e-SIDES Ethical and Societal Implications of Data Sciences

Privacy-preserving technologies are not widely integrated into big data solutions. What are the reasons for this implementation gap?

e-SIDES

Ethical and Societal Implications of Data Sciences

About the e-SIDES project

Data-driven innovation is deeply transforming society and the economy. Although there are potentially enormous economic and social benefits, this innovation also brings new challenges for individual and collective privacy, security, as well as democracy and participation. The main objective of the CSA e-SIDES is to complement the research on privacy-preserving big data technologies, by analysing, mapping and clearly identifying the main societal and ethical challenges emerging from the adoption of big data technologies, conforming to the principles of responsible research and innovation; setting up and organizing a sustainable dialogue between industry, research and social actors, as well as networking with the main Research and Innovation Actions and Large Scale Pilots and other framework program projects interested in these issues. It will investigate stakeholders' concerns, and collect their input, framing these results in a clear conceptual framework showing the potential trade-offs between conflicting needs and providing a basis to validate privacy-preserving technologies. It will prepare and widely disseminate community shared conclusions and recommendations highlighting the best way to ultimately build confidence of citizens and businesses towards big data and the data economy.

Deliverable D4.1 Results of the Gap Analysis

Find more at: https://e-sides.eu/resources/deliverable-41-results-of-the-gap-analysis

About this white paper

This white paper is based on Deliverable D4.1 of the e-SIDES project, which provides a gap analysis based on the findings related to the key ethical, legal, societal and economic issues emerging from the use of big data and the assessment of existing privacy-preserving technologies. We look at their effectiveness in addressing those ethical and societal issues and the challenges that arise in their implementation.

Find more: *Deliverable D2.2 Lists of ethical, legal, societal and economic issues of big data technologies* https://e-sides.eu/resources/deliverable-22-lists-of-ethical-legal-societal-and-economic-issues-of-big-data-technologies
Deliverable D3.2 Assessment of Existing Technologies https://e-sides.eu/resources/deliverable-d32-assessment-of-existing-technologies

IDC ANALYZE THE FUTURE

eLAW LEIDEN

Fraunhofer

This Deliverable provides a gap analysis related to the findings of Deliverable 2.2 (the assessment of ethical, legal, societal and economic issues that emerge in different big data contexts in general), and Deliverable 3.2 (the assessment of classes of currently existing privacy-preserving technologies – PPTs - including their effectiveness and the challenges that arise in their implementation), and builds on the conclusion that there is an implementation gap.

The figure below shows the process that led e-SIDES to undertake the gap analysis presented in Deliverable 4.1.

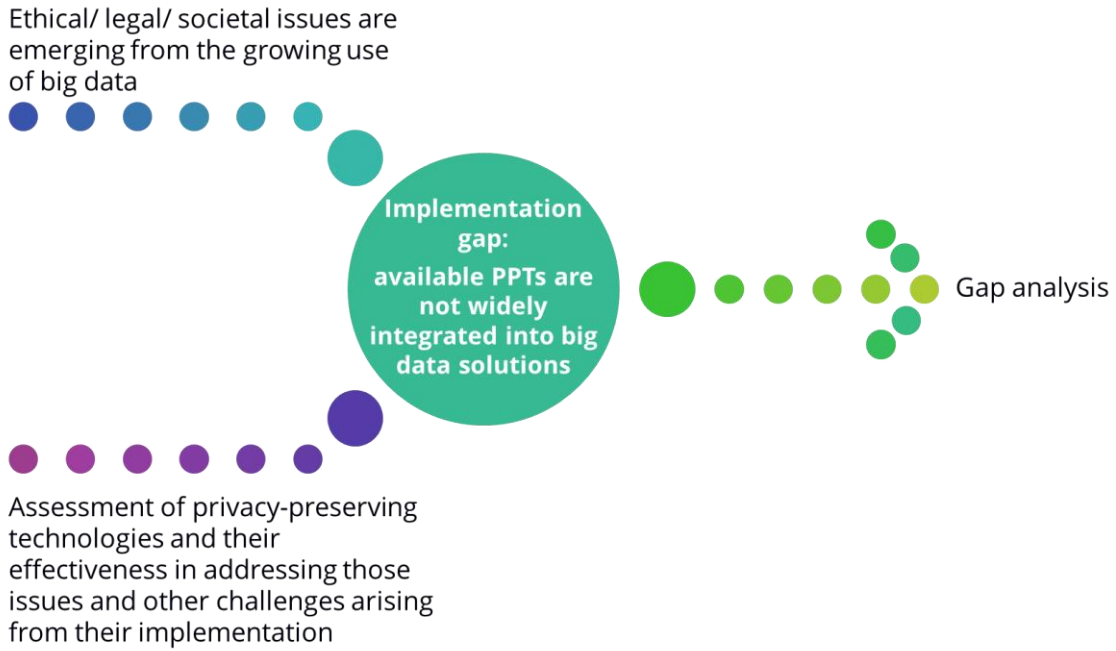
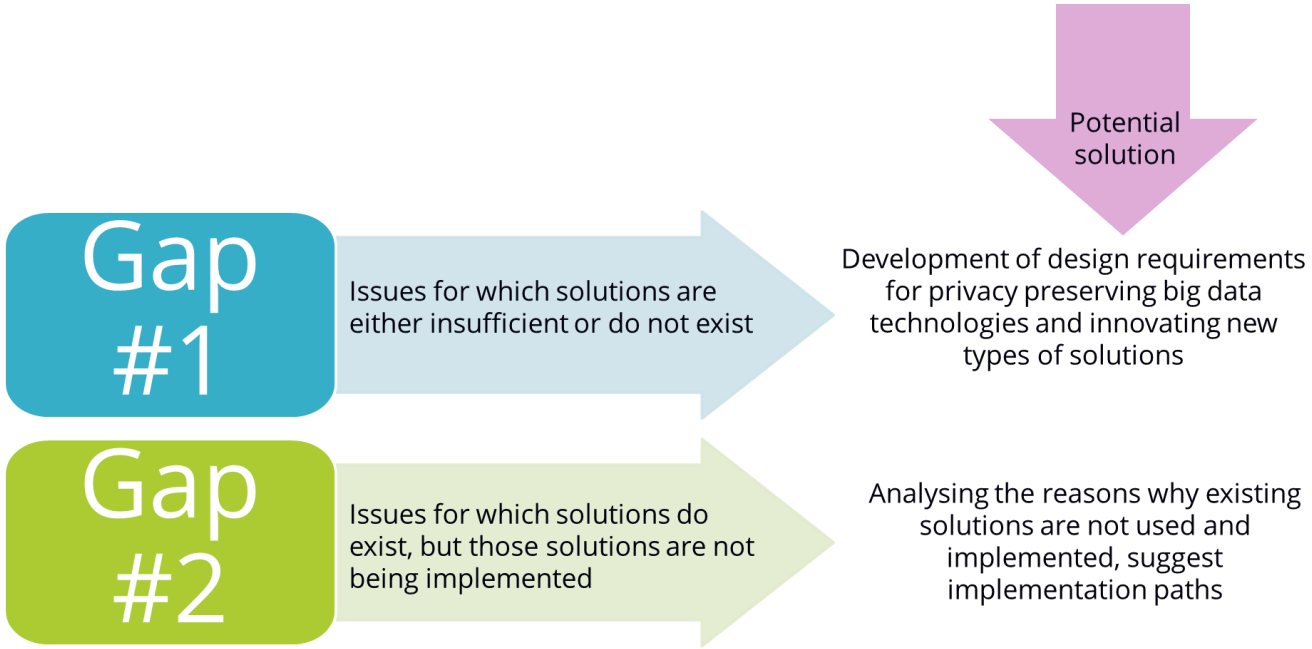


Figure 1 Gap Analysis Process

In the following pages we provide a summary of the key findings of this gap analysis.

Two broad categories of gaps can be distinguished. First, there may be issues for which solutions are either insufficient or do not exist. Second, there may be issues for which solutions do exist, but those solutions are not being implemented.



The first type of gaps could be addressed by further developing design requirements for privacy preserving big data technologies and innovating new types of solutions. For the second type of gaps, there is not so much need for further technological developments, but rather for finding the reasons for which the existing and available solutions are not used and implemented. Perhaps the solutions are unknown or too expensive or not prioritized. Depending on the reasons behind this, next steps can be formulated to address the ethical, legal, societal and economic issues.

In the analysis of the legal and ethical challenges emerging from the use of big data solutions, we highlighted that the explanations for the limited or scarce introduction of privacy-preserving technologies lies to a large extent in their flexible interpretation being both a blessing and a curse for practitioners. This point has also been strengthened by the economic and social analysis that stresses the point that the refrained introduction of privacy-preserving big data technologies was aligned with organisational struggles in defining privacy too narrowly, conflicting definitions and troubles in translating such definitions into design requirements.

With respect to legal and ethical reasons in the context of sensitivity of data, we found that although the GDPR offers clear benefits for protecting a broad set of sensitive information, not all professionals embrace its potential for strengthening the right to non-discrimination to the same extent, which right is clearly facilitated by Art. 9 of the GDPR. For instance, healthcare researchers argue that strict privacy protection and also the robust implementation of privacy-preserving technologies could hamper epidemiology research and big data's value for the advancement of healthcare research.

A strong component of the ethical and legal reasons leading up to or stemming from the limited or scarce introduction of privacy-preserving technologies relates to a number of liability and ethical responsibility concerns that need consideration. Organisations that collect, use and distribute data are in general responsible for privacy-related tasks such as anonymisation and encryption. Data controllers and processors have both legal and ethical obligations to implement such privacy-preserving technologies. When viewing the entire data value chain, privacy preservation must be a shared responsibility. Yet, in effect the levelling of responsibilities should correspond with the strength of a given party involved in the data value chain. This is currently not the case. Yet, an overall transparency for the data value chain is crucial in respect to the liability and responsibility of stakeholders so that they can be taken into account for the development and implementation of big data solutions.

European and American legal framework peculiarities impact on transparency and affect the adoption of privacy preserving technologies.

Currently, regional differences in data protection and antitrust or competition law regimes between the EU and the US also influence the extent to which liabilities of big data stakeholders are made transparent and the extent to which privacy-preserving technologies are embraced and implemented.

Privacy and civil liberties engineer at a software and services company specialised on big data analysis headquartered in North America

"North American companies are certainly interested in European markets. The companies try to strike a balance between investments and safeguards."

North American stakeholders

- prime the utility of data
- rely on case-based legal decisions
- do not seem to trust the government much

European stakeholders

- prime concerns about privacy
- live in a historically more rule-driven environment
- see governments as important privacy protectors

The EU becomes an **exporter of norms** or is **deprived of leading technologies**

Ideally the legal regimes of data protection, which should help to stem data breaches, and competition law, which should help prevent certain organisations from utilising a dominant position in the market, in general should complement and desirably mutually strengthen each other. This (the enforcement of data protection and competition law) is indispensable to both protect the rights of consumers and the rights of SMEs in doing big data-based business. On this subject US and EU approaches differ, yet some movements of the US antitrust regulators from September 2018 begin to point towards the EU's approach. This change in the US approach includes not only that criteria to measure price discrimination should be leading but also a general vision-change for companies to strive for a more equal treatment of consumers. In that regard, privacy-preserving technologies could play a facilitating role. The European Union's data protection supervisor, Giovanni Buttarelli, envisions probably the most

fruitful approach: he sees collaboration between the different regulatory regimes of data protection, consumer protection, and antitrust in order to address the platform power of organisations and its impact on consumers.

Budget limitations or concerns may prevent the implementation of privacy-preserving technologies

As much as these legal and ethical reasons and challenges are intertwined with each other so are the economic and social reasons that explain a lack, or limitations of incentives to introduce privacy-preserving technologies. One of our findings in the economic and social reasons sections relates first to the fact that, for instance, cutting-edge hardware and software is likely to be more expensive than solutions with a track-record. Although costs of resources needed in order to respond effectively are relevant in the privacy context, the costs related to the resources instrumental to repair damaged systems and data are often beyond the calculation of companies. This closely ties into our third finding, that from an economic point of view, putting the foundational principles of data protection into practice can be in conflict with business models. Yet with the GDPR going into effect in May 2018, some companies might have accepted the risk of ignoring data protection compliance requirements. In this sense the GDPR can help; especially, given the extensive fines, which are now more likely to follow from non-compliance, more and more companies are forced to adopt substantial changes. Our fourth finding with respect to the economic and social aspects was that business model conflicts often result from trade-offs drawn between privacy preservation and data use. One area of big data context where such business model is used is healthcare, and as explained above healthcare researchers have particular reservations as to introducing too strict privacy-preserving technologies as they fear that could impede innovation. Yet, our fifth finding underlines that the privacy, security and data protection standards drawn up in Europe have the capacity to become a trademark even beyond the EU. The developments in the legal framework facilitate a movement into this direction, which points towards addressing key economic and social reasons for the implementation gap.

Bridging cultural differences is challenged by the fact that privacy outcomes are often unpredictable and context-dependent

With respect to economic and social aspects in embracing privacy-preserving technologies a sixth point to make relates to cultural differences. For instance, cultural values can influence people's privacy perceptions such that countries with tighter privacy regulations experience fewer privacy problems. Yet, as our media analysis has also shown there were significant differences in the portrayal of the issues around the implementation of GDPR, including privacy-preserving technologies, if comparing the coverage in Germany and the UK. A large portion of cultural reasons, we argue, however could be addressed by offering individuals personal benefits – not only free access to online services, but monetary compensation – for the value of their data being used by big data companies.

A consumer mentality change and the acquisition of new skills may also help protect personal data and privacy in economic operations

A seventh economic and social reason to mention is that despite data breach scandals and the rise of cyberattacks, consumers are still often attracted to buy products and services from a provider who offers lower prices and lower data protection than companies offering a higher level of data security and higher prices for products and services. Developers need knowledge not only of maths and statistics, but also insight into data ethics, information law, and privacy law, among others. Users need to be tech savvy, aware of privacy risks, and have the skills to prevent or combat such risks. Furthermore, the amendment of business models towards a more value-sensitive approach could complement the process and motivate the embracement of privacy-preserving technologies. The capacities of the new EU data protection and competition law can clearly promote the integration of privacy-preserving technologies into big data solutions. Furthermore, the role of technologies in closing the implementation gap is also crucial to embrace. An increase in proactive approaches by privacy-preserving technologies that prevent breaches or rule violations in the first place are stimulated by the legal regime but shall desirably also be embraced as a mentality change. Furthermore, smaller companies might want to initiate competition law cases (as a violation of the freedom to do business) towards larger companies as well, especially after Google's antitrust case regarding Android in the EU.

The introduction of privacy-preserving solution needs to be periodically assessed with respect to their use and implications

As a final concluding remark for our analysis of ethical legal, economic and societal aspects leading up to and stemming from the limited or scarce introduction of privacy-preserving technologies we also stress the need for the constant reassessment of privacy-preserving technologies with respect to their design and use in relation to the social, ethical, legal and economic effects on persons and society at large. As we have demonstrated, these technologies alone cannot address all ethical and societal issues. A combination of legal, ethical, economic and societal changes are needed in order to facilitate transformations towards a more privacy-preserving data usage that capitalizes on the value of big data but respects the ethical, legal and societal limitations of exploiting that data. Privacy-preserving technologies can facilitate transformations in business models that are mainly aimed at data exploitation, in organisational structures and towards more cultural receptiveness of these technologies after walls around differences in definitions and expectations of privacy preservation are cracked down, or made more transparent among stakeholders. Each of these steps should bring us closer to a wider implementation of privacy-preserving technology solutions in the variety of big data contexts.

e-SIDES

To know more about e-SIDES:

www.e-sides.eu

To contact us:

info@e-sides.eu

@eSIDES_eu

e-SIDES

IDC ANALYZE THE FUTURE

eLAW LEIDEN

Fraunhofer