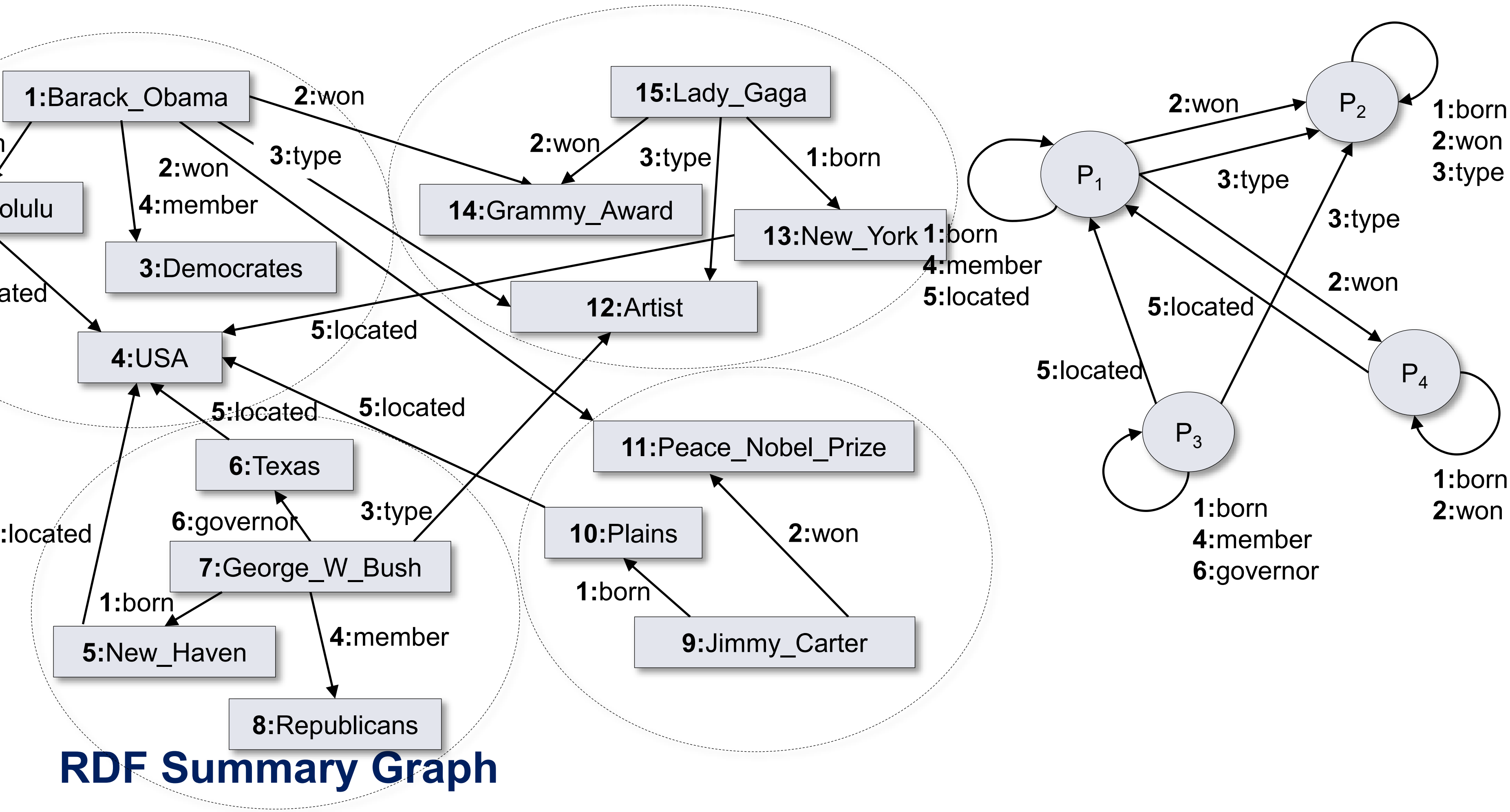
METIS

- Tools like METIS can efficiently approximate a min-k-cut partitioning for graphs with many millions of nodes/edges.

Min-k-Cut

- For a desired amount of k evenly sized partitions, assign each node in the RDF data graph to exactly one partition, such that the number of cut edges among those partitions is minimized.

Summary Graph



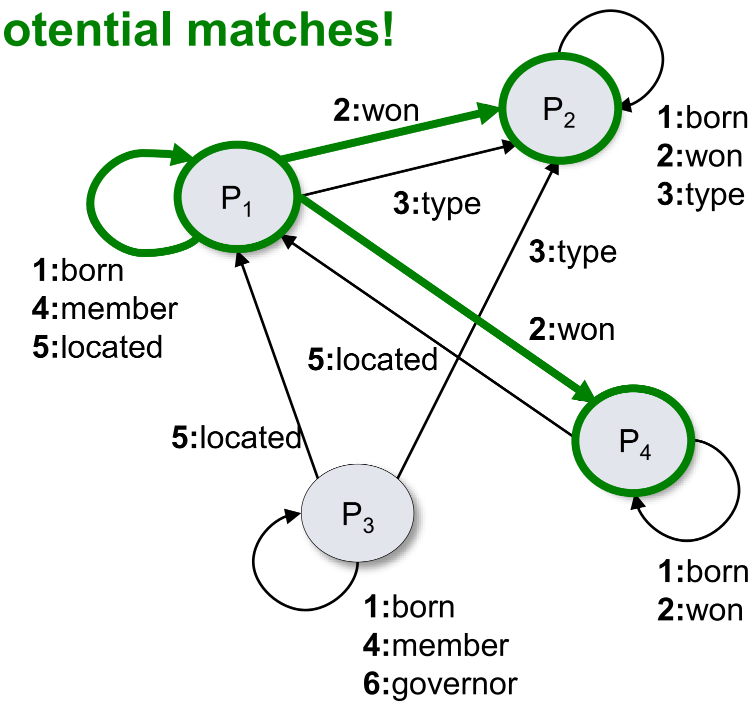
RDF Summary Graph

- Drop all nodes and edges inside the partitions
- Keep only inter-partition edges
- Introduce self-loop edges for intra-partition edges

Querying the Summary Graph

```
SELECT ?c, ?a
WHERE {
  <Barack_Obama> <born> ?c.
  <?c <located> <USA>.
  <Barack_Obama> <won> ?a }
```

Potential matches!



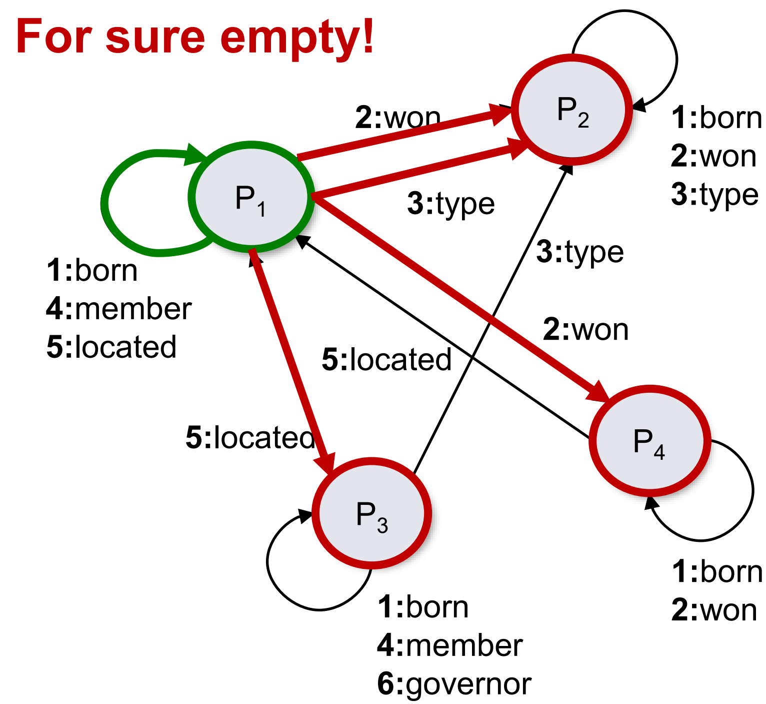
Global Dictionary:

Barack_Obama	$\rightarrow P_1$
USA	$\rightarrow P_1$
Lady_Gaga	$\rightarrow P_2$
Peace_Nobel_Prize	$\rightarrow P_4$

…

Querying the Summary Graph

```
SELECT ?c, ?s
WHERE {
   <Barack_Obama> <born> ?c.
   ?c <located> <USA>.
   <Barack_Obama> <governor> ?s
}
```



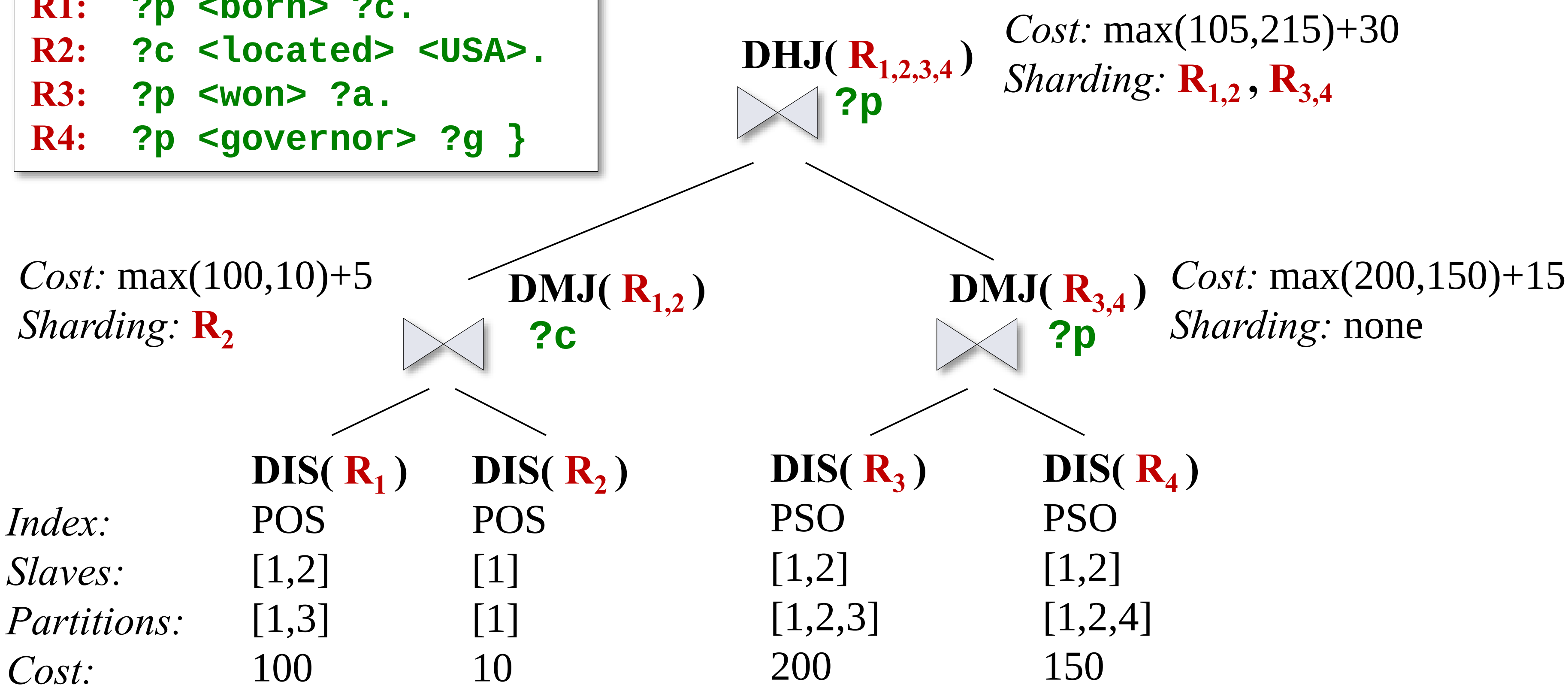
<u>Global Dictionary:</u>

Barack_Obama → P_1
USA → P_1
Lady_Gaga → P_2
Peace_Nobel_Prize → P_4
...

- Summary graph guarantees **no false negatives** (i.e., " missed results"); the subsequent processing of the query against the pruned data graph also ensures **no false positives**.
- Facilitates **join-ahead pruning** by skipping over irrelevant partitions.

Example Query Plan

```
SELECT ?p, ?c, ?a, ?g
WHERE {
R1:  ?p <born> ?c.
R2:  ?c <located> <USA>.
R3:  ?p <won> ?a.
R4:  ?p <governor> ?g }
```

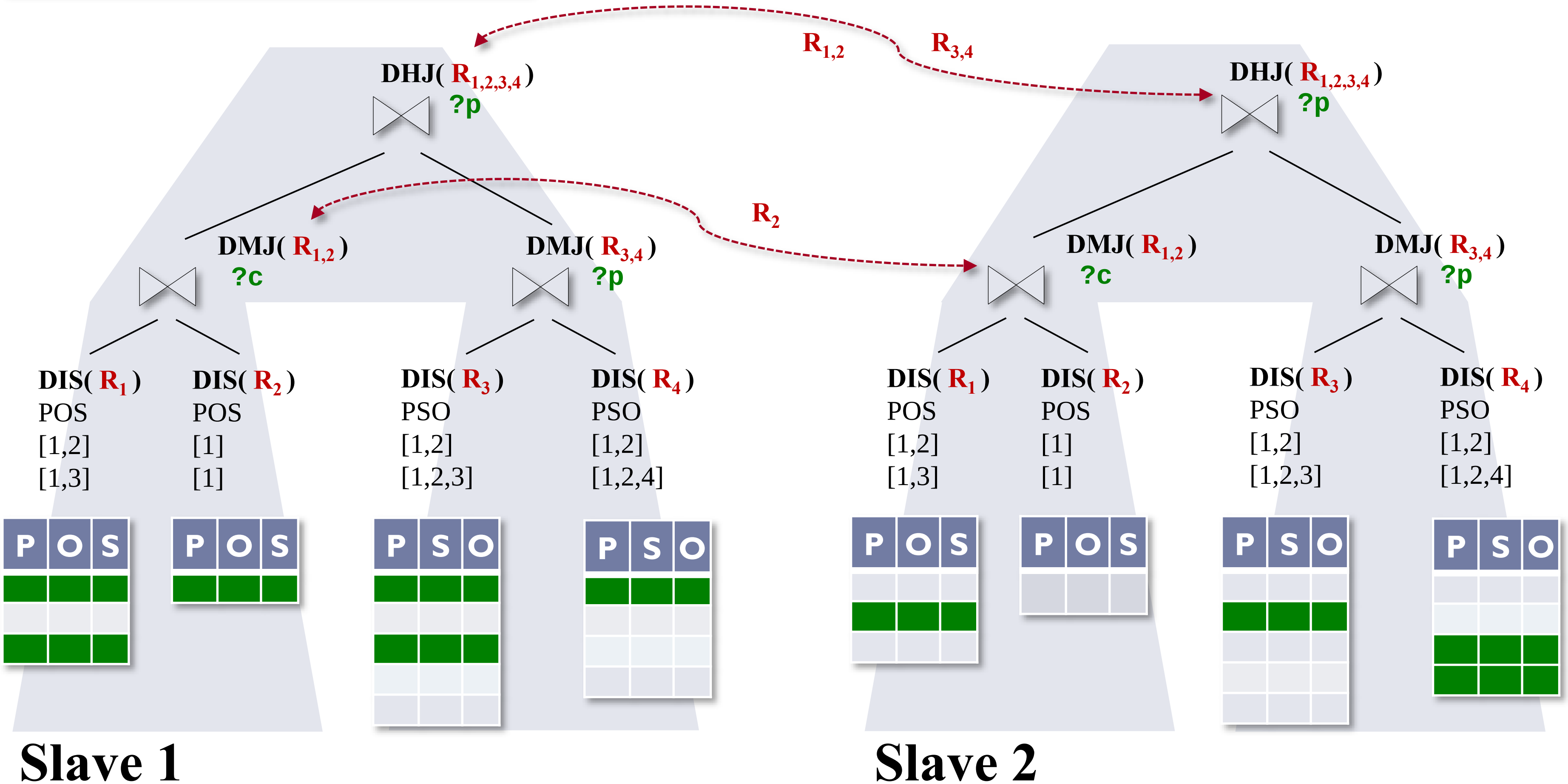


- A copy of the same query plan is shipped to all slaves:
  - DIS operators (leafs) are augmented with **locality** and **pruning information**.
  - 6 SPO permutations allow the usage of **DMJ op's at the first level of joins**.

Distributed & Multithreaded Query Execution

```
SELECT ?p, ?c, ?a, ?g
WHERE {
R1:  ?p <born> ?c.
R2:  ?c <located> <USA>.
R3:  ?p <won> ?a.
R4:  ?p <governor> ?g }
```

- All slaves **concurrently** and **asynchronously** process the same query plan, but each over **disjoint partitions** of the SPO permutation indexes.



Summary

Information Extraction

- Natural-Language Processing & Understanding
- Named-Entity Recognition & Disambiguation
- Relation Extraction
- Knowledge-Graph Construction, Integration & Maintenance

Uncertain Data

- Probabilistic & Temporal Databases
- Data Integration & Cleaning
- Model- & Dissociation-based Bounds
- Scalable Probabilistic Inference

Big Data

- Scalable Analytics
- Distributed Indexing & Query Processing
- Real-Time Stream Processing
- Message Passing & Asynchronous Protocols

References

- M. V. d. Heuvel, P. Ivanov, W. Gatterbauer, F. Geerts, M. Theobald: Anytime Approximation in Probabilistic Databases via Scaled Dissociations. SIGMOD Conference 2019
- K. Papaioannou, M. Theobald, M. H. Böhlen: Outer Joins and Anti Join in Temporal-Probabilistic Databases. ICDE 2019
- K. Papaioannou, M. Theobald, M. H. Böhlen: Supporting Set Operations in Temporal-Probabilistic Databases. ICDE 2018
- M. V. d. Heuvel, F. Geerts, W. Gatterbauer, M. Theobald: A General Framework for Anytime Approximation in Probabilistic Databases. StarAI 2018
- D. B. Nguyen, M. Theobald, G. Weikum: QKBfly: Query-Driven On-The-Fly Knowledge Base Construction. PVLDB 2017
- D. B. Nguyen, M. Theobald, G. Weikum: J-REED: Joint Relation Extraction and Entity Disambiguation. CIKM 2017
- S. Gurajada, M. Theobald: Distributed Set Reachability. SIGMOD 2016
- D. B. Nguyen, M. Theobald, G. Weikum: J-NERD: Joint Named Entity Resolution and Disambiguation with Rich Linguistic Features. TACL Vol. 4, 2016
- Hernán Blanco: Scaling Probabilistic Databases. VLDB PhD Workshop 2015
- D. B. Nguyen, J. Hoffart, M. Theobald, G. Weikum: AIDA-light: High-Throughput Named-Entity Disambiguation. LDOW 2014
- S. Gurajada, S. Seufert, I. Miliaraki, M. Theobald: TriAD: A Distributed Shared-Nothing RDF Engine based on Asynchronous Message Passing. SIGMOD 2014
- M. Dylla, M. Theobald, I. Miliaraki: Querying and Learning in Probabilistic Databases. Reasoning Web 2014
- M. Dylla, I. Miliaraki, M. Theobald: A Temporal-Probabilistic Database Model for Information Extraction. PVLDB 2013
- M. Dylla, I. Miliaraki, M. Theobald: Top-k Query Processing in Probabilistic Databases with Non-Materialized Views. ICDE 2013
- N. Nakashole, M. Sozio, F. Suchanek, M. Theobald: Query-Time Reasoning in Uncertain RDF Knowledge Bases with Soft and Hard Rules. VLDS 2012
- M. Yahya, M. Theobald: D2R2: Disk-Oriented Deductive Reasoning in a RISC-Style RDF Engine. RuleML 2011
- T. Meiser, M. Dylla, M. Theobald: Interactive Reasoning in Uncertain RDF Knowledge Bases. CIKM 2011
- N. Nakashole, M. Theobald, G. Weikum: Scalable Knowledge Harvesting with High Precision and High Recall. WSDM 2011
- M. Dylla, M. Sozio, M. Theobald: Resolving Temporal Conflicts in Inconsistent RDF Knowledge Bases. BTW 2011
- N. Nakashole, M. Theobald, G. Weikum: Find your Advisor: Robust Knowledge Gathering from the Web. WebDB 2010
- A. D. Sarma, M. Theobald, J. Widom: LIVE: A Lineage-Supported Versioned DBMS. SSDBM 2010
- A. D. Sarma, M. Theobald, J. Widom: Exploiting Lineage for Confidence Computation in Uncertain and Probabilistic Databases. ICDE 2008
- O. Benjelloun, A. D. Sarma, A. Y. Halevy, M. Theobald, J. Widom: Databases with uncertainty and lineage. VLDB-J. 17(2), 2008

Annex D – PhD candidate presentations

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Ethical, Legal and Social issues of eHealth regarding sharing personal sensitive data on an IoE platform

ESR 12 – Position 15

Bologna, 20 November 2019

Daniela Brešić

Background

<u>Digital Health:</u>

- The provision of quality care depends on ICT
- Increasing self-engagement of citizens and patients
- Care providers depend on transfer of correct information
- Improvement of healthcare systems depends on data

→ Data sharing can be <u>beneficial</u> for the *patient, public health* and *provision of care* in general

RIoE
Rights of Internet of Everything

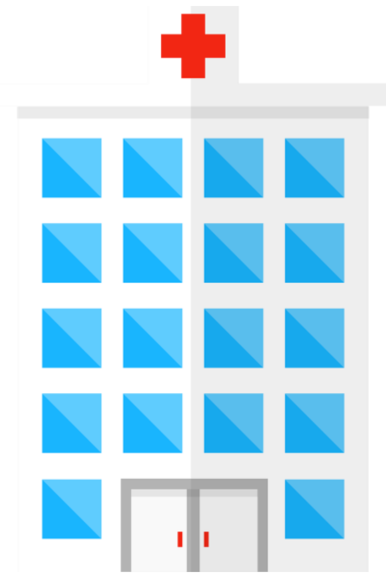
Research objective

Aim:

Elaboration of a desirable ethical-legal model for (medical) data sharing with an emphasis on the responsibility of citizens towards the healthcare system

→Analysis of a potential moral duty from the citizen's perspective towards the healthcare system and society in general to share (medical) data

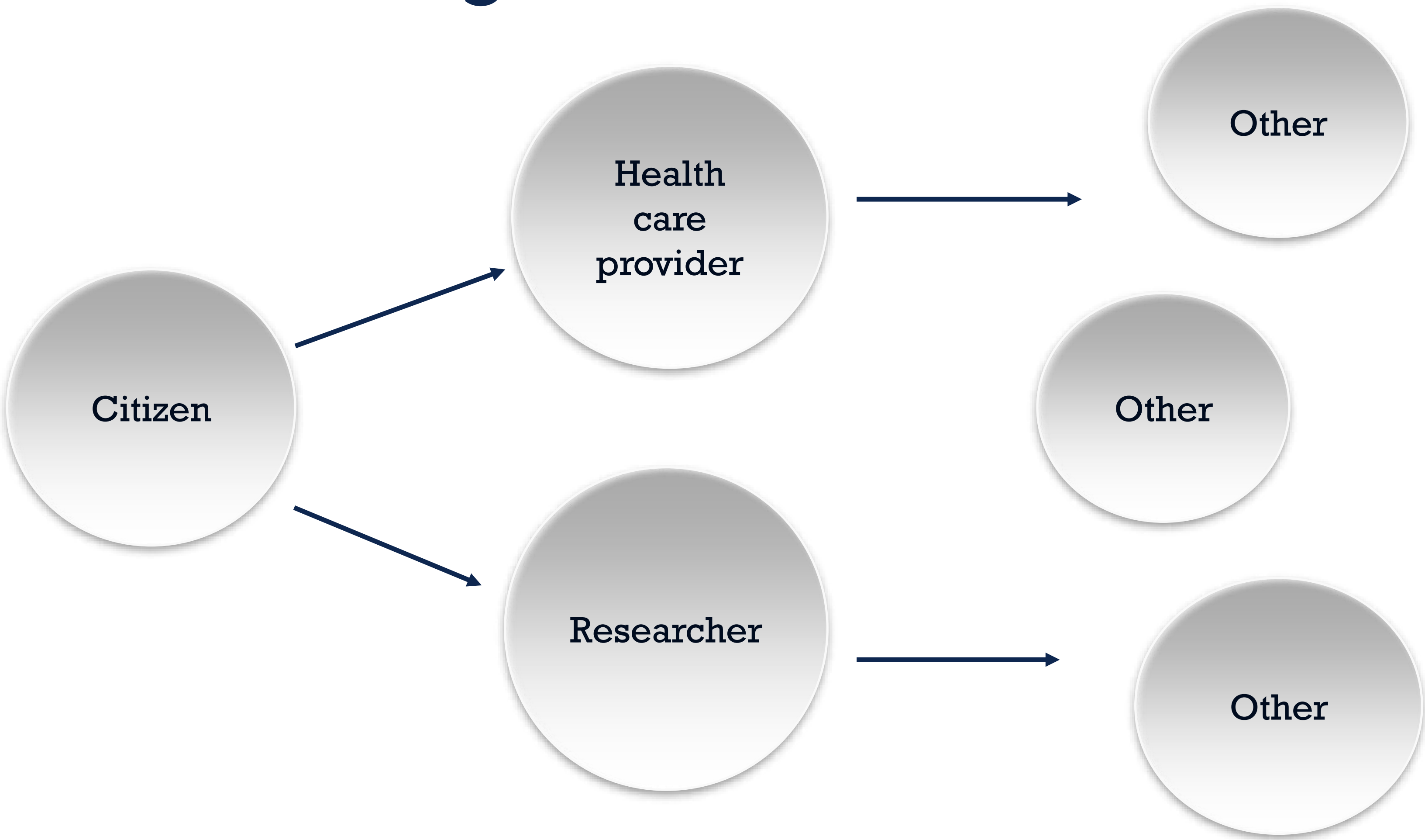
→ Balancing the rights of citizens with the public interest of improvement of eHealth services



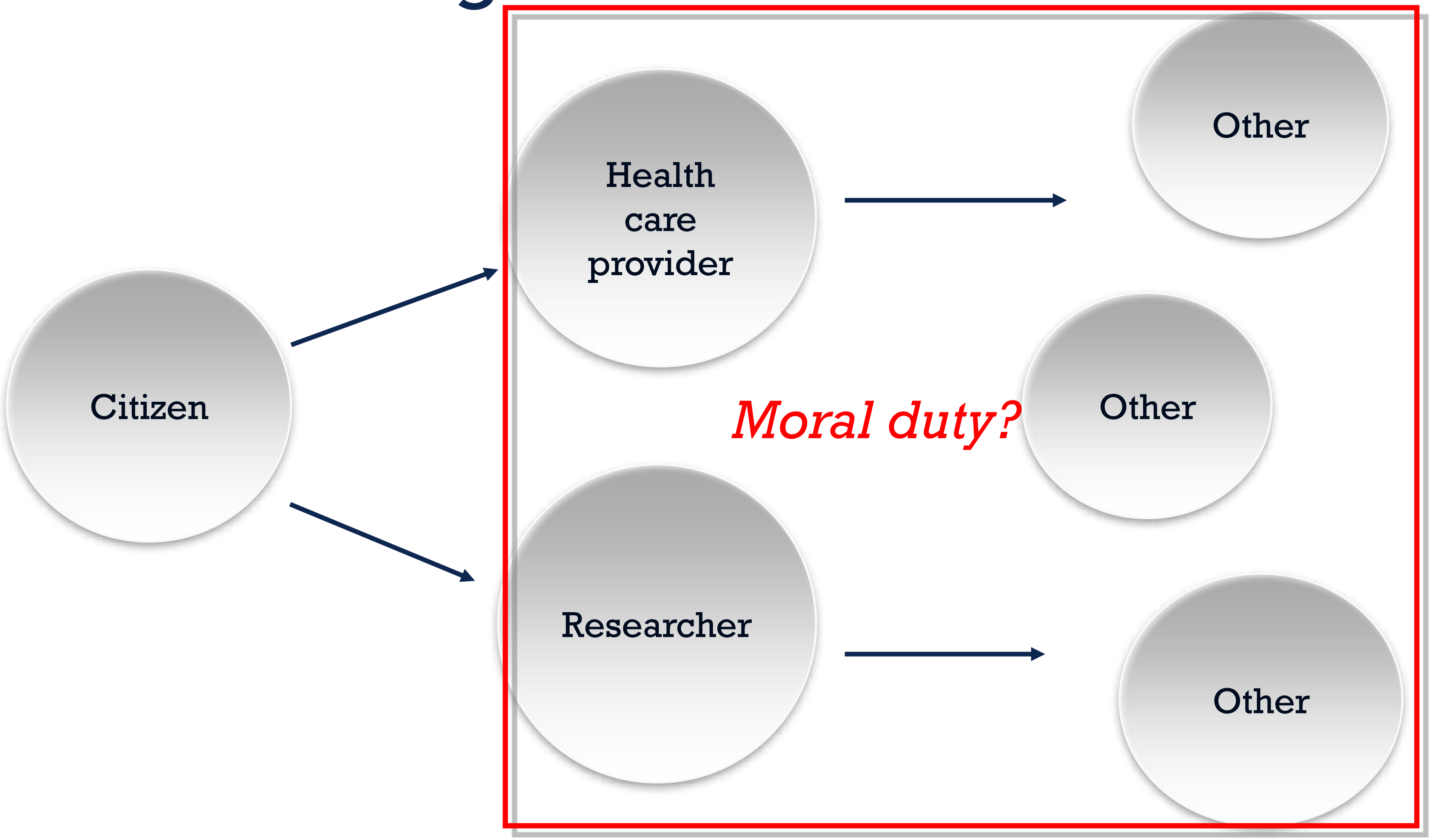
RIoE

Rights of Internet of Everything

Data sharing activities



Data sharing activities



Rights of Internet of Everything

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

WHAT ARE HUMAN RIGHTS? DONATE

UN expert warns of enormous privacy concerns over health data as he unveils international protection standards

NEW YORK (29 October 2019) – The UN Special Rapporteur on the right to privacy, Joseph Cannataci, has unveiled a set of international standards on how health data should be used and protected, warning of enormous threats to privacy if the industry is not regulated.

"My recommendations, which I believe are the first of their kind, provide a common international

https://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25221&LangID=E

State of the art

LEGAL

- Danger of unintended disclosure or misuse of health data.
- Practical approach for data sharing in smart health with a view to consent and privacy by design.
  - → Criticism: Difficulties of a consent-centered approach as citizens have the possibility to withdraw consent, and as privacy by design and by default principles are burdensome obligations for controllers and processors.
- Data subject's rights (e.g. right to be forgotten, right to access etc.) affected through the interconnected infrastructure of IoE.
- Only limited control over data sharing as it is difficult to trace data.

ETHICS

- Typical roles in healthcare characterised by the doctor-patient relationship seem to transition; issues arise with regard to the right to privacy and the duty of confidentiality.
- Some ethics-scholars identify trust in care providers as crucial for data sharing. At the same time, too much insight into data processing activities may confuse the citizen leading the citizen to refuse the participation in data sharing.
- Blurring boundaries between health and non-health data.

RIoE
Rights of Internet of Everything

Material Scope

The doctoral thesis will examine:

- The **framework of the European Union** (e.g. Regulation (EU) 2016/679) and the **Council of Europe** (e.g. Recommendation on the protection of health-related data);
- **National legislation** with regard to relevant issues related to data sharing and IoE Health platforms (e.g. data sharing for research purposes): likely national legislation of German-speaking Member States (e.g. Germany and/or Austria) and English-speaking Member States (e.g. UK and/or Ireland) of the European Union;
- **Ethical issues** through literature study with regard to eHealth platforms mainly from the perspective of the ethical theories of utilitarianism, deontology and Kantianism (method of reflective equilibrium).

RIoE
Rights of Internet of Everything

Novelty and Impact

NOVELTY

- (Medical) data sharing from the perspective of the citizens' increasing self-engagement and their potential responsibility towards healthcare providers.
- Legal debates seem to neglect a protection of health data from the perspective of the doctor's obligation to confidentiality.
- Inter-disciplinary and coherent ethical-legal system for data sharing in IoE and eHealth.

IMPACT

- The proposed research pursues to benefit a range of stakeholders:
  - Legislators
  - Scholars
  - Practitioners, and
  - Consumers/patients

RIoE
Rights of Internet of Everything

Output

1. An analysis of moral duties or responsibilities of citizens, patients, healthcare providers (organisations) and researchers.
2. A comprehensive overview of the citizens' rights under the current legal framework, i.e. data protection, privacy and confidentiality regulation, with a particular view to eHealth;
3. An investigation of ethical and legal issues that arise in the context of data sharing on IoE Health platforms with regard to the analysed citizens' rights;
4. A discussion of currently existing relevant legal and ethical framework;
5. Recommendation and guidance as regards to whether, how and to what extent the current legal and ethical framework ought to be modified with a view to the citizens', patients', healthcare providers', researchers' and organizations' moral duties.

Rights of Internet of Everything

Thank you for your attention!

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 814177

Rights of Internet of Everything

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Enforcing security data processing through a legal ontology

Candidate: Pier Giorgio Chiara

+

STATE OF THE ART

- IoT as the next step towards digitalization
- IoT resource-constrained devices are likely to challenge many principles of privacy and data protection
- Deployment of IoT resource-constrained devices poses a threat to data (or information) security
- Information security: protection of information (and information systems) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

+

- Article 32 of GDPR follows a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take

- Several security risk assessment methodologies and frameworks have been developed for the compliance and reliability of such systems

RESEARCH QUESTIONS

1. How do we account for poorly informed consent on weaknesses in security of processing, in order not to hinder informational self-determination of the users?

Rights of Internet of Everything

2. Since small and medium enterprises (SMEs) are increasingly relying on IT networks, systems and applications, how can data controllers be assisted in the comprehension of the specificities of the risks associated with processing, given that they do not have expertise and resources of a big company?

Rights of Internet of Everything

PROJECT PROPOSAL

The aim of the project is twofold:

1. Providing guidelines to data controllers (especially if SMEs) operating within IoT constrained-devices context to develop a security risk management plan

2. Enhancing users' trust by increasing transparency and risk perception of data processing in IoT systems

These goals shall be achieved through the development and implementation of an ontology aiming at providing a structured representation of these issues, following the MeLon methodology

+

Benefit of the chosen approach:

- Increasing transparency of data collections: most PETs are useless if they are not used properly or if they are not implemented in an automated way
- User awareness: improve the users' understanding and control over their data profile
- Accountability of data controller: encourage data controllers to implement practical tools for effective data protection

METHODOLOGY AND APPROACH

VERTICAL OBSERVABLE

- First phase: guidelines for SMEs on the security of personal data processing
- Second phase: improvement of users' understanding of the challenges posed to data security by IoT

HORIZONTAL OBSERVABLE

- Source of knowledge acquisition for the vertical observable

1. Regulative instruments
2. Standards
3. Guidelines
4. Code of conducts and certification mechanisms (art40 and 42 GDPR)

VERTICAL OBSERVABLE

FIRST PHASE

1. Assessing security risks

2. Appropriate measures ex art 32 GDPR:

   - Organizational

   - Technical

SECOND PHASE

1. Privacy by design and by default are closely interlinked with security of processing

2. PETs may be flawed: re-identification of personal data

3. DPIA required for high risk processing

HORIZONTAL PHASE

1. GDPR
2. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union
3. Cybersecurity Act
4. NIS Directive
5. Relevant extra-EU legal provisions: UK and US
6. Standards:

- Enisa (2016) Guidelines for SMEs on the security of personal data processing
- Enisa (2018) Recommendations on shaping technology according to GDPR provisions: Exploring the notion of data protection by default
- AIOTI

+

THANK YOU FOR THE ATTENTION

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Enforcing security data processing through a legal ontology

Candidate: Pier Giorgio Chiara

+

STATE OF THE ART

- IoT as the next step towards digitalization
- IoT resource-constrained devices are likely to challenge many principles of privacy and data protection
- Deployment of IoT resource-constrained devices poses a threat to data (or information) security
- Information security: protection of information (and information systems) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

+

- Article 32 of GDPR follows a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take

- Several security risk assessment methodologies and frameworks have been developed for the compliance and reliability of such systems

RESEARCH QUESTIONS

1. How do we account for poorly informed consent on weaknesses in security of processing, in order not to hinder informational self-determination of the users?

Rights of Internet of Everything

2. Since small and medium enterprises (SMEs) are increasingly relying on IT networks, systems and applications, how can data controllers be assisted in the comprehension of the specificities of the risks associated with processing, given that they do not have expertise and resources of a big company?

+

PROJECT PROPOSAL

The aim of the project is twofold:

1. Providing guidelines to data controllers (especially if SMEs) operating within IoT constrained-devices context to develop a security risk management plan

2. Enhancing users' trust by increasing transparency and risk perception of data processing in IoT systems

These goals shall be achieved through the development and implementation of an ontology aiming at providing a structured representation of these issues, following the MeLon methodology

RIoE
Rights of Internet of Everything

+

Benefit of the chosen approach:

- Increasing transparency of data collections: most PETs are useless if they are not used properly or if they are not implemented in an automated way
- User awareness: improve the users' understanding and control over their data profile
- Accountability of data controller: encourage data controllers to implement practical tools for effective data protection

METHODOLOGY AND APPROACH

VERTICAL OBSERVABLE

- First phase: guidelines for SMEs on the security of personal data processing
- Second phase: improvement of users' understanding of the challenges posed to data security by IoT

HORIZONTAL OBSERVABLE

- Source of knowledge acquisition for the vertical observable

1. Regulative instruments
2. Standards
3. Guidelines
4. Code of conducts and certification mechanisms (art40 and 42 GDPR)

+

VERTICAL OBSERVABLE

FIRST PHASE

1. Assessing security risks

2. Appropriate measures ex art 32 GDPR:

   - Organizational

   - Technical

SECOND PHASE

1. Privacy by design and by default are closely interlinked with security of processing

2. PETs may be flawed: re-identification of personal data

3. DPIA required for high risk processing

HORIZONTAL PHASE

1. GDPR
2. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union
3. Cybersecurity Act
4. NIS Directive
5. Relevant extra-EU legal provisions: UK and US
6. Standards:

- Enisa (2016) Guidelines for SMEs on the security of personal data processing
- Enisa (2018) Recommendations on shaping technology according to GDPR provisions: Exploring the notion of data protection by default
- AIOTI

THANK YOU FOR THE ATTENTION

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

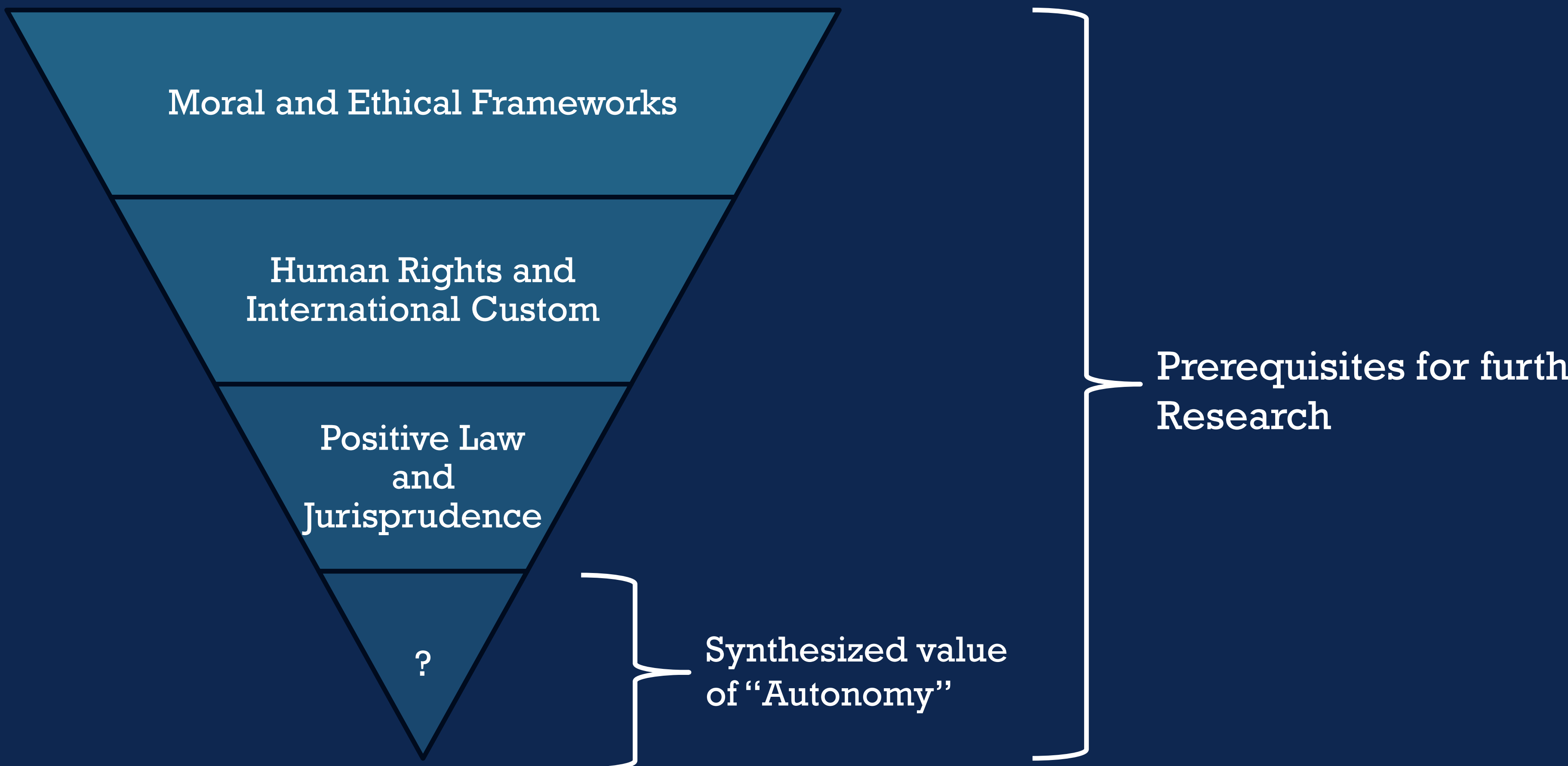
Influenceable Autonomy and Predictable Freedom in the IoE

Maximilian Gartner

Overview

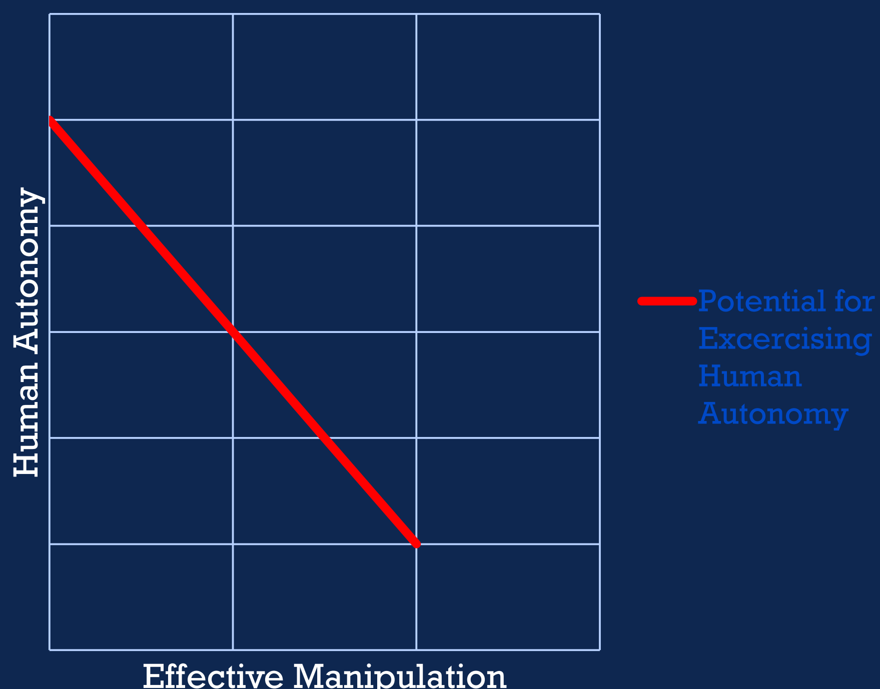
- Freedom & Autonomy
- Agents in the IoE
- Influencable Autonomy / Predictable Freedom
- Attribution of Agent Behaviour
- Existing Regulatory Framworks: Analysis and Outlook
- Research Questions

Freedom & Autonomy I Framework



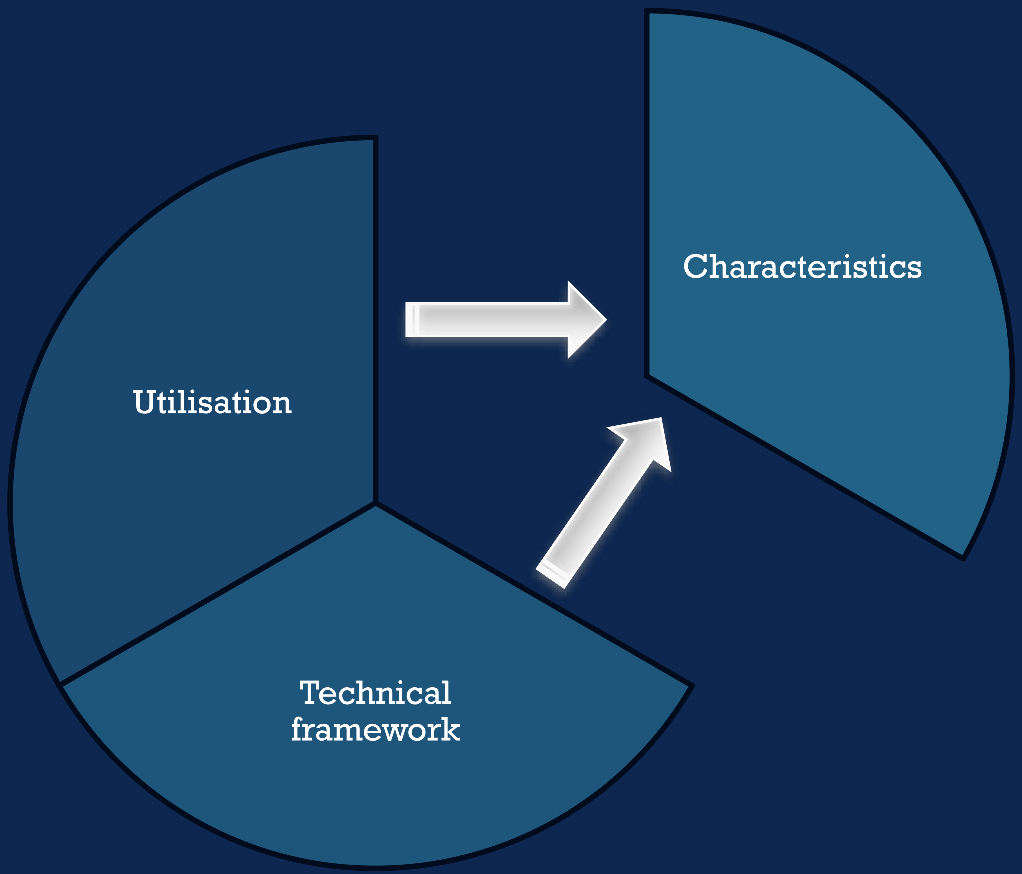
Freedom & Autonomy II
Autonomy as a Human Trait

- Manipulation of human autonomy presupposes human autonomy. Effective influence impacts realistic excercise of human autonomy, creating an "autonomy gradient".



Benefits	**Disadvantages**
• Utility from Agency • Utility from Meaning • Positive Self-Attribution • No Lack of Perceived Self-Determination • Option Attachment	• Responsibility as a Burden • Agency as a Cost • Choice Overload

+ Agents in the IoE - Fundamentals



- Agents usually exhibit characteristics, that make them difficult to control with respect to enforcing autonomy
  - Inscrutability
  - Adaptability
  - Insights from Inconspicuous Data
  - Irrelevance of Anonymity

Influencable Autonomy / Predictable Freedom I

Information Handling

Assignation of Attributes to Human Users

Inhibition/Exacerbation of Human Behaviour

Human as an adjustable variable?

Preemptive Behaviour

Positive Influence / Nudging

Privacy as a Prerequisite to Autonomy?

Attribution of Agent Behaviour

- Attesting Moral Agency to IoE-Agents allows exculpation of human "decision-makers".
- Agents do not always exhibit result-specific "intent".
- Distributed Responsibility: Network of different agents with varying moral agency values and humans.
- Complexity / Unpredictability allows for humans to yield accountability.

Existing Regulatory Frameworks: Analysis and Outlook

- Ethical Frameworks
- Legal Frameworks
  - UDHR / ECHR / ICCPR
  - GDPR
  - National Legislation

Effectiveness?

Autonomy as a Necessary Sacrifice? (Convenience / Necessity)

Macro-Impact beyond the Affected Individual

RIoE

+ Research Questions

- How does influence of agents on the autonomy of humans manifests itself in the IoE?
- How is the type of effectiveness of influence predicated by the underlying technology or method of an agent?
- How is such influence in contrast or to the benefit of the principle of human autonomy?
- How can humans become part of the optimization process of adaptive agents and what is the impact of such adjustment?
- How are existing legal and ethical frameworks equipped to deal with such influence?

Thank you for your attention!

Maximilian Gartner

maximilian.gartner2@unibo.it

UNIBO / MRU / KUL

Main Supervisor: Prof. Giovanni Sartor

Supervisors: Prof. Anton Vedder, Prof. Mindaugas Kiškis

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Examination of Current AI Systems within the Scope of Right to Explanation and Designing Explainable AI Systems

Orhan G. Yalcin

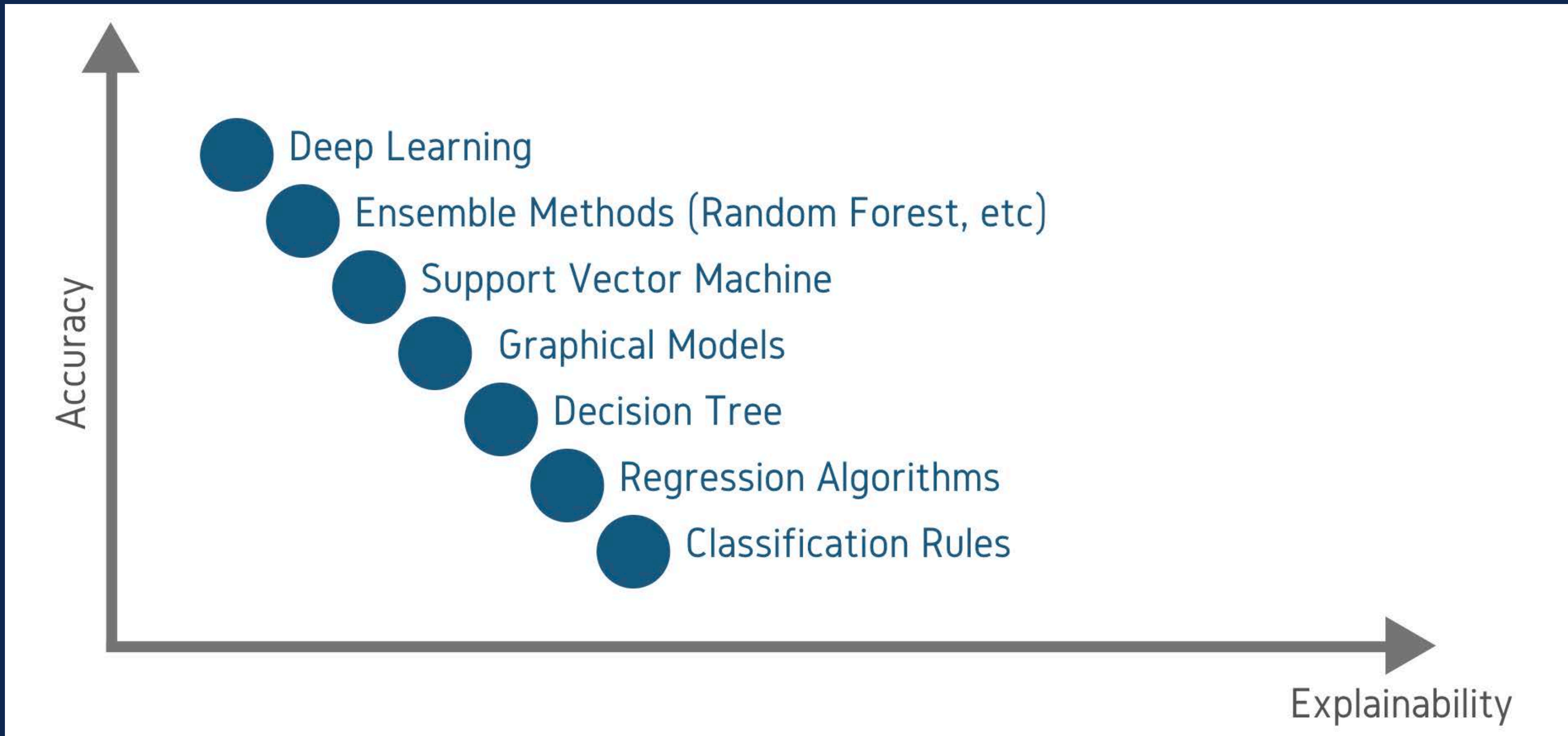
+ Right to Explanation and Explainable Artificial Intelligence

RtE →"A right to information about individual decisions made by algorithms" [1]

XAI → AI system that we can explain

- its decisions & process;
- its strength and weakness;
- how the system may behave in the future.[2]

The Problem



Accuracy-Explainability Plot of Various AI Algorithms [1] [2]

Current Developments Legal

GDPR

- Article 13-15:
  - The data subject shall have… access to … the existence of automated decision-making… ” and “… meaningful information about the logic involved

ECHR[4]

- Art 6: Right to a fair trial
  - A court decision without reasoning violates the right to a fair trial

Credit Scoring [5]

- The Fair Housing Act (FHAct)
  - According to the official interpretation of the law, An adverse action notice must provide specific reasons for denying credit

+ Current Developments Technical Research

CP	Performer	Explainable Model	Performer
Both	UC Berkeley	Deep Learning	Reflexive and Rational
	Charles River	Causal Modeling	Narrative Generation
	UCLA	Pattern Theory+	3-level Explanation
Autonomy	Oregon State	Adaptive Programs	Acceptance Testing
	PARC	Cognitive Modeling	Interactive Training
	CMU	Explainable RL (XRL)	XRL Interaction
Analytics	SRI International	Deep Learning	Show and Tell Explanation
	Raytheon BBN	Deep Learning	Argumentation and Pedagogy
	UT Dallas	Probabilistic Logic	Decision Diagrams
	Texas A&M	Mimic Learning	Interactive Visualization
	Rutgers	Model Induction	Bayesian Teaching

Accuracy-Explainability Plot of Various AI Algorithms [3]

Preliminary Approach

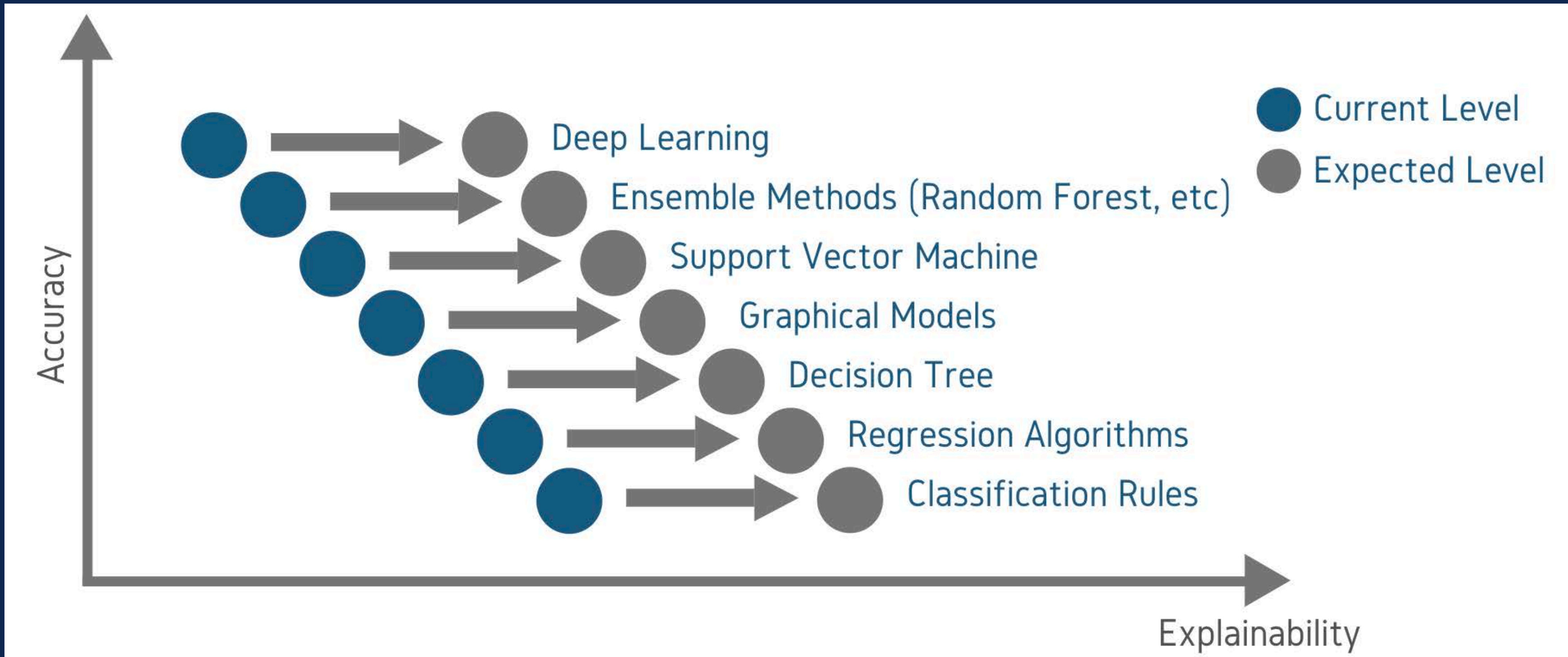
Law

- Accountability
- Transparency
- Liability
- Fundamental Rights & Freedoms

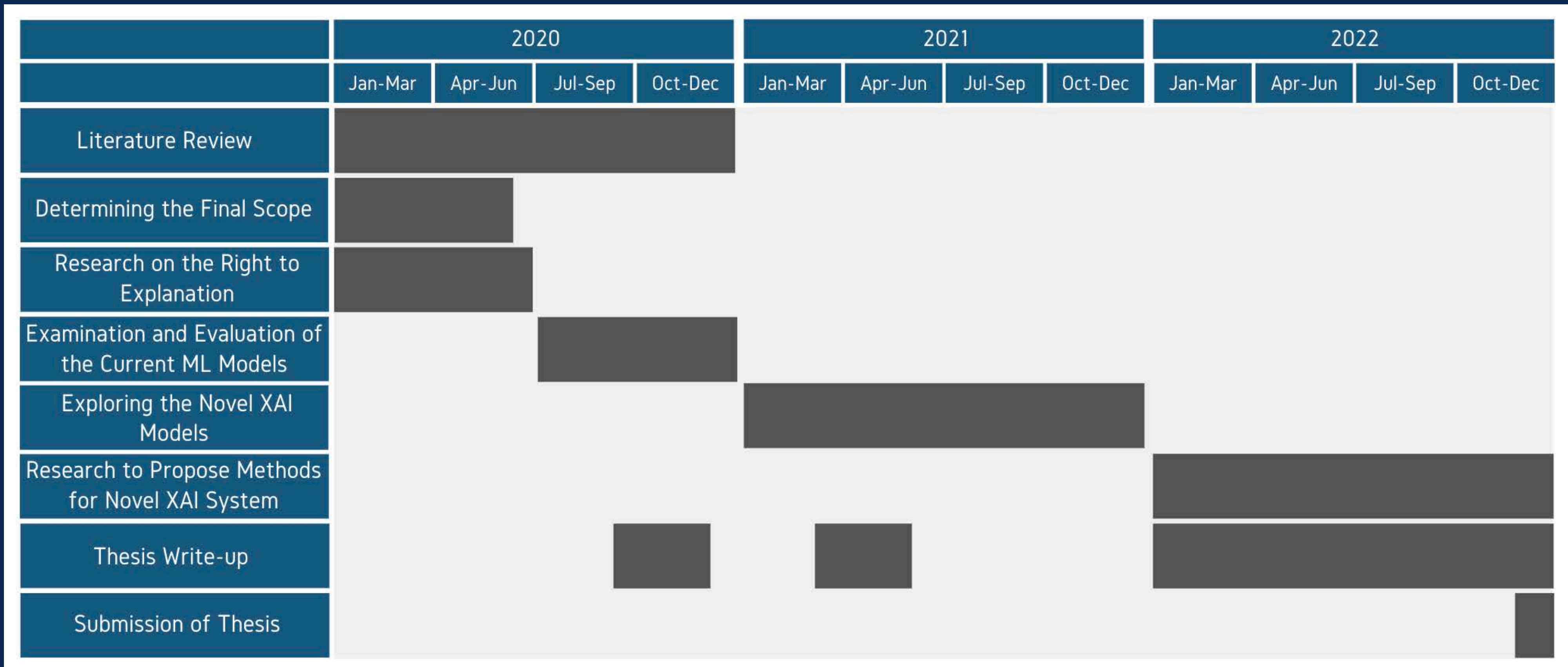
Data Science

- Algorithm Design
- Interface Design
- Interpretability and Better Control

The Main Goal of the Research



Lead Time for Implementation



THANK YOU

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

From home owners to home users: a new model of liability for a smarter and safer home

Francesca Gennari

MRU, UNIBO, UNITO, 18-19-20 November 2019

+

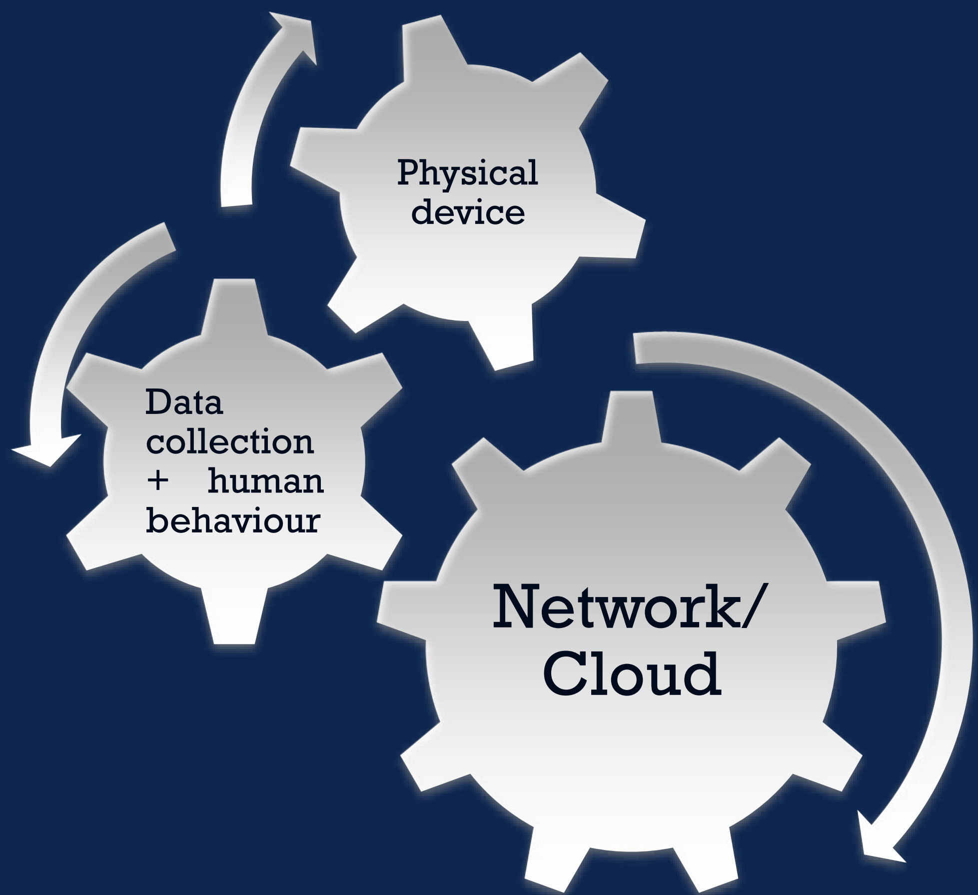
IoE: a definition

" The Internet of Everything (IoE) extends the concept of Internet of Things (IoT) to encompass not only devices but also *individuals* and *data*"

https://last-jd-rioe.eu/

RIoE
Rights of Internet of Everything

The IoEd objects in the house: scheme



The state of the art

I. EU Consumer Law

II. Data protection

III. Intellectual Property Rights

Ianus, statue, representing the IoEd objects duality, Wikimedia Commons

Rights of Internet of Everything

I. EU Consumer Law in general and Product Liability in particular

Consequences of the technological convergence phenomenon

EU Consumer Law

- IoEd objects: relatively cheap
- For the house: no professional use = Consumer Law
- Compliance with Consumer Rights Directive? Case of Amazon Dash button
- Fair access to the market? Competition issues
- New ways of fidelisation of clients. Compliance with the Unfair Practices Directive?

Product Liability Directive (PLD)

- 2016-2018: Fitness Check
- Guidance expected mid-2019 form EC (expert groups)
- Which liability apply to IoEd objects in the smart house? 3 approaches

II. Data Protection

Towards an ever more solid integration as a Consumer-User right

i. GDPR: privacy by design and by default (Art. 25 GDPR)

ii. Minimization principle (Art.5,1,c GDPR) + fairness of process (Art. 5,1,a GDPR)+ lawful consent (Art.7 GDPR)

V.

I. Huge quantity and quality of data for AI to train

II. Right not to be obliged to an entire automatized treatment trumped by exceptions Art. 22, 2 a and/or c GDPR

III. Intellectual Property Rights (IPRs)

IP

Code

- AI unit
- Self produced and applied → hazardous situations

EU IP Law

- Database, Copyright, Digital Content, Trade Secrets directives
- Liability of IoEd object?
- Authorship?

Data Protection

- IP v. property rights

The research question

The duality of the IoEd objects means that:

Keeping on legal traditions	**Moving forward**
It is necessary to use ***<u>different kinds</u>*** of liability According to the type of damage or situation	New rules through an ***<u>Integrated</u>*** ***<u>Holistic</u>*** approach (which harmonises the EU Consumer Law & IPRs)

Bibliographic, comparative and academic legal research

+

Software architecture training

+

Experiments to understand the smart house influence over consumers

Copyrights Pixhere &Pixabay

Methodology

Time schedule & expected results

1st Year

- EU Legal Background
- AI fallacies

2nd Year

- Experiments on Consumers' habits
- Thesis: answer to the Research question

3rd Year

- Write the legal model
- Internship at LIC

Wikimedia Commons

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

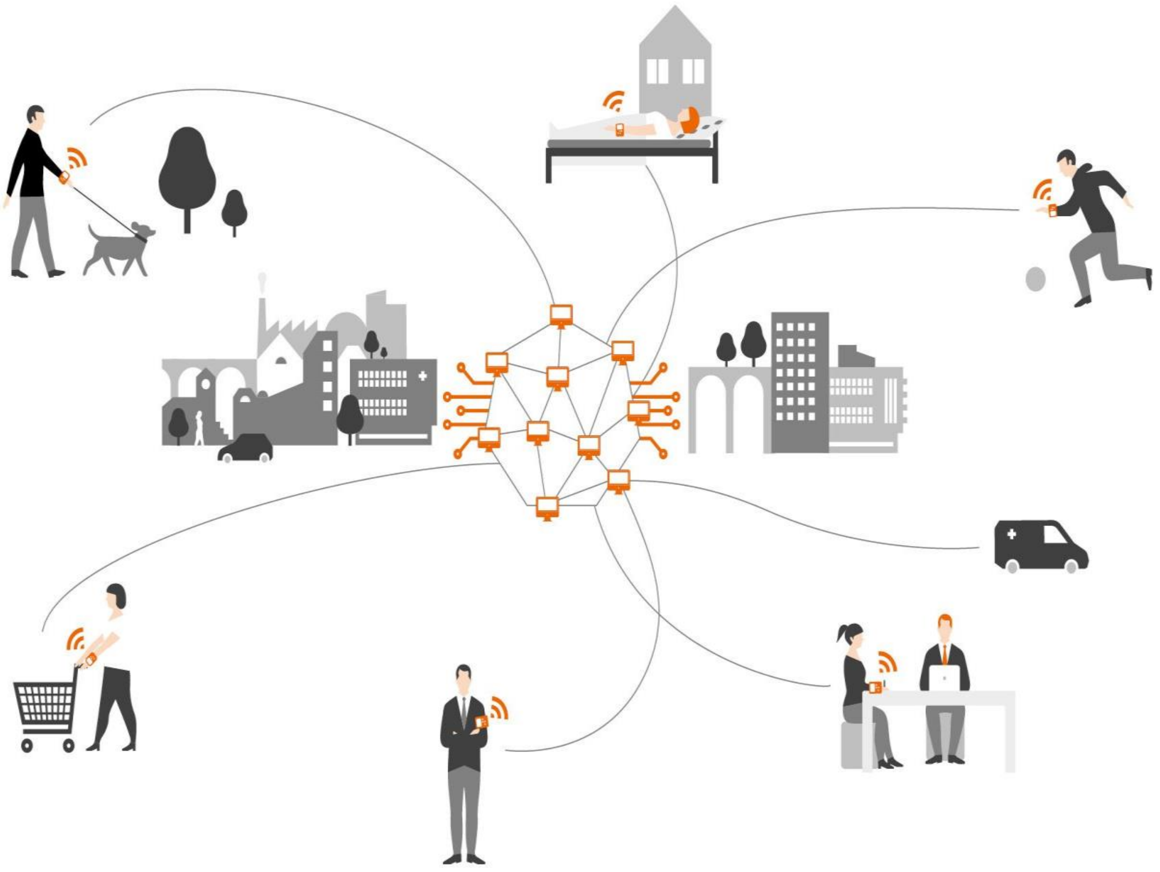
Big Data in health in IoE in emergency situations: investigating IT approaches to Big Data in healthcare

Aiste Gerybaite

Context

Rights of Internet of Everything

The Internet of Medical Things (IoMT): Driving the next generation of connected healthcare



BIG DATA, BIG PROBLEMS?

Technical issues

Will third-party hackers have easy access to all this information?

Are the newly networked medical devices secure?

How will the challenges of new data be solved, considering existing data is already difficult to process?

How will we handle the terabytes of data that may skew known patterns and trends?

What are the existing IT approaches to Big Data collection? Are they adequate? If not, can technologies such as machine learning, distributed ledgers technology, AI facilitate faster real-time processing of the collected heterogenous data?

How do you ensure scalability, integration, fault-tolerance, timeliness, consistency, heterogeneity and incompleteness, load balancing, high throughput, and privacy within such systems?

Legal and ethical issues

What constitutes an emergency from an empirical and legal perspectives? Legal qualification of an emergency may vary depending on jurisdictions;

Whilst some emergencies can be predictable what are the unpredictable emergencies?

What are the concepts of security and safety within healthcare in relation to Big Data and taking into account GDPR?

How to balance competing rights and interests of the affected parties with respect to data;

How will the law ensure ownership rights to data and the control of how patients can dynamically opt-in and opt-out from such data aggregation systems?

Liability issue in case of non-performance of the monitoring device?

How to ensure purpose limitation principle and the principle of data minimization within Big Data in healthcare?

Should health data be seen as a kind of public good that can be conscripted for some potentially publicly minded uses? Would the use of personal sensitive data be ethical and legal depending on the context where such data is used? What if in a situation where privacy is violated, it may be that, all things considered, the violation is outweighed by equitably distributed benefits in some instances?

METHODOLOGY

Mapping out and collecting the current state-of-art and identifying gaps within the current state-of the art

Systematic, multidisciplinary evaluation, and comparative analysis of state-of-art

Decision of a legal framework for Big Data in emergency situations

+ Other related information

- Supervisors: Prof. Ugo Pagallo; Prof. Monica Palmirani; Prof. Martin Theobald;
- Mobility plan: UNIBO (M8-M13-included- 6 months in total), UNITO M14-M19; UL (M20-M28-included- 9 months in total) , UNITO (M29-M37); Caretek (M38-M43 months 6 months)

Aiste Gerybaite
aiste.gerybaite2@unibo.it

Rights of Internet of Everything

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Surveillance risks in IoT applied to Smart Cities

Isadora Neroni Rezende

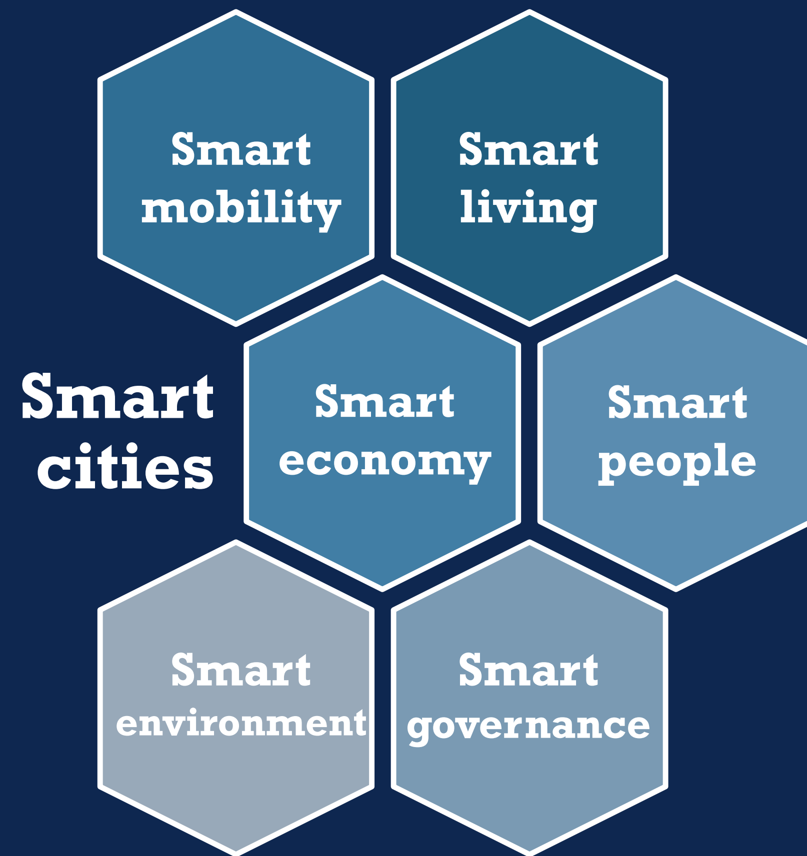
+

Setting the context:
What is a smart city?

- No generally agreed definition of the term «smart city» in academic literature

- The «city of the future»: dense presence of ICT in city services and infrastructure

- Key components of smart cities (Vienna Institute of Technology)



+

Smart Cities and the IoT

Sensing

- Fixed sensors embedded in the infrastructure
- Mobile IoT devices
- Crowdsourcing

Processing

- Storage in the cloud
- Big data analytics

Decision making

- Holistic view of the city
- Evidence-based approach

+ IoT Surveillance risks in Smart Cities

An overview

Consent-based gathering of IoT data

When or *where* is IoT data gathered?

Algorithmic processing of Big urban data

How is IoT data processed by public and private entities?

Big urban data in criminal justice

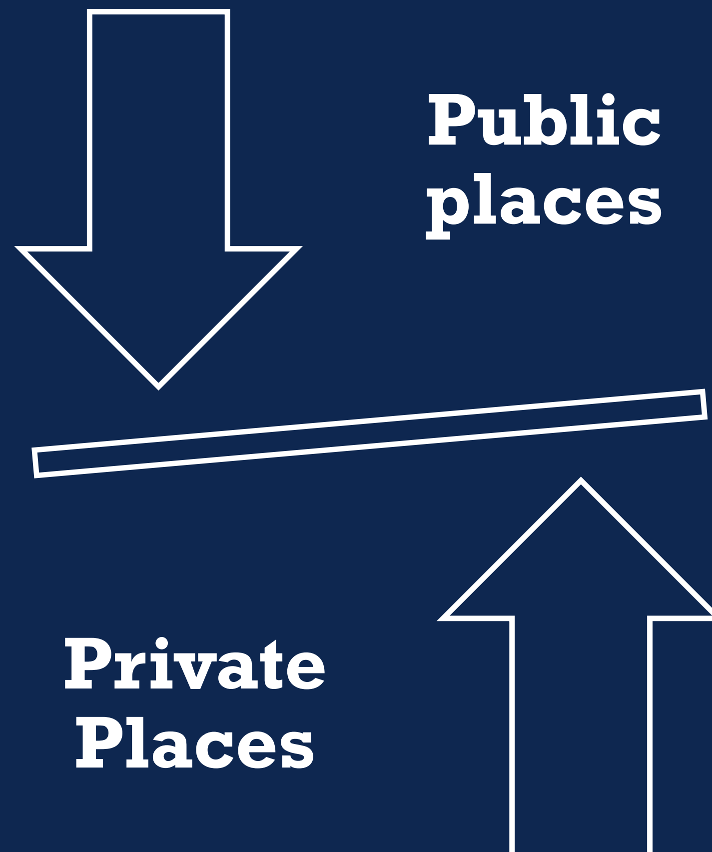
Which conditions for law enforcement access?

Public authorities' accountability

How to exercise a democratic control over public authorities' decisions?

Private-Public Places in Smart Cities

- Public places are full of privately operated sensors (e.g. roads, town squares..)
- Smartphones and other mobile devices storing personal (and sensitive) data are carried around in public streets
- IoT data may provide for insights into activities carried out in the home (e.g. smart grids)



Research Question n. 1

How can citizens effectively exercise their rights to privacy and data protection in the context of smart cities IoT-driven surveillance?

+

Research Question n.1

Objectives

A proposal for a European Regulatory Framework for Sensorveillance in Smart Cities

Trust between citizens – public authorities

⇩

Clear rules on IoT data processing in smart cities

⇩

Human-centric development of smart cities

⇨

Normative framework:

- Proportionality
- Equality
- Security
- Social justice
- Trust

+

Research Question n.2

Can individuals claim to have a *reasonable expectation of privacy* in smart cities IoT public environments?

+

Research Question n.2

Objectives

A new legal categorisation for IoT public-private environments in Smart Cities

Place-based assumptions ⇒ **Reasonable expectation of privacy**

- Major private-life intrusions occur in the home
- People can walk anonymously in public streets

- Extending privacy protections outside the home
- Flexible criterion: need to continuously adapt legal rules to new surveillance technologies

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Thank you for your attention!

Law, Science and Technology
MSCA ITN EJD n. 814177

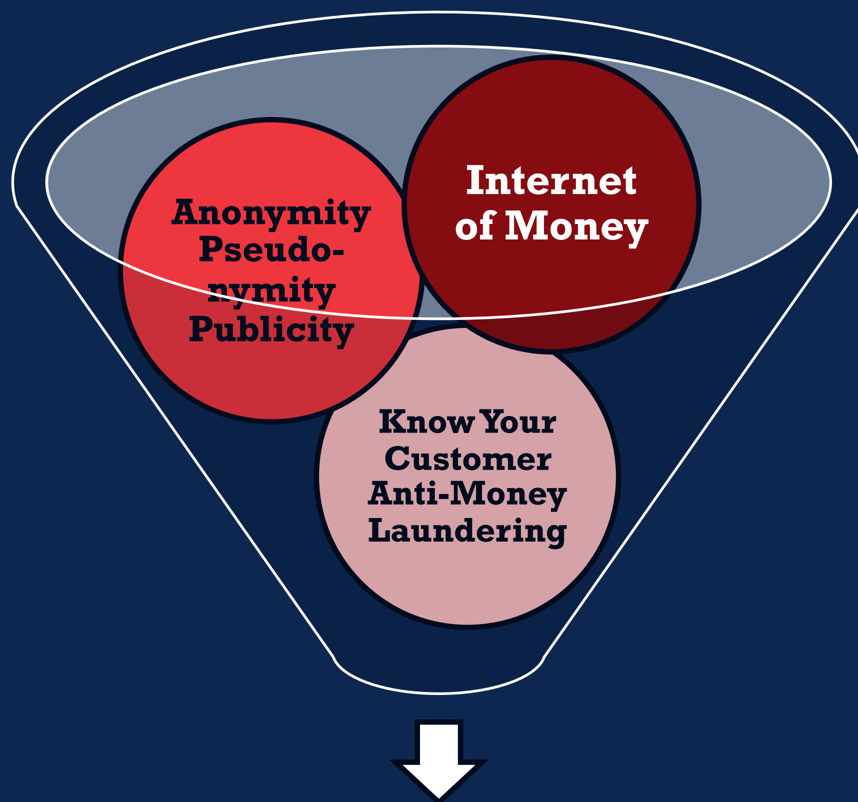
Rights of Internet of Everything

Distributed Ledger Technologies between anonymity and publicity

PhD candidate: *Nadia Pocher*

Welcome Camp – CIRSFID University of Bologna, November 2019

Research Track: Distributed Ledger Technologies between anonymity and publicity



The Internet of Money between anonymity and publicity:
legal challenges of DLTs in the crypto financial landscape

foundational state-of-the-art remarks (1/4)

the crypto-economy and the role of underlying technologies

Bitcoin

the Internet of Money

Initial Coin Offerings

Libra

Distributed Ledger Technologies:

BLOCKCHAIN and beyond

the Internet of Value

decentralization and **disintermediation**

verifiability and **transparency**

inalterability

trust and **security**

illicit use of cryptocurrencies and the race to legislative and regulatory intervention

crypto-traceability, pseudonymity and money laundering

the limits of conventional approaches to cryptocurrency regulation

foundational state-of-the-art remarks (2/4)

- the crypto-economy and the role of underlying technologies
- **illicit use of cryptocurrencies and the race to legislative and regulatory intervention**
  - **illicit purposes**
    - **transactions on the Dark Web** (Silk Road case)
    - **money laundering**
    - **terrorist financing**
  - **regulatory scrutiny and intervention**: **pro-active** vs. **reactive**
  - **FATF**: **AML/CFT framework for VCs and VAs**
    - **EU**: **5th AML Directive**
  - **approved parties**
    - **gateways to/from the traditional financial system**
    - **fiat/crypto exchanges and wallet service providers**
    - **KYC, CDD, STR, etc**
    - **active cooperation**
- crypto-traceability, pseudonymity and money laundering
- the limits of conventional approaches to cryptocurrency regulation

foundational state-of-the-art remarks (3/4)

the crypto-economy and the role of underlying technologies

illicit use of cryptocurrencies and the race to legislative and regulatory intervention

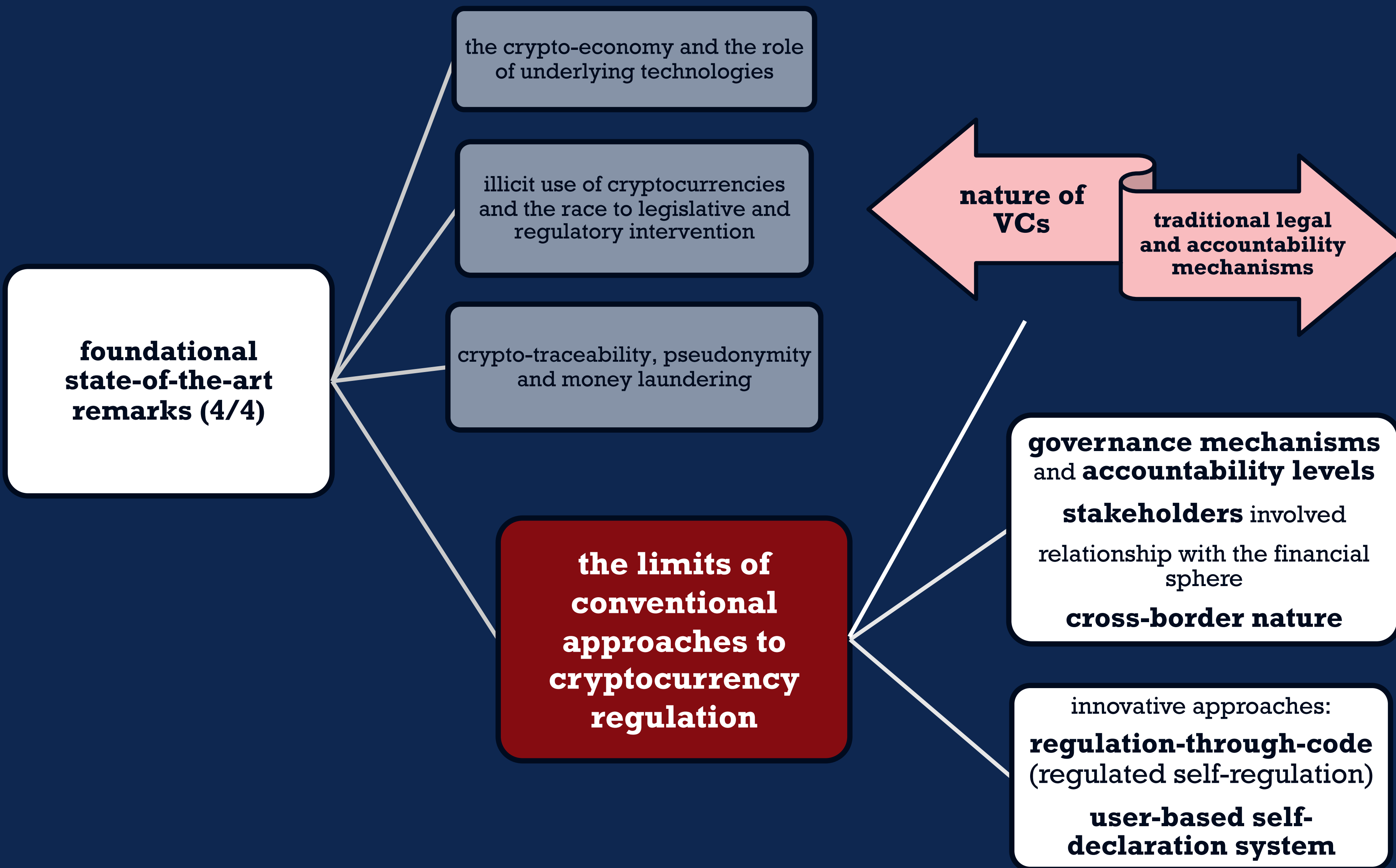
crypto-traceability, pseudonymity and money laundering

- disputed levels of **anonymity** and **privacy**
- **anonymity vs. pseudonymity**
- **intelligence/forensics techniques**
- **de-anonymization** (WSM case)

- **privacy/anonymity-enhanced cryptocurrencies**
- **mixing/tumbling**

traditional ML schemes via VCs → ← **crypto-currencies laundering**

the limits of conventional approaches to cryptocurrency regulation


foundational state-of-the-art remarks (4/4)
the crypto-economy and the role of underlying technologies
illicit use of cryptocurrencies and the race to legislative and regulatory intervention
crypto-traceability, pseudonymity and money laundering
the limits of conventional approaches to cryptocurrency regulation
nature of VCs
traditional legal and accountability mechanisms
governance mechanisms and accountability levels
stakeholders involved
relationship with the financial sphere
cross-border nature
innovative approaches:
regulation-through-code (regulated self-regulation)
user-based self-declaration system

Research Questions and Objectives

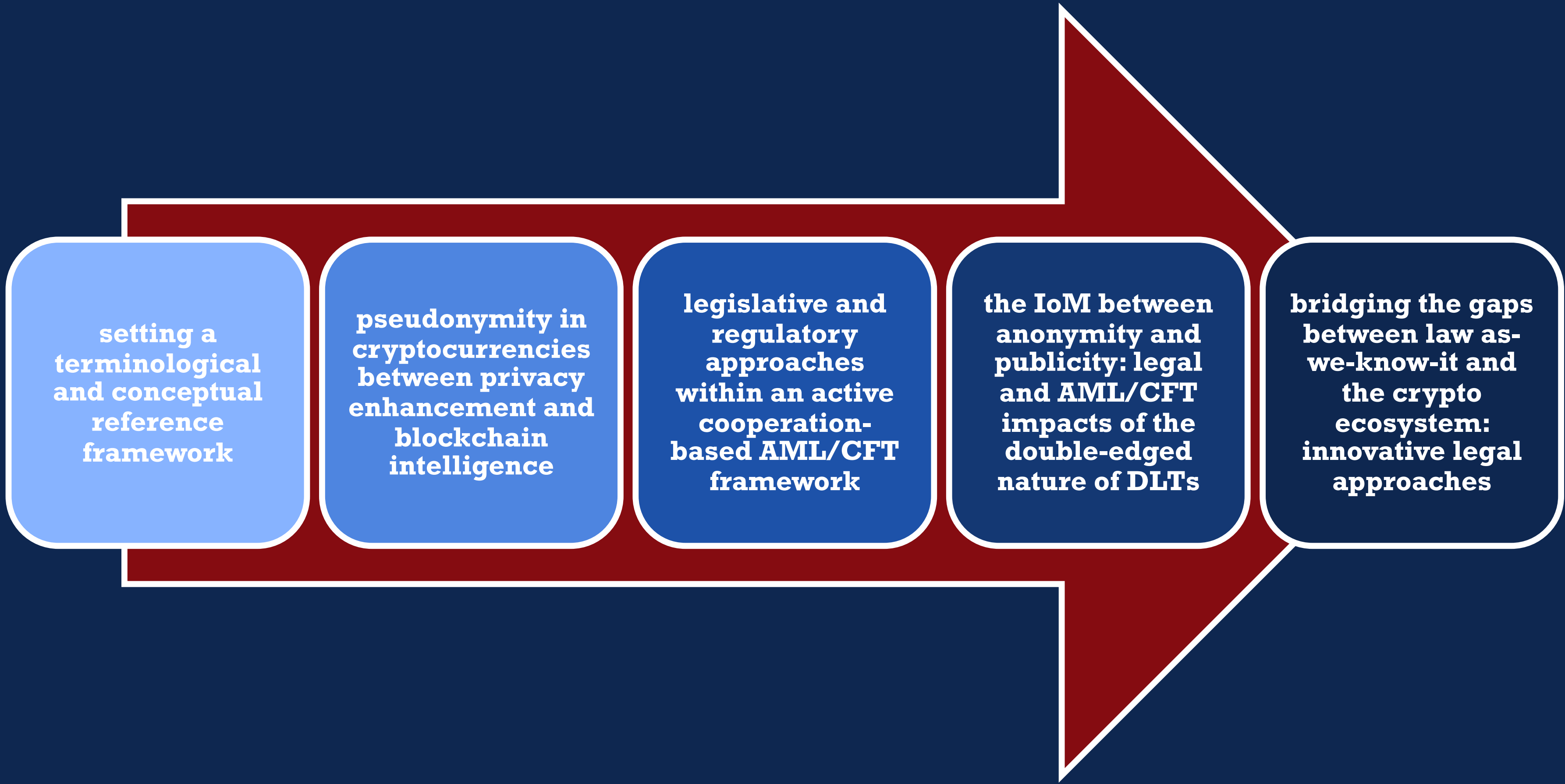
- Is any principle-wise aspect of the EU legal framework to prevent the misuse of the financial system called into question by cryptocurrencies being inherently influenced by the double-edged nature of DLTs as both transparent and privacy-oriented?

- Is there an effective level and type of legislative and regulatory intervention to ensure crypto accountability from an Anti-Money Laundering standpoint, possibly leveraging on pseudonymity?

- What innovative legal approach(es) and concepts, such as regulation-through-code, may secure AML/CFT active cooperation in the crypto landscape and mitigate anonymity and traceability concerns?

while respecting both the value of publicity and transparency in the law and the conceptual origin of the crypto economy

Description of the project: an overview



Description of the project: step 1

PRINCIPLES and VALUES behind the evolution of DLT-and BT-related IoM implementations

definitional clarity

vs.

terminological interchangeability

"cryptocurrencies", "VCs", "VAs", "blockchain", "Bitcoin blockchain", "DLTs", "non blockchain-based DLTs", "stablecoins", "altcoins", "convertible and non-convertible (i.e. open and close) VCs", "centralized vs. decentralized VCs", "VASPs"

sector-specific notions:

"TRANSPARENCY", "PRIVACY" and "PUBLICITY"

socio-economic remarks

cryptocurrencies and PRIVACY

case-study approach

(1) **meaning**

(2) **secrecy, traceability, pseudonymity**

(3) **inherent?**

(a) **privacy of identity** (user-identity privacy)

(b) **privacy of information** (of transaction data)

(c) **privacy of the total blockchain state**

privacy and anonymity are not binary, but rather a spectrum

Description of the project: step 2

PSEUDONYMITY and TRANSACTION TRACEABILITY in cryptocurrencies

(1) case-based remarks

(2) meaning(s)

(3) prospective scenarios

intelligence strategies: **blockchain and crypto-forensics**

definitively or statistically matching actual users to transactions performed by crypto-IDs

privacy/anonymity-enhanced cryptocurrencies

(e.g. Monero, Zcash, Dash)

financial flows obfuscation:

(a) mixing/tumbling

(b) zero-knowledge-based privacy

(c) user best practices

MIXING/TUMBLING

CRYPTOCURRENCY LAUNDERING

CRYPTO-TO-CRYPTO MIXERS

VIRTUAL-TO-VIRTUAL LAYERING SCHEMES

Fiat money

(regulated) exchange

Bitcoin

(unregulated) mixer

AECs (held in multiple digital wallets)

TOR

drugs

DWM

Description of the project: step 3

Legislative and regulatory approaches within the EU financial ecosystem and AML/CFT framework

AML/CFT initiatives

international guidelines, EU level, MS transposition

-> **principles**, **concepts**, **actors**, **obligations**

perceived peculiarities of VCs **from a risk perspective**

more dangerous implementations

case-based technical approach

crypto-transactions, non face-to-face business relationships, digital payments

multi-layered relationship between VCs and the concept of ML

crypto-related "obliged entities" and "approved parties": advantages and disadvantages

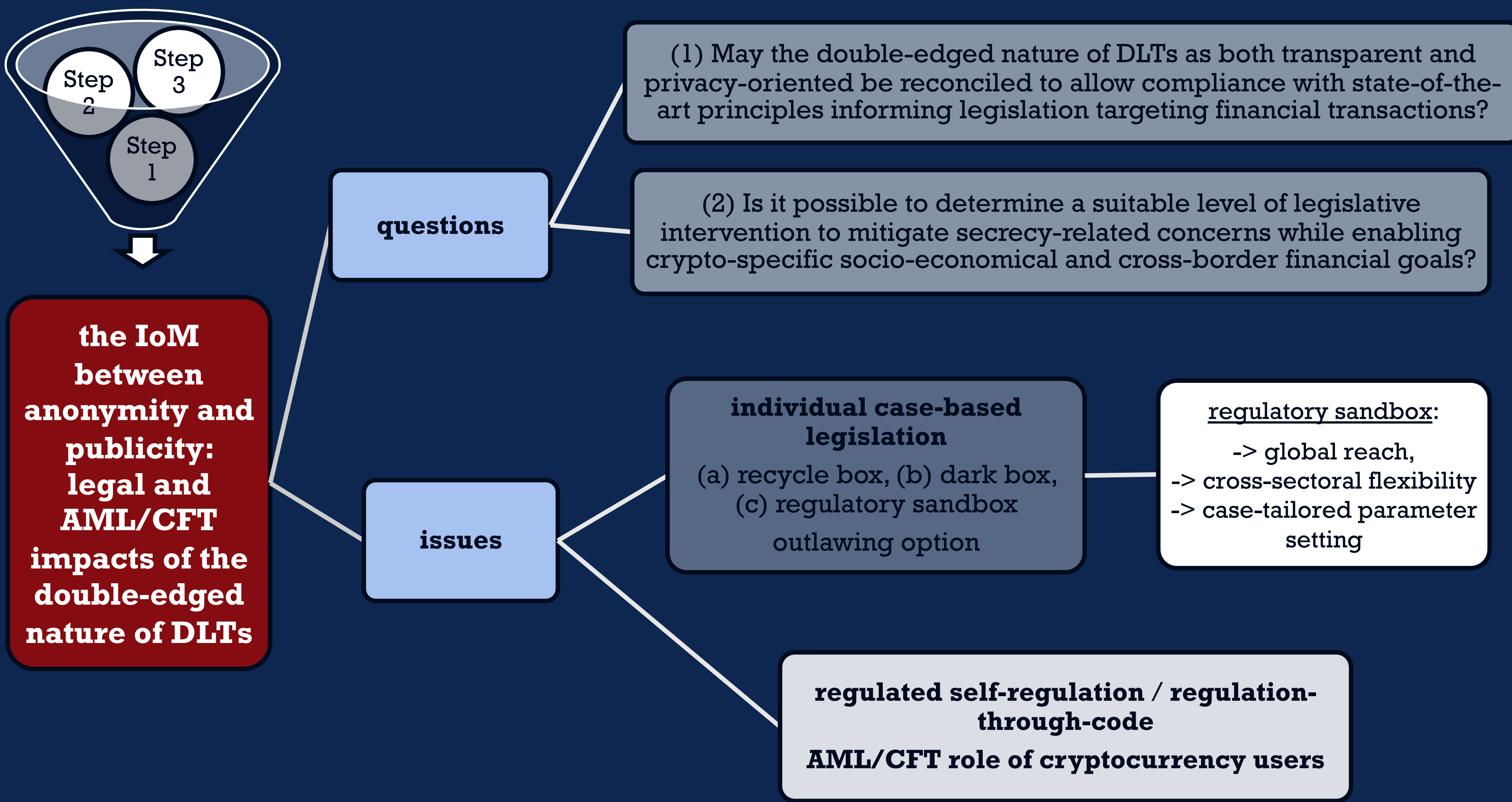
active cooperation

IoM VS. gateways and gatekeepers

diverse stakeholders

roles and accountability

Description of the project: step 4



Description of the project: step 5

clashes between cryptocurrencies and existing AML/CFT schemes and concepts

fences to be mended by innovative solutions

de iure condendo

bridging the gaps between law as-we-know-it and the crypto ecosystem

Expected results

DLT-based IoM implementations **VS.** principles informing legislative approaches to financial transactions

anonymity-enhanced ecosystems **VS.** state-of-the-art regulations

AML/KYC requirements **VS.** DLT-powered opportunities, privacy and disintermediation

disruptive technology does **not** necessarily equal disrupted law

but

BTs implement task traditionally performed by law and legal institutions and carry an **alternative vision** of the economic system

BTs transpose interactions to a virtual, potentially horizontally-structured and hyper-connected world

deep power shift among stakeholders ("**emergent technocracy**") + challenged legislative frameworks

- cross-jurisdictional cooperation and integrated approach
- regulation-by-design and regulation-through-code
- RISK of OVERFITTING: the analysis aims at a moving target

Thank you very much for your attention!

RIoE
Rights of Internet of Everything

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Big data analysis systems in IoE environments for managing privacy and digital identity: pseudonymity, deanonymization, and the right to be forgotten

PhD Candidate: Emanuela Podda
Main Supervisor: Prof. Monica Palmirani

Following the most recent informatics research, researchers have demonstrated that anonymized data ca be de-anonymized, never being total anonymous, thus the data subject can be identified.

Big Data European Legal Framework

- **Regulation (UE) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (***General Data Protection Regulation - GDPR***)

- **Regulation (EU) 2018/1807** of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (***Free Flow Data***)

- **Directive (EU) 2019/1024)** which regulates the re-use of the open data according to the principle of "*open by design and by default*": government makes its data accessible to the public by default (***Open Data***).

Regulations - have binding legal force throughout every Member State and enter into force on a set date in all the Member States

Directives - lay down certain results that must be achieved but each Member State is free to decide how to transpose directives into national laws

Open Data Directive (EU) 2019/1024)

- principle of "*open by design and by default*": government makes its data accessible to the public by default

- relying on the rules and the assumptions contained in the GDPR and in the FFD Regulations

RIoE
Rights of Internet of Everything

+

GDPR & FFD

- introduce the difference between **personal data** & **non-personal data**
- tailor a different level of protection considering that **personal data deserve an incresed protection**

Moreover…

PSEUDOANONYMISED DATA due to the fact that the data subject can be identified, they are to be treated as **personal data**

ANONYMISED DATA because the data subject cannot be identified, it is **no longer personal data**, and subsequent uses of the data are no longer regulated by the GDPR.

DATA SET OF PERSONAL AND NON PERSONAL DATA

expression of the personal identity

in the digital context

↓

data subject can be identified

↓

+

PERSONAL IDENTITY

RIoE

Rights of Internet of Everything

+

PERSONAL IDENTITY

Expression of human dignity

(*uncountable-self*)

Charter of Fundamental Rights of the European Union

Art. 1

"Human dignity is inviolable. It must be respected and protected."

In the context of *Open Data*, can the collection and re-use of such data set will be used for automated individual decision-making, including profiling, Artificial Intelligence, Machine Learning and Clustering?

Still in the context of *Open Data*, to what extent the anonymization techniques can be considered as a proportional and reasonable tool to safeguarding identity and human dignity?

+

What kind of informatic tools can be implemented or developed for protecting personal identity and privacy?

Thank you

This project has received funding from the European Union's

Horizon 2020 research & innovation programme under the
Marie Sklowdoska-Curie grant agreemant No. 814177

Rights of Internet of Everything

Law, Science and Technology
MSCA-ITN EJD n. 814177

Rights of Internet of Everything

Internet of Healthcare (Law): Privacy and Data Protection Aspects in IoE

DR. RICHARD RAK

20/11/2019

CONTENTS

1.) RESEARCH CONTEXT

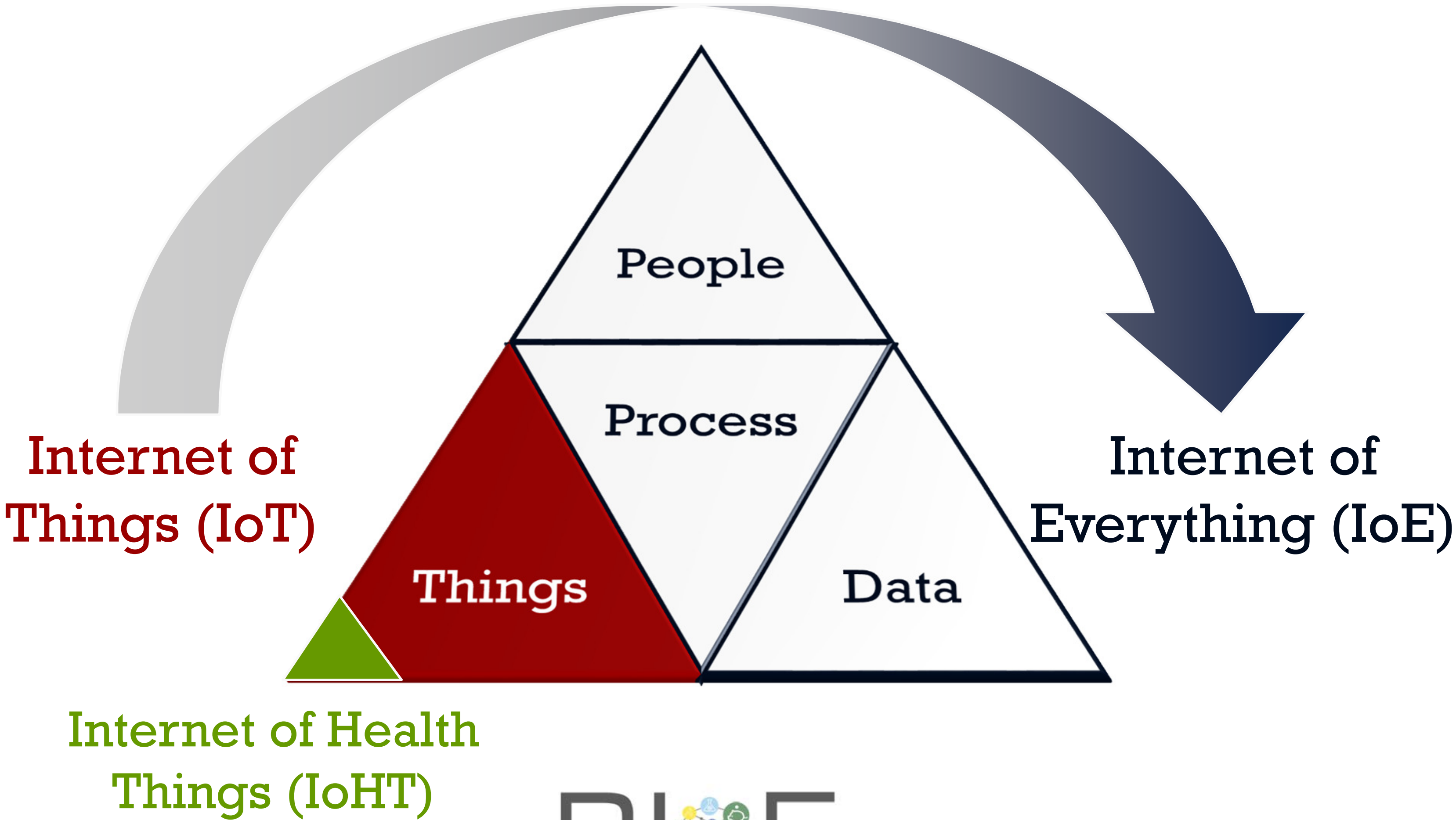
2.) RESEARCH PROBLEM

3.) RESEARCH OBJECTIVES AND QUESTIONS

4.) METHODOLOGY

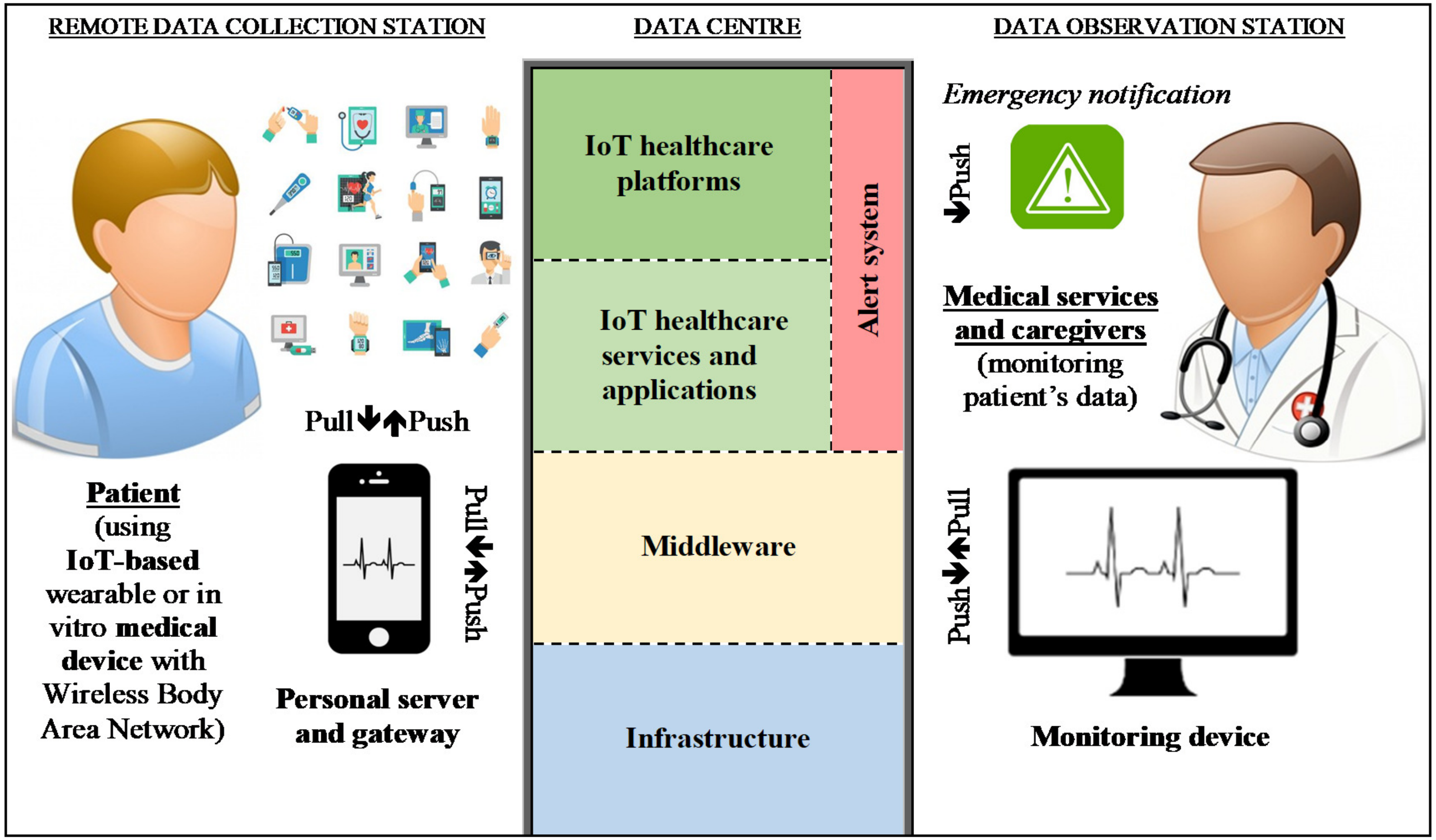
Rights of Internet of Everything

1.) RESEARCH CONTEXT



RIoE
Rights of Internet of Everything

1.) RESEARCH CONTEXT (cont.)



Generic data model for end-to-end IoHT systems

RIoE Rights of Internet of Everything

Own graphic, icons are used courtesy of public domain licenses.

2.) RESEARCH PROBLEM

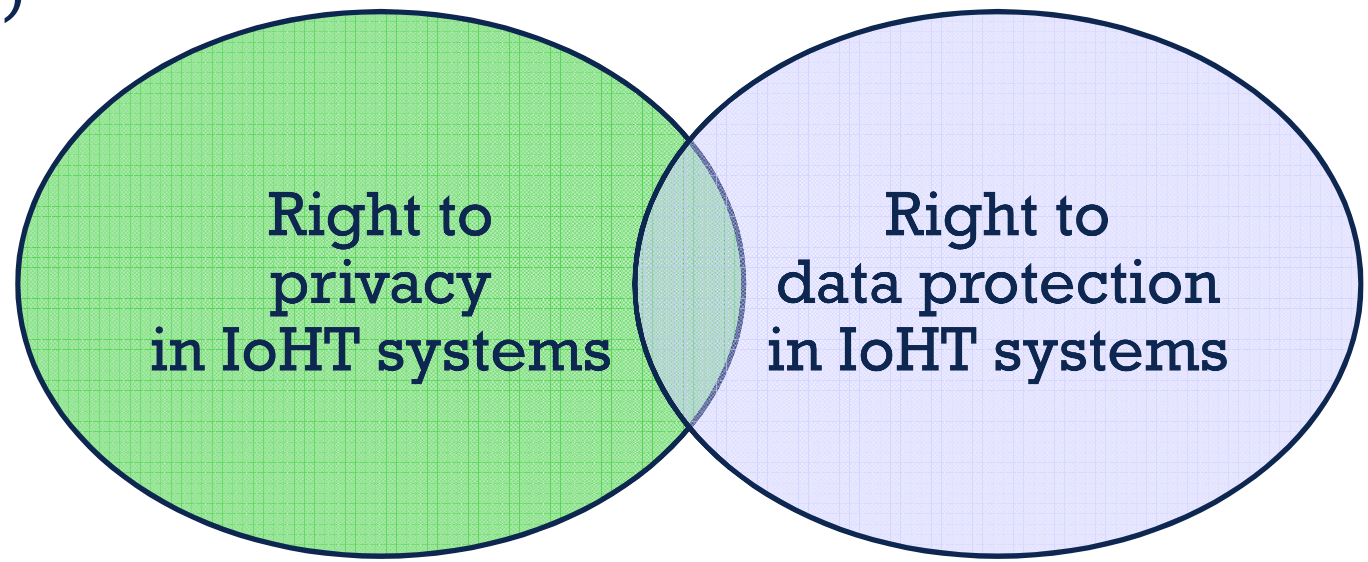
INDUSTRIAL		**PROBLEMS**
TECHNOLOGICAL	***MARKET***	
ETHICAL		
LEGAL		
DE LEGE LATA	***DE LEGE FERENDA***	
TRUST		

Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS

I.) Defining the scope of privacy and personal data in the Internet of Healthcare

I/a.)

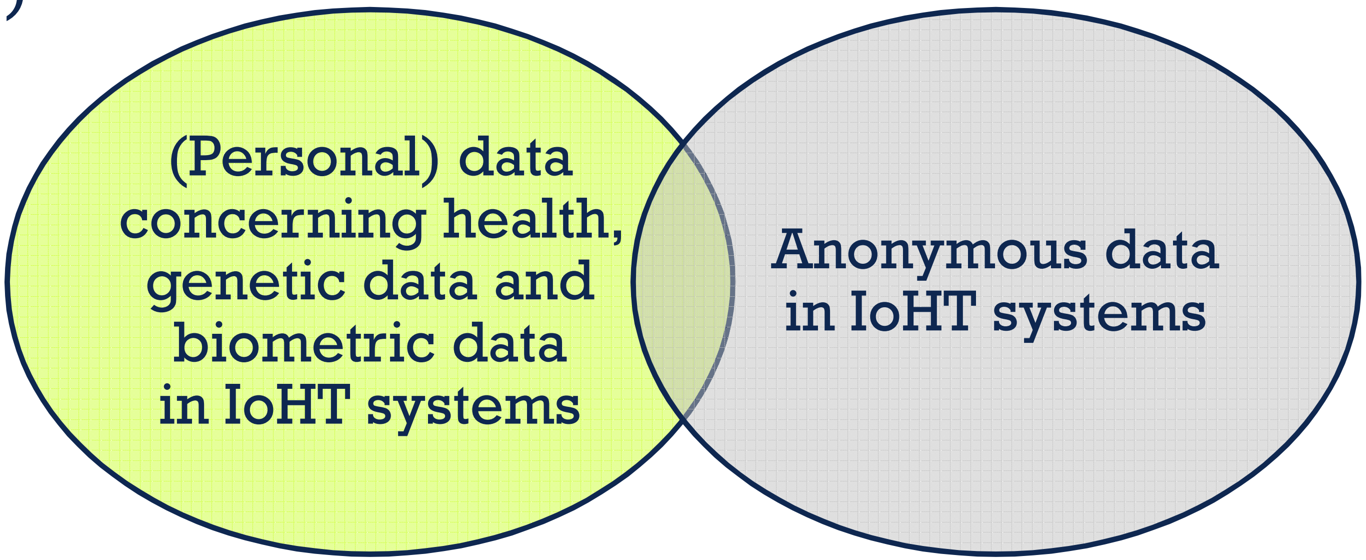


Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS

I.) Defining the scope of privacy and personal data in the Internet of Healthcare

I/b.)



Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS (cont.)

II.) Applying EU data protection law to the Internet of Healthcare

II/a.) Material and territorial scope of GDPR

II/b.) Inherent tensions between:

Prohibition of processing (personal) data concerning health, genetic data and biometric data	⟷	Provisions permitting exemptions and derogations
Consent based on GDPR	⟷	Consent based on ePrivacy proposal or Medical Devices Directive

Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS (cont.)

II.) Applying EU data protection law to the Internet of Healthcare (cont.)

II/b.) Inherent tensions between (cont.):

Privacy	⬌	Identifiability
Principles of data minimisation, purpose limitation and storage limitation	⬌	Potential benefits of big data technologies

II/c.) Rights of the data subject

II/d.) Data controller(s) and data processor(s)

Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS (cont.)

III.) Data protection by design and by default in the Internet of Healthcare

III/a.) privacy and data protection concerns resulting from data processing in IoHT systems

III/b.) technical (security, anonymity, autonomy and transparency) tools for data protection

III/c.) interplay between normative principles and privacy-enhancing technologies

III/d.) privacy and data protection-related corporate social responsibility activities

Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS (cont.)

IV.) Normative alternatives for increasing the effectiveness of data protection in the Internet of Healthcare

IV/a.) dynamic consent as a new approach to informational self-determination

IV/b.) alternative data protection framework based on risk management and end-to-end accountability

IV/c.) propertisation (i.e. the creation of a non-exclusive, flexible and extensible ownership right) in (personal) data concerning health, genetic data and biometric data

Rights of Internet of Everything

3.) RESEARCH OBJECTIVES AND QUESTIONS (cont.)

V.) Towards a European Health Data Space: facilitating the free movement of (personal) data concerning health, genetic data and biometric data in Internet of Healthcare systems and related safeguards

Policy visions, normative tools, governance and coordination models → Innovative and industry-driven European Internet of Healthcare ecosystem

?

rules relating to the free movement and protection of (personal) data concerning health, genetic data and biometric data

Rights of Internet of Everything

4.) METHODOLOGY

- primarily qualitative legal research combining theoretical and non-doctrinal (problem, policy and law reform-based) research methods
- legal analyses will focus on privacy, data protection and medical laws (primarily on a European level)
- technological issues only to the extent that they are essential for the understanding of the application of normative tools
- sources: legislative acts, case law, academic periodicals, working papers, reports and studies

Rights of Internet of Everything

4.) METHODOLOGY (cont.)

Technological tiers	Cloud computing	Infrastructure	Configurable data storage and computational resources	Management and security functions ensuring privacy and data protection
	Fog computing	Networking	Long-range communications	
		Local connectivity	Short-range communications	
	Things	Embedded intelligence	Embedded computation	
		Transducers	Sensing and actuating technologies	
		Devices	Ubiquitous medical devices	

Proposed conceptual model describing the layers of the IoE with related IoHT functionalities

Rights of Internet of Everything

4.) METHODOLOGY (cont.)

Social tiers				Management and security functions ensuring privacy and data protection
	Value (for patients, society and businesses)	People and processes	Ethical issues, policy-making, regulation and implementation	
			Healthcare management	
			IoT-assisted medical decision-making	
	Human–computer interaction	Application	IoHT platforms	
			IoHT services and applications	
	Big data and semantic technologies	Data abstraction	Computational semantics and automated processes	
		Data analytics	Data analysis, modelling and AI	
		Data ingestion	Data collection, storage and structuring	

Rights of Internet of Everything

Thank you for your attention!

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 814177.

Rights of Internet of Everything

Corresponding e-mail address:
richardrudolf.rak2@unibo.it

Law, Science and Technology
MSCA ITN EJD n. 814177

Internet of Data: Fundamental Rights in the Context of the IoE and Big Data

Stephan Varga (35th cycle)

+ Content

Early stages of research

3 parts -> 4 assumptions -> 5 preliminary research questions

The Past

The Present

The Future

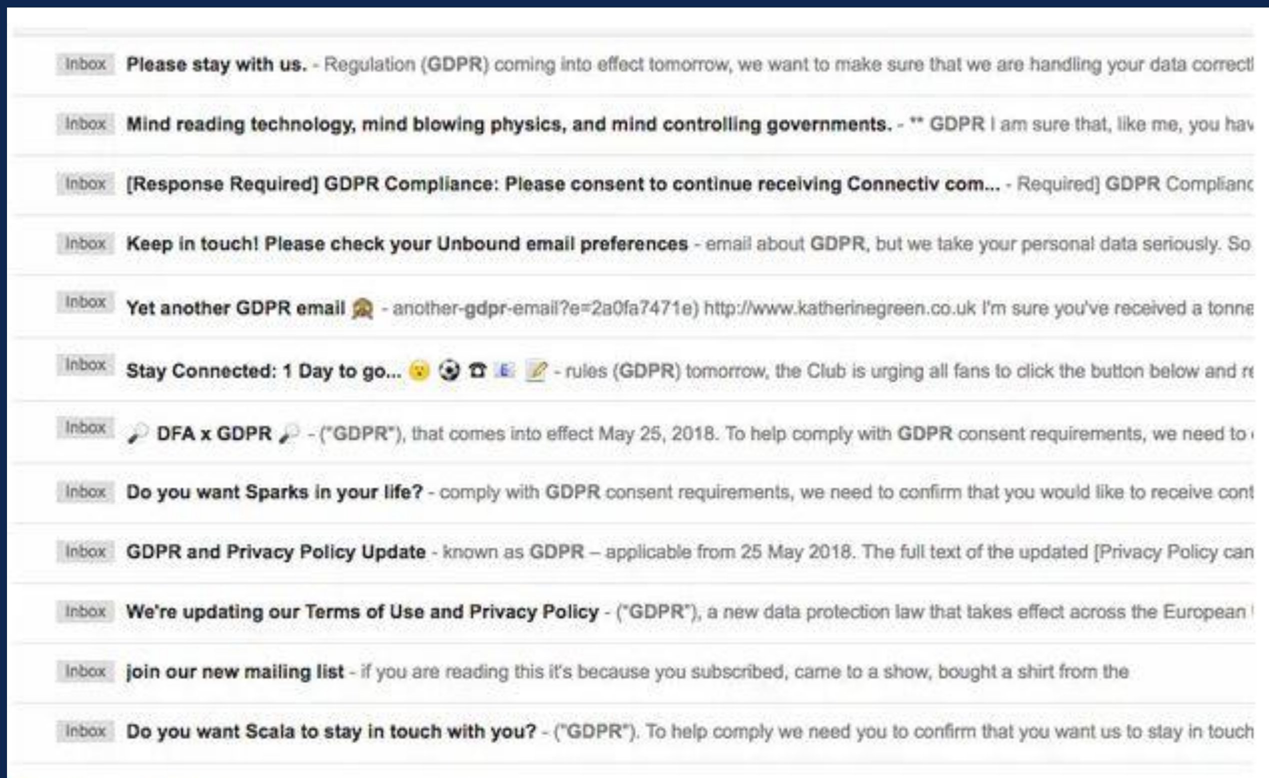
+

1. The Past

+

1. The Past

Days leading up to 25 May 2018



▲ An inbox full of GDPR emails. Photograph: Gmail

Source: https://www.theguardian.com/technology/2018/may/24/businesses-resort-to-desperate-emailing-as-gdpr-deadline-looms

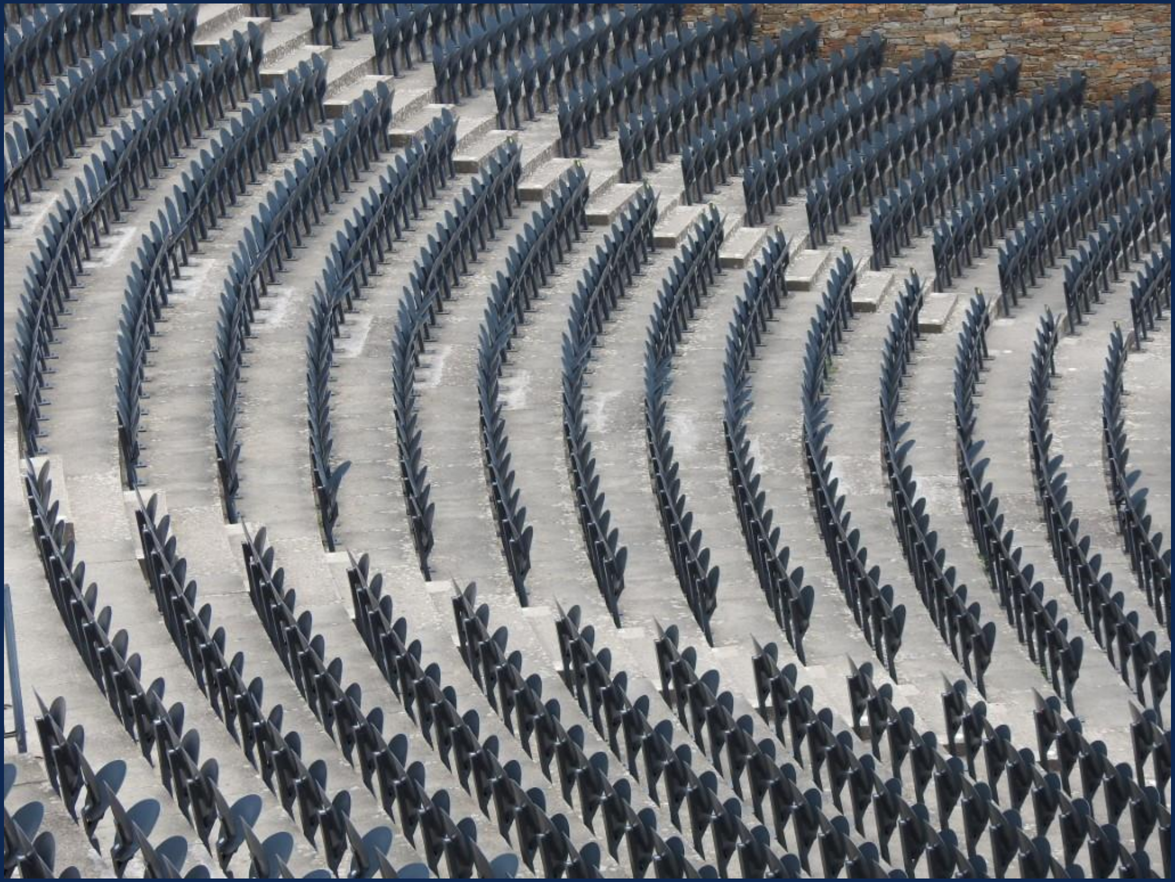
+

1. The Past

1. With the GDPR (and its fines), data protection issues continue to be important.

RIoE
Rights of Internet of Everything

+ 2. The Present



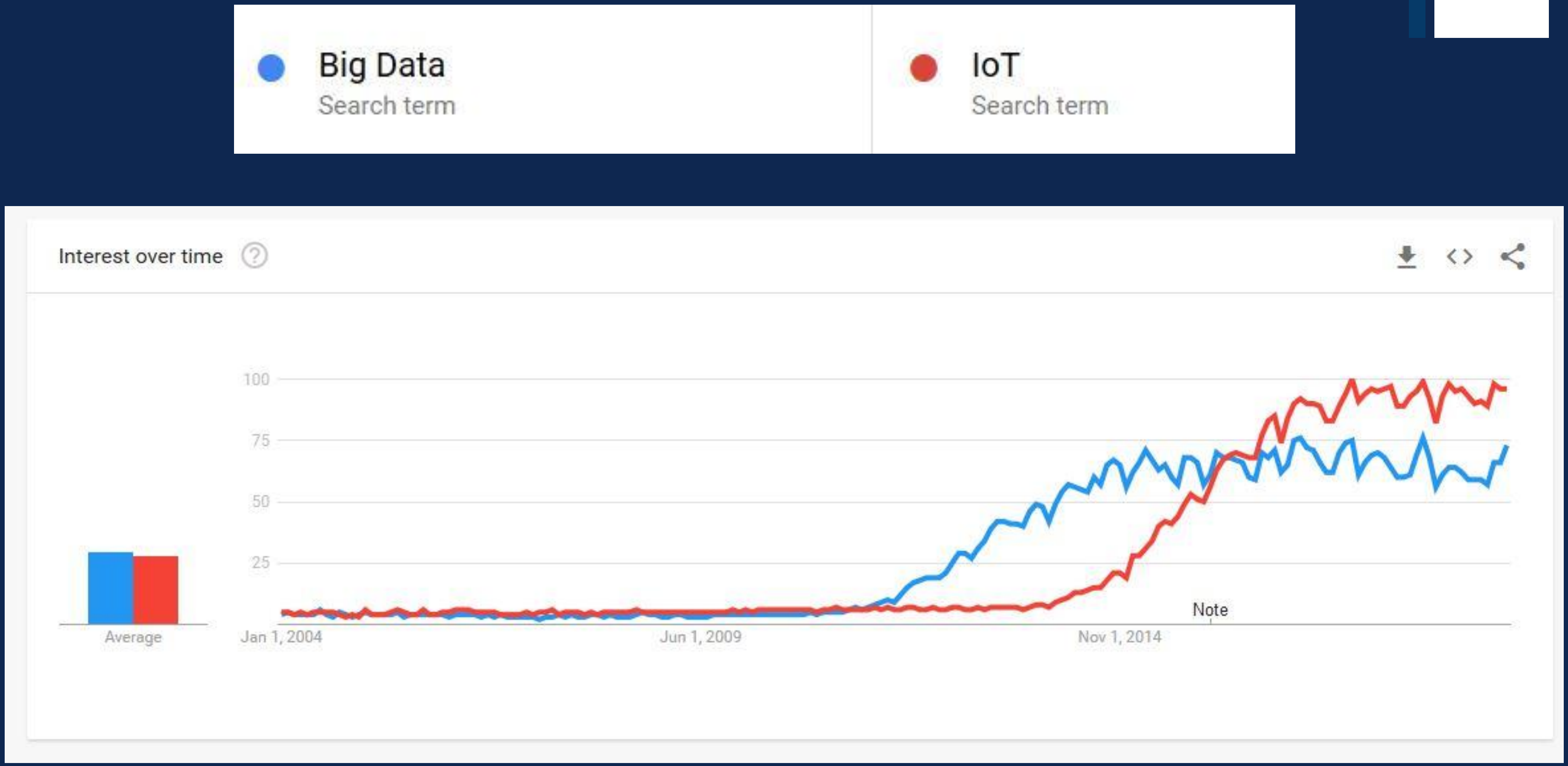
2. The Present

2a. Advancement of Technology

2b. Permanence of Law

- Stability
- Stagnancy

+ 2a. Advancement of Technology



Source: https://trends.google.com/trends/explore?date=all&q=Big%20Data,IoT&hl=en

2b. Permanence of Law

Directive 95/46/EC

- lawfulness, fairness
- purpose limitation
- data minimisation
- accuracy
- storage limitation

+ 2b. Permanence of Law

Directive 95/46/EC	Regulation (EU) 2016/679
lawfulness, fairness	lawfulness, fairness and transparency
purpose limitation	purpose limitation
data minimisation	data minimisation
accuracy	accuracy
storage limitation	storage limitation
	integrity and confidentiality
	accountability

+
2b. Permanence of Law

(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980)

Directive 95/46/EC	Regulation (EU) 2016/679
lawfulness, fairness	lawfulness, fairness and transparency
purpose limitation	purpose limitation
data minimisation	data minimisation
accuracy	accuracy
storage limitation	storage limitation
	integrity and confidentiality
	accountability

2. The Present

2a. Technology has progressed significantly in the lastest years (Big Data, …).

2b. The data protection framework has however largely stayed the same.

+
2. The Present

2a. Technology has progressed significantly in the lastest years (Big Data, …).

2b. The data protection framework has however largely stayed the same.

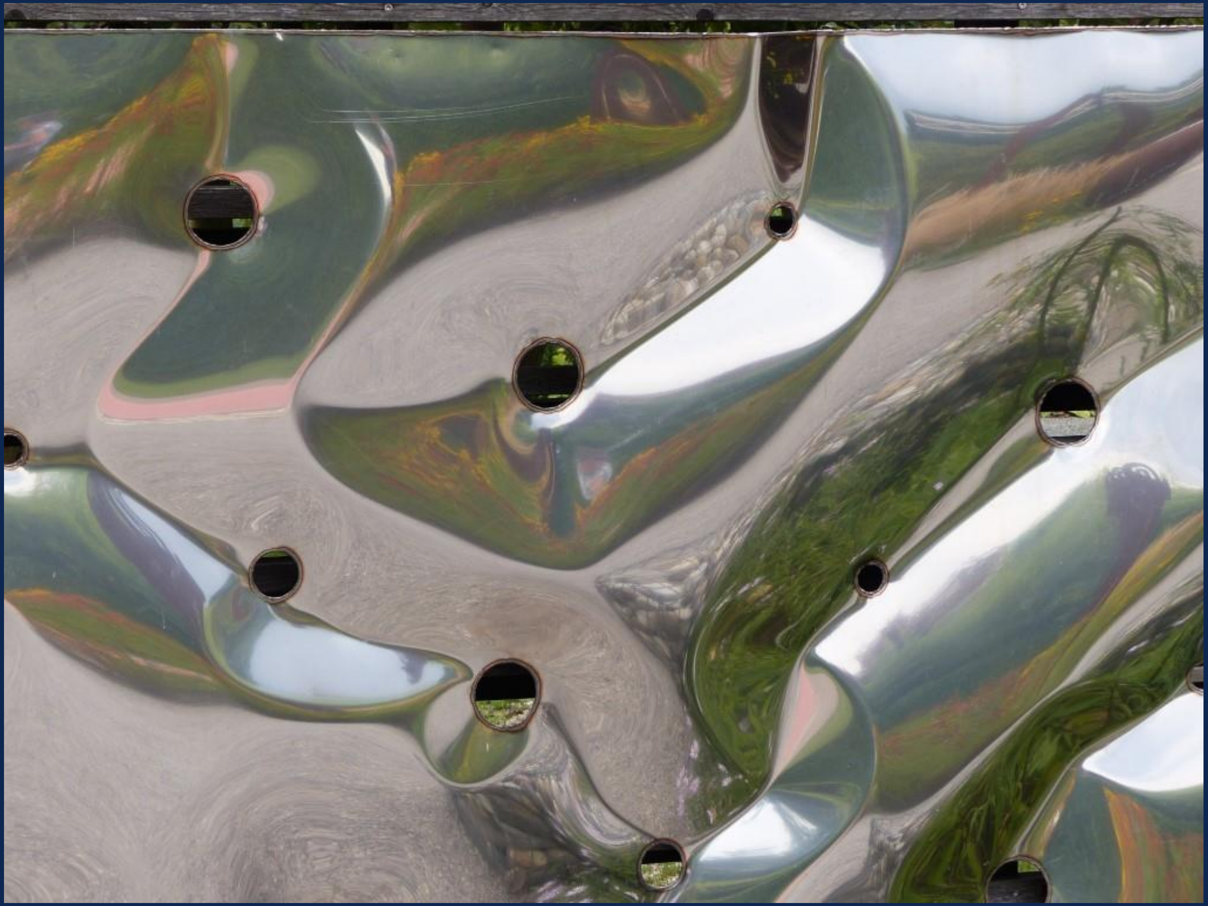
Preliminary research questions:

1 (existing literature):

Under which circumstances (if any) are Big Data Applications possible under the GDPR?

+

3. The Future



3. The Future

◆ WSJ NEWS EXCLUSIVE | TECH

Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans

Search giant is amassing health records from Ascension facilities in 21 states; patients not yet informed

Tech giants like Amazon and Apple are expanding their businesses to include electronic health records -- which contain data on diagnoses, prescriptions and other medical information. That's creating both opportunities and spurring privacy concerns. Here's what to know. Photo Composite: Heather Seidel/ The Wall Street Journal

Source: https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

3. The Future

3. There is demand for medical (big) data (health data, genetic data, …).

+

3. The Future

3. There is demand for medical (big) data (health data, genetic data, …).

Preliminary research questions:

#2: Under which circumstances (if any) are Big Data Applications possible in the healthcare sector?

#3: How does data protection align with other regulations (human subject research, …)

#4: How can data protection be balanced with other fundamental rights and the public interest?

#5: What margin of discretion do the Member States have?

Thank you

Law, Science and Technology, RIoE (Rights of Internet of Everything)

MSCA ITN EJD n. 814177

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Algorithmic accountability, perspectives on transparency in data mining processes in the platform economy

Y.A. Vogel

Proposal and Topic history

- Algorithmic accountability & censorship
- Sharing Economy
- Merger

Data Mining perspective

Kitchin's new epistomologies
Quantification of everything
Knowledge production
Understanding the applicable processes

RIoE
Rights of Internet of Everything

Data Driven Sharing Economy

Sharing/Collaborative/Platform

Why data mining is key

Understanding the different processes individually

Innovation–co-evolution–complexity

+

From the Data Driven Sharing Economy to Algorithmic Accountability

preliminary research question:

What would a normative framework for algorithmic accountability in the data mining- platform economy require to remedy GDPR shortcomings?

How does one understand Algorithmic Accountability and its components?

Why transparency may not be the best solution

Why article 22 does not relieve all issues by matter of scope

What are its shortcomings?

Kitchin's idea of knowledge production

Random Group Profiling

Random group pattern finding

Personal data not necessarily a result nor outcome

Transparency mechanisms focus on the individual

+

Goals:

Identify the shortcomings in Algorithmic Accountabilty as Data Protection framework in relation to the processes of the data driven sharing economy.

Understand how transparency works in regard to this framework.

Creating a normative framework on how to improve this framework of algorithmic accountabilty based on the identified problems.

Thank you for your attention!

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

Research Topic (position n.13) : Risk Analysis and Regulatory Compliance of Distributed Ledger Technologies (DLT) for Transaction and Management of Securities

Title : On the Optimized Utilization of Smart Contracts from the Perspective of Legal Representation and Legal Reasoning

Yu Liuwen

Content

Rights of Internet of Everything

1.Introduction

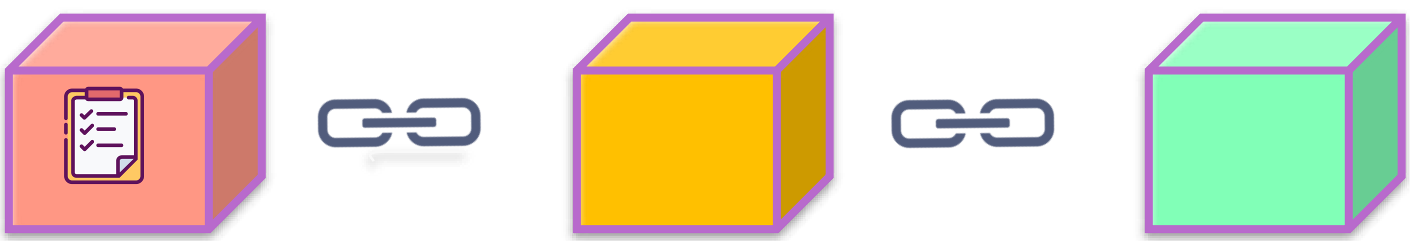
Smart Contract

Traditional Contract（ written in natural language ）

They are completely digital；In fact a smart contract is actually a tiny computer program that is stored inside a blockchain.

Smart Contracts（ written in lines of code ）

Problems Arise！



1.Introduction

Translation Errors

↓

Influence the legal effect of smart contract

↓

Cause an unreasonable and unfair result on the parties involved in the contracts.

Due to the complexity, contradictoriness, and constantly changing conditions of the law, the analysis, representation, and inference of legal knowledge within smart contracts need more advanced and flexible methods

RIoE
Rights of Internet of Everything

1.Introduction

- Legal representation → Logic-based Language
  - Defeasible logic
  - Deontic logic
  - . . .
- Legal reasoning → Formal Argumentation
  - Abstract Argumentation
  - Structured Argumentation

RIoE

Rights of Internet of Everything

2.State of The Art

(1).Logic–based Language

a) Defeasible Logic (DL) is a rule-based skeptical approach to non-monotonic reasoning due to its flexibility (Nute2001).

b) Deontic logic with deontic operators (e.g. permissions, obligations, and violation) (Governatori and Rotolo 2006).

c) Contrary-to-duty obligations (CTD) is a conditional obligation that arises when another obligation has been violated (Carmo and Jones 2002)

d) Various novel and powerful implementations

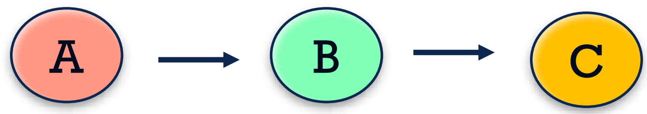
RIoE

Rights of Internet of Everything

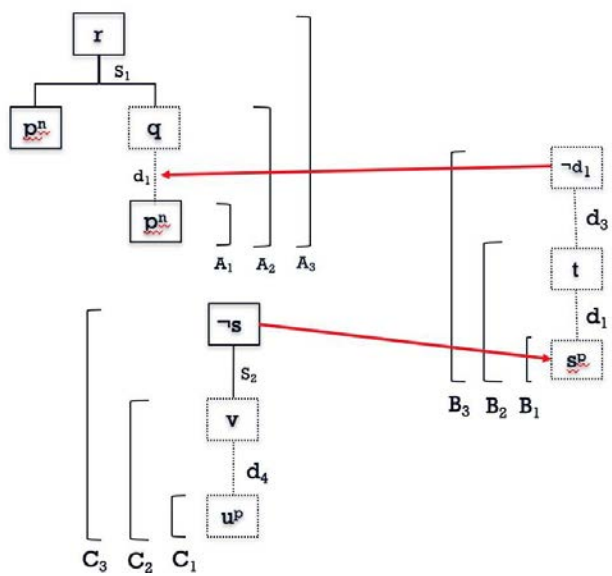
2.State of The Art

(2) Formal Argumentation

Dung's abstract argumentation framework (AF) (Dung.P.M. 1995)



ASPIC^{+} (Henry.P 2014)



2.State of The Art

(2) Formal Argumentation

AF （limited ability of expression）

Bipolar abstract argumentation framework(Cayrol 2009)

Deductive , Necessary and Evidential support…

Rights of Internet of Everything

2.State of The Art

In an argumentation framework, one of the key problems is characterizing the dynamic aspect of it.

Baumann proposed a similar approach(Baumann 2012) that is based on Lifschitz and Turner‘s splitting results for logic programs(Lifschitz1994).
Beishui proposed a division-based method to cope with the dynamics of the argumentation system(Beishui.L.2014).

These researches are oriented to abstract argumentation frameworks, but there is little attention to an important relation between structured arguments, i.e., sub-argument relation.

Rights of Internet of Everything

3.Research Question

(1) to what extent it is possible to establish and formalize correspondences between traditional legal contracts and smart contracts, able to incorporate different legal interpretations of the terms included in the former?

(2) On argumentation perspective, a) how to define sub-argument and argumentation framework with sub-argument(AFwS), if there are additional constraints? b)how to calculate the semantics of AFwS efficiently? c)What are the principles governing the semantics of AFwS?

(3) how it is possible to include in the smart contracts self-adjustment mechanisms for fast adapting them to new legal interpretations?

Rights of Internet of Everything

3.Method

(1).Investigate proper and novel representations of legal expressions in smart contracts; Starting points for this investigation will be (Governatori, G. and Idelberger, F. and Milosevic, Z. and Riveret, R. and Sartor, G. and Xu, X. 2018) and (Robaldo, L. and Sun, X. 2017);

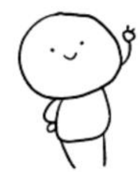
(2).In the aspect of argumentation, I will investigate the definition of sub-argument and AFwS from both structured and abstract perspectives. Besides, I need to do more systematic study and comparison of semantic. Starting points for this investigation will be(Bin.W and Henry. P.2017) and (Leon. V.D.T and Srdjan.V.2018;

(3)Investigate a multi-agent system incorporating the software agents with sensing, inferring, learning, decision-making and social abilities.Starting points for this investigation will be (Batsakis, S. and Baryannis, G. and Governatori, G. and Tachmazidis, I. and Antoniou, G. JURIX2018).

Bibliography

[1]https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf
[2] DTCC, Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape, White Paper, 2016.
[3] Nute,D. Defeasible logic: Theory, Implementation and Applications. In Proceedings of the 14th International Conference on Applications of Prolog. INAP 2001. Springer, Berlin,Tokyo, Japan, pp.151–169. 2001.
[4] Governatori, G., Rotolo, A.: Logic of Violations: A Gentzen System for Reasoning with Contrary-To-Duty Obligations. Australasian Journal of Logic 4, pp.193–215 2006.
[5] Carmo, J., Jones, A.J.: Deontic Logic and Contrary-to-Duties. In: Gabbay, D.,Guenthner, F. (eds.) Handbook of Philosophical Logic, pp. 265-343. SpringerNetherlands, Dordrecht, 2002.
[6] C.Pereira, B.Liao, A. Malerba, A Rotodo, Andrea G. B.Tettamanzi, L. van der Torre, and S.Villata. Handling norms in multi-agent system by means of formal argumentation. IFCoLog Journal of Logic and its Applications, 4(9),2017.
[7] Dung, P.M.: On the Acceptability of Arguments and its Fundamental Role in Nonmonotonic Reasoning, Logic Programming and n-Person Games. Artificial Intelligence 77(2), 321–358, 1995.
[8] Sanjay Modgil and Henry Prakken. The ASPIC+ framework for structured argumentation: a tutorial. Argument & Computation, 5(1):31–62, 2014.
[9] C.Cayrol, Marie-Christine Lagasquie Schiex. Bipolar abstract argumentation systems. Argumentation in Artificial Intelligence, pages 65–84. 2009.
[10] G. Boella, D.Gabbay, L.van der Torre, and S.Villata. Support in abstract argumentation. In Proc. of COMMA 2010, pages 111–122, Amsterdam, The Netherlands, 2010.
[11]F.Nouioua. AFs with necessities: Further semantics and labelling characterization. In Weiru Liu, V.S. Subrahmanian, and Jef Wijsen, editors, Proc. SUM'13, volume 8078 of LNCS, pages 120–133. 2013.
[12]N.Oren and T.J. Norman. Semantics for evidence-based argumentation. In Proc. COMMA '08, volume 172 of Frontiers in Artificial Intelligence and Applications, pages 276– 284. IOS Press, 2008.

[13]P. Baroni, M. Giacomin, B. Liao, On topology-related properties of abstract argumentation semantics. a correction and extension to dynamics of argumentation systems: A division-based method, Artifficial Intelligence 212, pp.104-115. 2014.
[14]R. Baumann, G. Brewka, W. Dvork, S.Woltran, Parameterized splitting:A simple modification-based approach, in: Correct Reasoning, Springer, pp. 57-71. 2012.
[15]V. Lifschitz, H. Turner, Splitting a logic program, in: Principles of Knowledge Representation, MIT Press, pp. 23-37. 1994.
[16]Deters R. How to Detect and Contain Suspicious Transactions in Distributed Ledgers [A]. Smart Block 2018 [C].Germany:Springer, pp.149 ~ 158.2018.
[17]Governatori, G. and Idelberger, F. and Milosevic, Z. and Riveret, R. and Sartor, G. and Xu, X. On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artificial Intelligence and Law, 26(4), 2018.
[18]Robaldo, L. and Sun, X.: Reified Input/Output logic: Combining Input/Output logic and Reification to represent norms coming from existing legislation, The Journal of Logic and Computation, Vol. 27, Issue 8.2017.
[19]https://www.oasis-open.org/committees/legalruleml/
[20]B.Wei and H. Prakken. Defining the structure of arguments with AI models of argumentation. In F. Bex, F. Grasso, N. Green, F. Paglieri, and C. Reed, editors, Argument Technologies: Theory, Analysis, and Applications, pages 1–22. College Publications, London, 2017.
[21]L.van der Torre and S.Vesic. The principle-based approach to abstract argumentation. In Pietro Baroni, Dov Gabbay, Massimiliano Giacomin, and Leendert van der Torre, editors, The Handbook of Formal Argumentation. College Publications, 2018.
[22]Batsakis, S. and Baryannis, G. and Governatori, G. and Tachmazidis, I. and Antoniou, G.: Legal Representation and Reasoning in Practice: A Critical Comparison. Proc. of the 31st International Conference on Legal Knowledge and Information Systems (JURIX2018).



Rights of Internet of Everything

Law, Science and Technology
MSCA ITN EJD n. 814177

Rights of Internet of Everything

The use of Decentralized and Semantic Web Technologies for Personal Data Protection and Interoperability

Mirko Zichichi

20/11/2019

Outline

- Introduction
  - Personal Data
  - Problem
- State of the Art
  - GDPR
  - Semantic Web
  - Solid *by Tim Berners Lee*
  - Distributed Ledger Technologies (DLTs)
- Objectives
- Hypoteses
- Research Questions
- Methodology
- Research Plan

+ Personal Data

- Any piece of information that can **identify** or be identifiable to a natural person

- Generated by the interaction of a user with a software or a hardware in form of:

  numbers, characters, symbols, images, sounds, electromagnetic waves, bits, etc. [1]

- Collected to improve of **safety and security** in citizens surveillance

- But also for a "not so new" **data-driven economy**

+ Problem

Abuse of personal information (Cambridge Analytica 2018)

- Personal data is sometimes **concentrated in few points** and transacted in **opaque transfers** without the individual's control or even knowledge

- Data is stored differently through several **data silos**, maintained by entities to which it is convenient **hampering** data exchange and its economical exploitation

- Individuals are not capable of determining the **fate** of their personal data, whereas they may be good willing to offer it for the **social good** (e.g. better policy making, research) or they want to make direct **profit** from it.

General Data Protection Regulation (GDPR)

It [2] has empowered data privacy of citizens by radically changing operations carried out by data providers

Requires data providers to **release** to their users the complete dataset they collected on them, when requested.

- **No standards** for this requests
- There is the tendency to **hinder the progress** of these

\+ GDPR **data portability** provides the right to have data directly transferred from one data provider to another making a step towards user-centric platforms of interrelated services

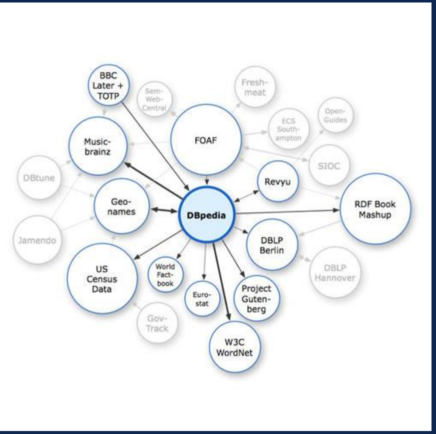
- **Interoperability** [3]

Semantic Web

Extension of the World Wide Web through standards by the World Wide Web Consortium (W3C)

Brings structure to the **meaningful contents** of the Web by promoting common data formats and exchange protocols [4] e.g.:

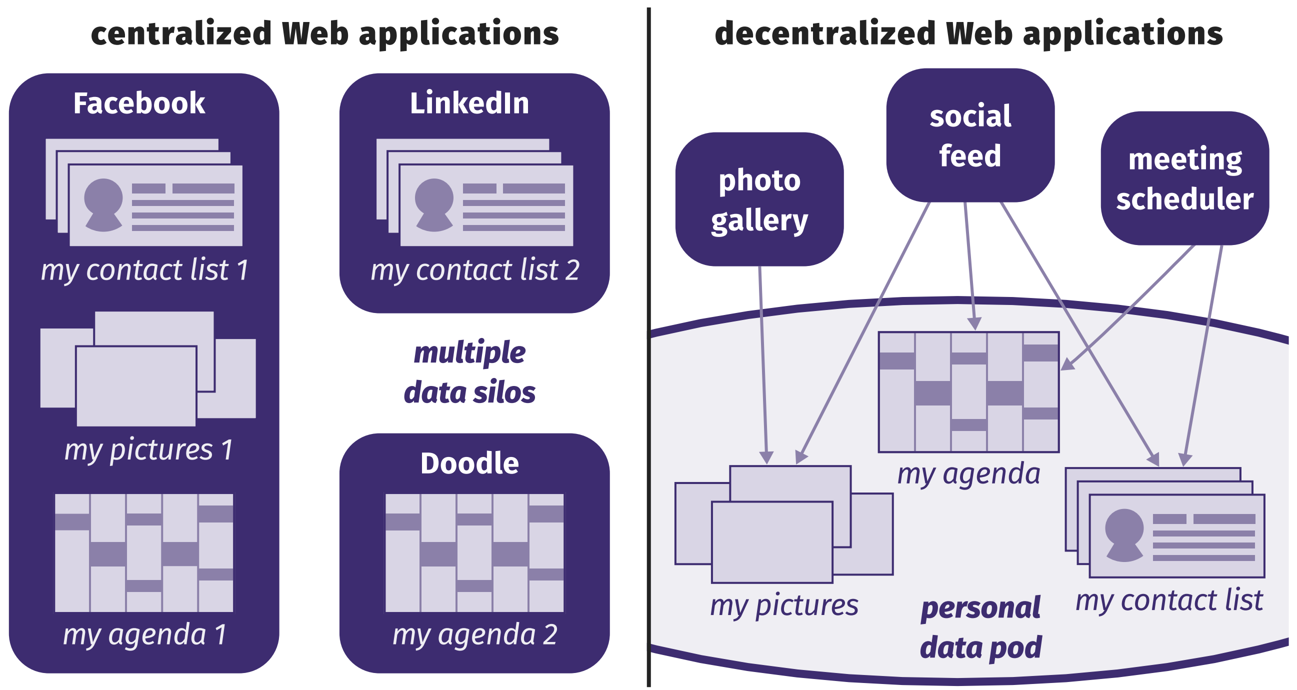
- **RDF** (Resource Description Framework) [5]
- **OWL** (Web Ontology Language) [6]



\+ **Linked Data**: data published in a structured manner, in such a way that information can be found, gathered, classified, and enriched using annotation and query languages.

SOLID (Tim Berners Lee's project)

Involves the use of distributed technologies and Semantic Web integration in social networks. Born with the purpose of giving users their data sovereignty, letting them choose where their data resides and who is allowed to access and reuse it [7]



https://rubenverborgh.github.io/Solid-DeSemWeb-2018/

Distributed Ledger Technologies

ethereum IOTA

- A software infrastructure maintained by a p2p network, where the network participants must reach a **consensus** on the states of transactions submitted to the distributed ledger
- A DLT brings trust when there are several parties that concur in handling some data in a **trustless** manner
- The Ethereum **Smart Contract** [8] is a new concept of contract that brought a second blockchain revolution, removing the technology bond with finance and providing a new paradigm where **unmodifiable instructions** are executed in an **unambiguous manner** during a transaction between two parts.

https://www.cbinsights.com/research/what-is-blockchain-technology/

+ Objectives

Design methods and systems to support the right of individuals to the **protection** of personal data, at the same favoring its **portability** and economic exploitation and fostering the social good

1. To design methods and systems that store and transfer personal data in a **controlled, transparent and non-centralized** manner

2. To identify **modeling and evaluation** methodologies for the analysis of decentralized and complex systems, such as those considered in this domain

3. To specify languages and protocols that favour personal data **interoperability**

4. To specify the languages and algorithms necessary to **represent and reason with policies in smart contracts** to govern the access to personal data

+ Hypotheses

1. The use of **DLTs** to represent and transact with personal data would grant data validation and access control, as well as no central point of failure and immutability

2. It is possible to use **decentralized file systems** for storage in order to allow continuous data availability.

3. Interoperability can be best achieved if data models adapt the **W3C specifications** for the semantic web.

4. By means of defeasible deontic logic in **smart contracts** individuals are able to state how their personal data is managed.

5. Operating with these technologies is **fast enough** to ensure the correct execution of processes that require individuals' personal data.

+ Research Questions

1. Which technologies and algorithms can ensure the **privacy and security** of individuals' personal data when these are transacted in a decentralized manner?

2. Which decentralized technologies can offer a suitable solution for handling large quantity of data, **maintaining efficiency** in privacy, indexing and accessibility?

3. According to which **criteria** can a decentralized solution be evaluated?

4. Is the current specification of smart contracts able to assure the **correct execution** of individuals intentions?

5. Which challenges to the **use and diffusion of semantic web technologies** do entities that extract and/or process data from individuals present?

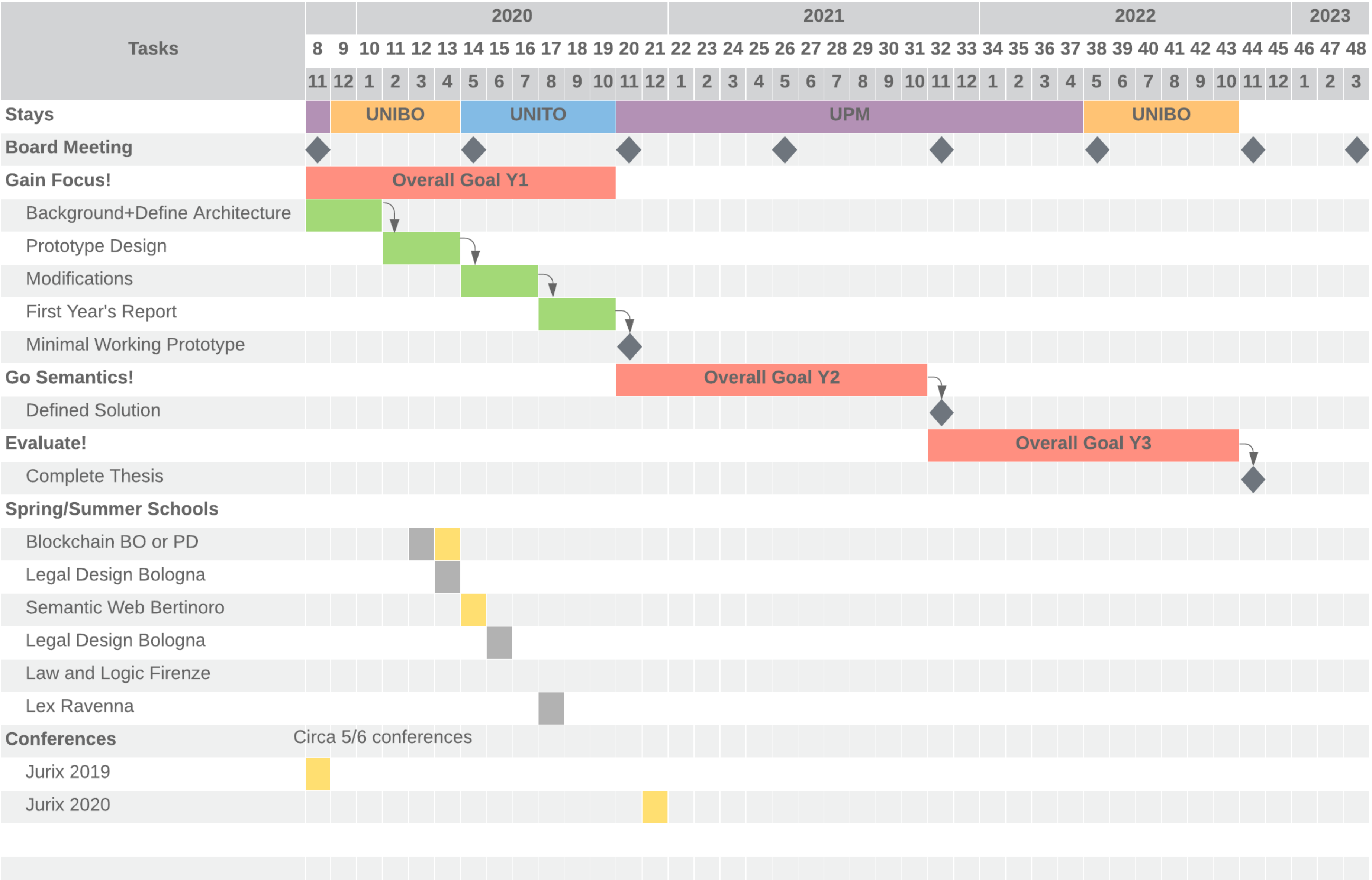
+ Methodology

1. An infrastructure will be specified, where each individual will be associated to a **digital space** that will contain personal data.
   This space will be used to attend the requests of data providers and data consumers.
   The methodology is requirement-driven and empirically validated.

2. The approach of **O1** will be evaluated for its feasibility, performances and security. But the evaluation itself must be evaluated because in such case we are dealing with a **complex system** that does not present a regular structure.

3. A network of **ontologies** will be developed to model the personal data life-cycle and their actors.

4. The language elements to be reasoned with will be supported by smart contracts. These will be designed following reasoning tasks that involve **legal requirements** and **privacy preferences**, in compliance with GDPR


Tasks
2020
2021
2022
2023
8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3
Stays
UNIBO
UNITO
UPM
UNIBO
Board Meeting
Gain Focus!
Overall Goal Y1
Background+Define Architecture
Prototype Design
Modifications
First Year's Report
Minimal Working Prototype
Go Semantics!
Overall Goal Y2
Defined Solution
Evaluate!
Overall Goal Y3
Complete Thesis
Spring/Summer Schools
Blockchain BO or PD
Legal Design Bologna
Semantic Web Bertinoro
Legal Design Bologna
Law and Logic Firenze
Lex Ravenna
Conferences
Circa 5/6 conferences
Jurix 2019
Jurix 2020

20/11/2019

References

1. R. Kitchin, The data revolution: Big data, open data, data infrastructures and their consequences. Sage, 2014.

2. Council of European Union, “Regulation (eu) 2016/679 - directive 95/46,” pp. 1–88

3. P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez, “The right to data portability inthe gdpr: Towards user-centric interoperability of digital services,”Computer Law & Security Review,vol. 34, no. 2, pp. 193–203, 2018

4. T. Berners-Lee, J. Hendler, O. Lassilaet al., “The semantic web,”Scientific american, vol. 284, no. 5,pp. 28–37, 2001

5. https://www.w3.org/TR/rdf-syntax-grammar/

6. https://www.w3.org/TR/owl-features/

7. A. V. Sambra, E. Mansour, S. Hawke, M. Zereba, N. Greco, A. Ghanem, D. Zagidulin, A. Aboulnaga,and T. Berners-Lee, “Solid : A platform for decentralized social applications based on linked data,”2016

8. V.Buterin et al.,“Ethereum whitepaper” 2013.[Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

The LAST-JD-RIoE project

03/12/2019

LAST-JD-RIoE-D1.1

Horizon 2020