Data Protection in the era of Artificial Intelligence

Charlotte van Oirsouw, TNO, BDVe
Data Protection in the era of Artificial Intelligence

DATA PROTECTION IN THE ERA OF ARTIFICIAL INTELLIGENCE.

Trends, existing solutions and recommendations for privacy-preserving technologies

October 2019

https://bit.ly/2QfBsoC
BDVA: what is it and what does it do?

- Building Big Data Ecosystem
- Support EC research programs
- 50% industry, 50% academia
- 42 projects, +250 partners
Position paper focussed on technical solutions & trends in Privacy-Preserving Technologies

- Why? To give a podium to PPT developments & to highlight challenges
- For which audience? EC, Policymakers, SMEs, the world…
- Who is talking? Experts from several h2020 research projects
- Why focus on technological solutions? To break tech/society dichotomy in data-thinking and to show alternatives (to big tech from US)
Research Questions

How to protect personal data in an era of **big data analysis and AI**? (and is it still about personal data?)

What is the **current state of art** when it comes to PPTs?

What do projects see as **main challenges and trends** in PPTs?

How can research into -and **uptake** of- PPTs be **stimulated**?

How can regulators and **policymakers** help?
Classifying harms and risks

- From the **perspective** of the end-user, data actor, data-driven object, society at large? Economic, social, scientific harm, inferred harms, harms from proxy? Harms based on **inferred** data – boundary of personal data?
- Qualitative vs quantitative ‘**proofs**’ of risks and harms
- Blurring boundary between **privacy harms and safety risks**
- Main challenge for PPTs – **scaling and adoption**
Solutions are either **data-centred**, **actor-centred** or **risk-based**.

ISO: privacy preserving **techniques** & privacy-preserving **models**. It also mentions **synthetic data as a technique for de-identification** (which is debatable).

Hoepmans’ Blue Book: **data-related** vs **process –related** mitigating measures.

**e-SIDES classification** has been mentioned above.

**Summarizing:** there is no 1 way to classify PPTs.
Trend 1: end user back as focus point

Giving people ownership of their personal data

DECODE provides tools that put individuals in control of whether they keep their personal data private or share it for the public good

Find out more

Giving data control back to users. See https://decodeproject.eu/
Trend 2: Automation of policy for big data

SPECIAL Technical Foundations – A Walk-Through

Sticky policy walkthrough. SPECIAL project. See https://www.specialprivacy.eu/flowchart/157-flowchart-01
Trend 3: secure data analytics

MPC visual. TNO. See https://bit.ly/2PEV9X2
Some key topics among h2020 ICT projects

**GDPR COMPLIANCE**

- [https://smoothplatform.eu/](https://smoothplatform.eu/)
- [https://www.pdp4e-project.eu/](https://www.pdp4e-project.eu/)
- [https://www.defendproject.eu/](https://www.defendproject.eu/)

**MPC & SECURE BDA**

- [https://www.soda-project.eu/](https://www.soda-project.eu/)
- [https://www.papaya-project.eu/](https://www.papaya-project.eu/)
- [http://musketeer.eu/](http://musketeer.eu/)
- [https://mosaicrown.eu/](https://mosaicrown.eu/)

**USER CONTROL**

- [https://decodeproject.eu/](https://decodeproject.eu/)
- [https://privacypatterns.eu/](https://privacypatterns.eu/)
- [http://www.myhealthmydata.eu/](http://www.myhealthmydata.eu/)
- [https://pripare.aup.edu/](https://pripare.aup.edu/)

**AUTOMATING COMPLIANCE**

- [https://www.specialprivacy.eu/](https://www.specialprivacy.eu/)
Recommendations for policy

1) Create a (continuously updated) **overview of privacy challenges** caused by BDA and AI
2) **Support R&D** into technical solutions - keeping up with social, ethical and legal developments
3) Supporting **uptake** of privacy-preserving technologies
4) Develop, offer and support **regulatory sandboxes** in which new data services can be tried and tested
BDVA website
http://www.bdva.eu/

BDVA position papers
http://www.bdva.eu/downloads

Webinars, events & marketplace
https://www.big-data-value.eu/