Legal implementation barriers of privacy-preserving technologies

Karolina La Fors PhD MA LLM
Post-doc researcher
eLaw – Center for Law and Digital Technologies
Leiden University

BDV Meet-Up
Thursday, 27th June 2019, Riga (Latvia)

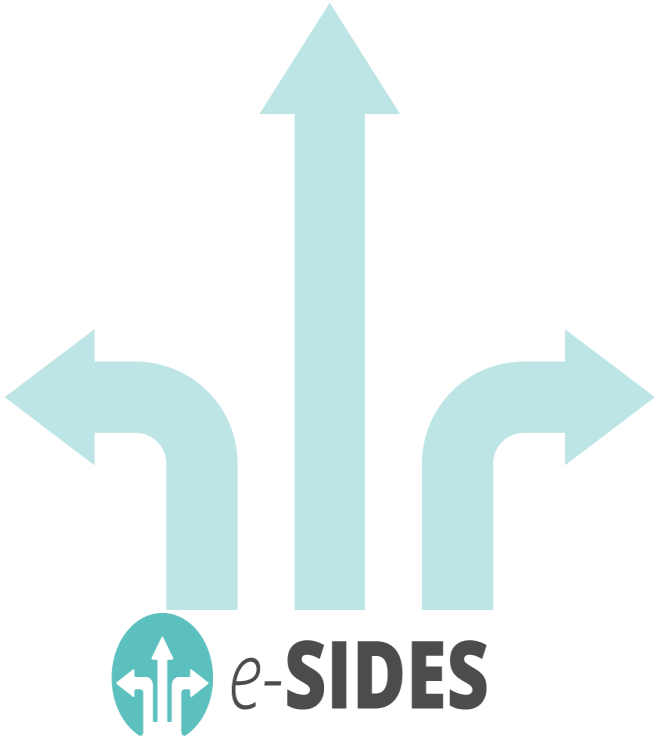
Project overview

Why?

- Reach a common vision for an **ethically sound approach** to big data and facilitate **responsible research and innovation** in the field
- Improve the **dialogue** between stakeholders and the **confidence** of citizens towards privacy-preserving and big data technologies

What?

1) Identify ethical, legal, societal and economic issues
2) Identify existing technologies
3) Assess existing technologies
4) Conduct gap analysis
5) **Identify design requirements**
6) Assess solutions under development
7) Identify implementation barriers
8) Make recommendations



How?

- **Review** of articles (scientific & professional)
- Liaise with researchers, business leaders, policy makers and civil society through **community events**
- Provide an **Internet-based meeting place** for discussion, learning and networking
- Provide a collective **community position paper** with choice points

Legal implementation barriers of PPTs

- Despite being effective PPT not implemented and deployed to their full extent
- Reasons are also societal, legal, economic & technical, but now:

*What **legal barriers** limit the implementation of privacy-preserving technologies into today's big data solutions?*

Reasons for legal implementation barriers

- Based on desk research we distilled 4 reasons:

  1) regional differences

  2) sensitive data

  3) inferred data

  4) liability & responsibility for the effects of big data-based decisions.

Regional differences

- GDPR: advantage as extraterritorial effects are applicable also for US companies (but threat of 2nd class treatment of citizens)

- Anti-trust law in US & EU differ:
In US anti-trust law legitimize the use of consumer data "as a key competitive strategy" and as a clear asset to foster innovation.

Sensitive data

- Flexible interpretation of privacy and privacy-preserving technologies is both a blessing & a curse for practitioners
- Specific rules for the protection of special categories of data are embraced to differing extents
  - healthcare professionals see strict data protection rules as impediments for epidemiological research

Inferred data

- EU regulation lags behind in providing legal remedy for the unforeseen implications of big data analytics (e.g.: non-discrimination law applies only for ‘protected characteristics’ as input data but not for inferences)

- A broad interpretation of the right to data portability in GDPR could address challenges of the undesired consequences of inferred data

Shared responsibility

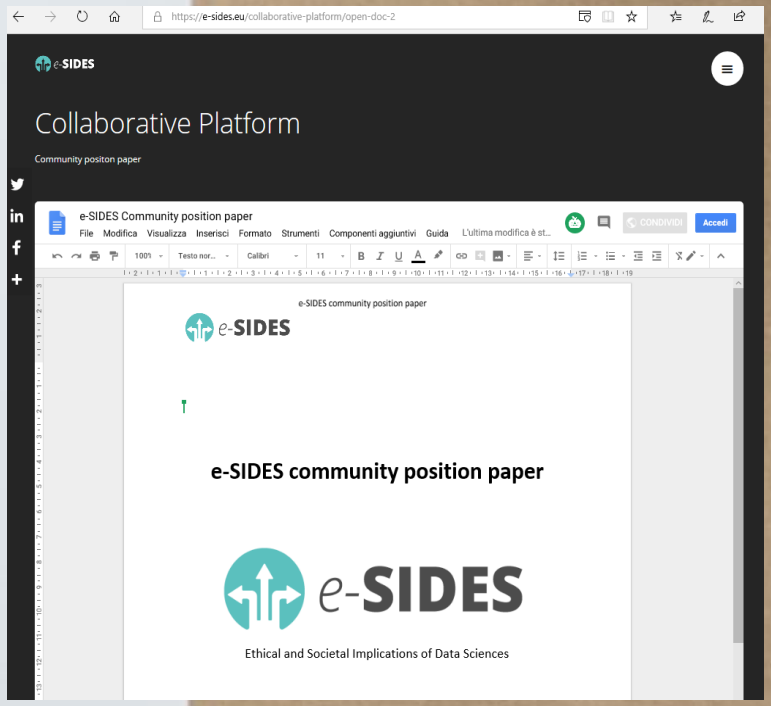
- The **entire big data value chain** should embrace privacy-preservation as a shared responsibility
- **Beyond legal compliance** also context specific **ethical codes of conduct** could help **bringing down barriers** for the implementation of privacy-preserving technologies.

Community Position Paper (eLaw leads)

- Title: *Towards more accountable big data governance and responsible innovation of privacy-preserving technologies*

- Topics addressed
- Timing
- Creation process (6 months)
- Contribution of the community

- April 2019 expert workshop organized for input



Questions?