BDVe Meetup Workshop Session

Technology solutions for privacy issues: what is the best way forward?

May 14, 2018 from 17.00 to 18.30

BDVe Meetup, Sofia (BG)

Is this our future?

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Agenda

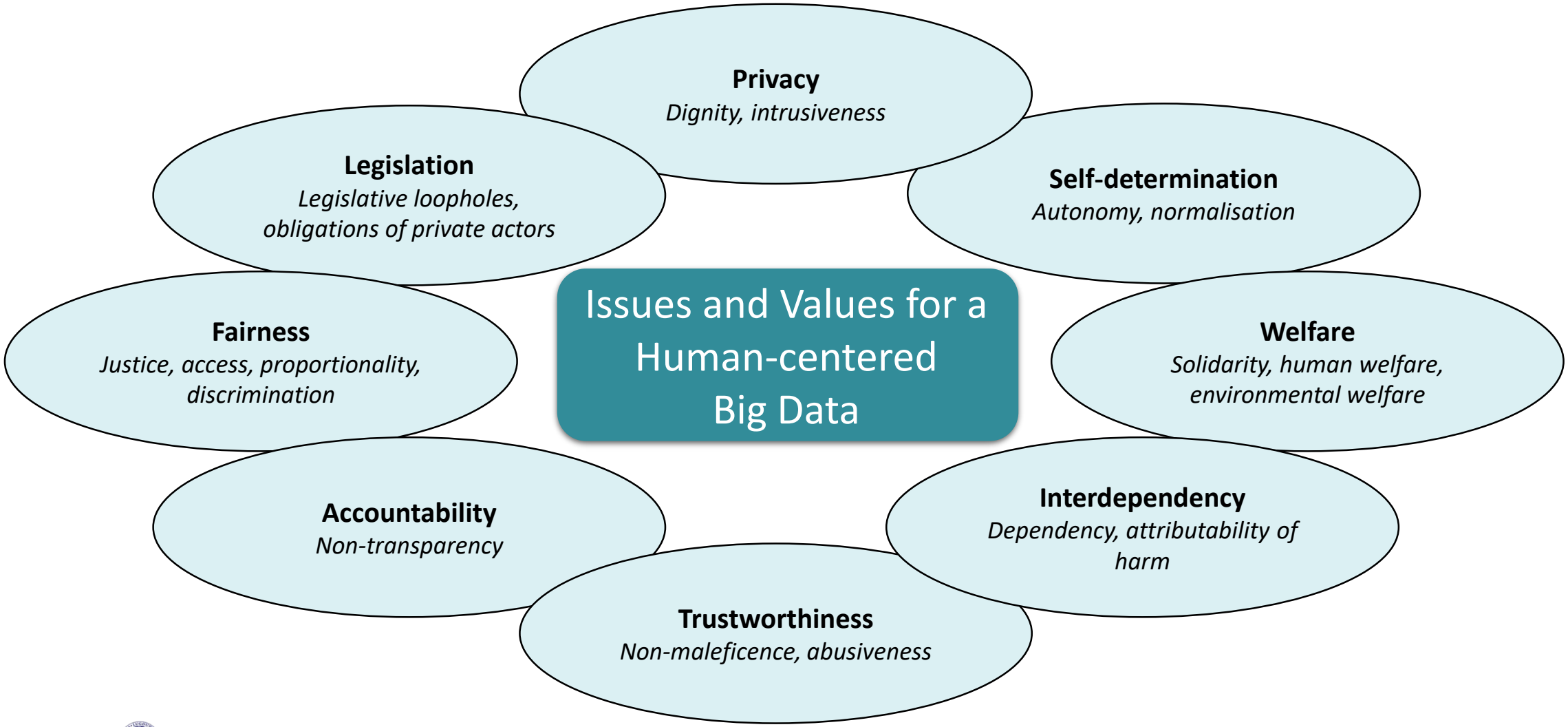
May 14, 2018	BDVe Meetup Workshop Session
17:00-17:15	Welcome and Introduction by Gabriella Cattaneo, e-SIDES Presentation on "Privacy-enhancing technologies: do no evil?"
17:15-17:45	Panel with Presentations by ICT 18 projects SPECIAL, SODA plus others
17:45-18:00	Q&A and Voting with Mentimeter tool
18:00-18:30	Open discussion "What is the best way forward?" on most promising technologies and potential guidelines for responsible research and innovation in developing PETs Wrap up and close

Privacy-enhancing technologies: do no evil

Gabriella Cattaneo, IDC, Daniel Bachlechner, Fraunhofer

E-Sides consortium

“Do no Evil”: yes, but how?



E-SIDES PETs classification

What is mainly done

Sanitisation
Encryption or removal of sensitive information

Anonymisation
Encryption or removal of personally identifiable information

Multi-party computation
Distribution of data and processing tasks over multiple parties

Encryption
Encoding of information so that only authorised parties can access it

Policy enforcement
Enforcement of rules for the use and handling of resources

Access control
Selective restriction of access to places or resources

What we need

Accountability
Evaluation of compliance with policies and provision of evidence

Transparency
Explication of information collection and processing

What is coming up

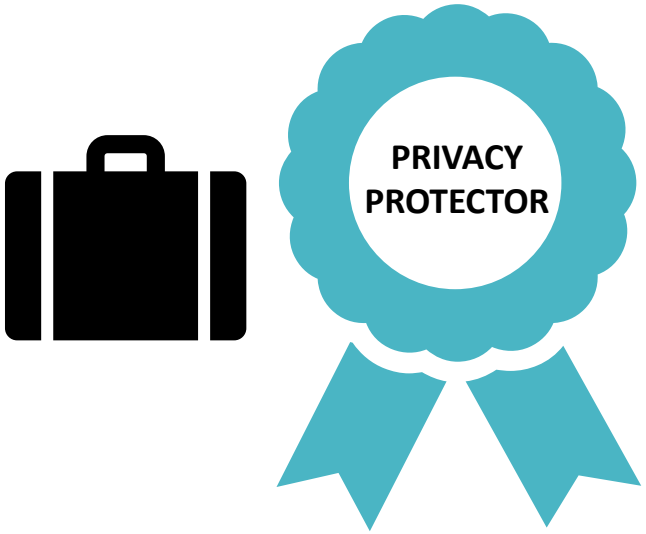
Data provenance
Attesting of the origin and authenticity of information

Access and portability
Facilitating the use and handling of data in different contexts

User control
Specification and enforcement of rules for data use and handling

Today's privacy enhancing solutions

- Insufficiently integrated
- Slow deployment
- Conflicts with new business models
- Enterprises increasingly want to be seen as **privacy protector = brand**



Professor focusing on machine learning, data and text mining, and privacy at a North American university

"Unfortunately, the Cambridge Analytica and Facebook incident may result in further reluctance of the GAFA and similar companies to share data. What is needed are privacy-preserving technologies that make sharing data safe."

What Users Want

- Customers **blinded by the benefits**
- Low consumer demand for privacy
- Add-ons don't work, try embedded
- **The role of policy**

Associate professor focusing on the design, analysis and application of technologies to protect privacy at a European university

"People are worried but at the same time do not know what to do. Technologies and concepts are often complex and counter-intuitive. Moreover, people are not used to the adversarial thinking required to understand threats."

Cowboys vs …Lawyers?

USA

- A consumer right
- Priority: use of data
- Case-based legislation
- Not much trust in government

European Union

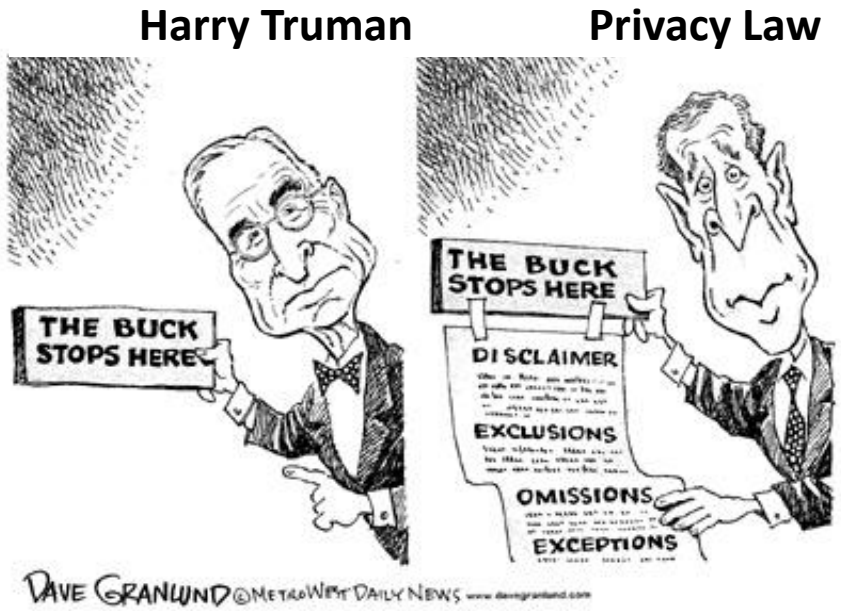
- A fundamental right
- Priority: protect privacy
- Historically more rule-driven
- Belief in Government as protector

A choice for Europe

Opportunity: leader of world privacy regulation

Risk: be deprived of leading technologies

Privacy violations? Not my fault



Associate professor at a European university

"The responsibility placed on the user should be as small as possible"

Professor at a North American university

"Tools for the individual data owners must be provided to control what happens with their data. The research community must develop these tools and they should be available cost-free or at a minimal cost"

- Data protection should not be considered as ***"somebody else's problem"***
- Data owners are responsible for data management and anonymisation
- The **strongest party** should carry the largest responsibility

BUT…

- **Consumers need to protect themselves**
- **Supervisory authorities** and **governments** should shape the framework conditions

Working with privacy by design

- Companies must implement both **technical and organisational measures**
- **Move from proactive prevention** rather than passive defense
- **Awareness** and **education** on the topic for all

Winning mix
technology solutions
+
appropriate processes
+
appropriate agreements and policies
in the right legislation framework

Technology advisor for a national data protection authority in Europe

"The technologies are not the key challenge. In order to make them effective, it is not sufficient if just a single person in the organisation has the required expertise, the entire environment must be aware of the technologies and the related opportunities and threats."

Summary of PETs Issues

ORGANISATIONAL ISSUES
Adapt organizational processes
Assign responsibility
Design Ethical boards and ethical internal review processes

TECHNOLOGY ISSUES
Insufficient Integration in BDT solutions
Deployment too slow
Privacy by Design not fully implemented

POLICY ISSUES
Raise awareness
Provide education
Develop appropriate regulatory framework

What is your opinion?

Real time survey

Which PETs are most effective and/or promising?

You have 100 points to invest (Billions? Researchers?)

Distribute them between the following technologies

Anonymisation

Encryption

Access control

Sanitisation

Multi-party computation

Policy enforcement

Accountability

Transparency

Data provenance

Access and portability

User control

Technology solutions for privacy issues
What is the best way forward?

Which one of the following actions is most relevant, on a scale from 1 (not relevant) to 5 (most relevant) ?

Putting Privacy-by-design into action

- *Pursue user-centric design approaches*
- *Experiment with users to understand their concerns*
- *Employ multidisciplinary and diverse teams to leverage different viewpoints*

Focus on Responsibility in Data Use

- *Design internal ethical review processes*
- *Name a Chief ethical officer*
- *Develop a code of conduct for your organization, research community, or industry*
- *Design your data and systems for auditability*

Keep Transparency, Trust and User control at the centre

- *Develop algorithmic transparency*
- *Liaise with stakeholders to build trust*

What is your opinion?

- Technology can guarantee the anonymization of personal data without losing the value added of analytics: Agree/disagree (vote from 1 to 5)
- We can move from technology as the problem (violating privacy) to technology as the solution: Agree/disagree (vote from 1 to 5)

We want your input!

Go to **www.menti.com** and use the code **28 70 88**

www.menti.com

1 Grab your phone

2 Go to www.menti.com

3 Enter the code **28 70 88** and vote!

Questions for Round Table Discussion

- Which technologies do you consider particularly relevant for privacy preservation in the big data context?
- How effective/mature are the technologies in addressing privacy issues?
- What problems/challenges (may) arise when addressing privacy issues with the technologies?
- What drives/hinders the integration of the technologies in big data solutions? (the general demand for privacy-preserving big data solutions as well as regional differences in value systems could be discussed)
- Where are the boundaries of technology solutions to address privacy issues in the big data context? (organizational solutions including processes, governance, education or awareness raising are necessary to complement technology solutions)
- Who along the value chain is or should be responsible for addressing privacy issues? (e.g., the data processor, the data controller, the data subject, the regulator, all collectively)

To know more about e-SIDES:
www.e-sides.eu

To contact us:

info@e-sides.eu

@eSIDES_eu

Back-up Slides

Real time survey

Potential Guidelines for Responsible Research and Innovation in Big Data

Putting Privacy-by-design into action

- *Pursue user-centric design approaches*
- *Experiment with users to understand their concerns*
- *Employ multidisciplinary and diverse teams to leverage different viewpoints*

Focus on Responsibility in Data Use

- *Design internal ethical review processes*
- *Name a Chief ethical officer*
- *Develop a code of conduct for your organization, research community, or industry*
- *Design your data and systems for auditability*

Keep Transparency, Trust and User control at the centre

- *Develop algorithmic transparency*
- *Liaise with stakeholders to build trust*

Ten Simple Rules for Responsible Big Data Research

1. Acknowledge that data are people and can do harm
2. Recognize that privacy is more than a binary value
3. Guard against the reidentification of your data
4. Practice ethical data sharing
5. Consider the strengths and limitations of your data; big does not automatically mean better
6. Debate the tough, ethical choices
7. Develop a code of conduct for your organization, research community, or industry
8. Design your data and systems for auditability
9. Engage with the broader consequences of data and analysis practices
10. Know when to break these rules

Source: Zook M, Barocas S, boyd d, Crawford K, Keller E, Gangadharan SP, et al. (2017) Ten simple rules for responsible big data research. PLoS Comput Biol 13(3): e1005399. https://doi.org/10.1371/journal.pcbi.1005399