# Article information:

When data protection by design and data subject rights clash | International Data Privacy Law | Oxford Academic
[https://academic-oup-com.ezproxy.st-andrews.ac.uk/idpl/article/8/2/105/4960902?login=true=eyJhbGciOiJub25lIn0.eyJleHAiOjE2ODM0MDc2MzcsImp0aSI6Ijc2N2M2NDhjLWY2ZmYtNDUwOC1hZmVjLTcwYzE1OTU0NGEzMyJ9.](https://academic-oup-com.ezproxy.st-andrews.ac.uk/idpl/article/8/2/105/4960902?login=true&token=eyJhbGciOiJub25lIn0.eyJleHAiOjE2ODM0MDc2MzcsImp0aSI6Ijc2N2M2NDhjLWY2ZmYtNDUwOC1hZmVjLTcwYzE1OTU0NGEzMyJ9.)

# Article summary:

1. Data protection by design (DPbD) is a qualified duty in the GDPR, but practitioners often frame it through the confidentiality-focused lens of privacy enhancing technologies (PETs), which can limit data subject rights while leaving data reidentifiable by capable adversaries.

2. Case studies of Apple's Siri voice assistant and Transport for London's Wi-Fi analytics demonstrate how some DPbD strategies used by large data controllers can reduce their own data protection obligations and shift risk onto the data subject, who loses her ability to manage the risk herself.

3. To make deployed DPbD more accountable and data subject-centric, the article suggests building parallel systems to fulfill rights, making trade-offs more explicit through Data Protection Impact Assessments, and providing information concerning DPbD trade-offs through ex ante and ex post information rights.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article discusses the clash between data protection by design (DPbD) and data subject rights, highlighting how some confidentiality-focused DPbD strategies used by large data controllers leave data re-identifiable by capable adversaries while heavily limiting controllers’ ability to provide data subject rights, such as access, erasure and objection. The authors suggest three main ways to make deployed DPbD more accountable and data subject-centric: building parallel systems to fulfill rights, making inevitable trade-offs more explicit and transparent through Data Protection Impact Assessments, and through ex ante and ex post information rights.

The article provides case studies of Apple’s Siri voice assistant and Transport for London’s Wi-Fi analytics to illustrate the issue. However, the article seems to have a bias towards privacy-as-control rather than privacy-as-confidentiality. It argues that PETs are primarily focused on information disclosure guarantees rooted in either information theory or computational “hardness” of the resultant re-identification or disclosure problem. The authors argue that this notion of privacy-as-confidentiality sits at least apart from, and potentially at tension with, the notion of privacy-as-control as espoused by the FIPs and GDPR.

The article also suggests that some controllers pursue an interpretation of these provisions which is unfavorable to the effective exercise of data subject rights. However, it does not provide evidence for this claim or explore counterarguments. Additionally, while the article notes possible risks associated with DPbD strategies used by large data controllers, it does not present both sides equally.

Overall, while the article raises important issues related to DPbD and data subject rights, its bias towards privacy-as-control may limit its perspective on potential solutions. Additionally, it could benefit from exploring counterarguments and presenting both sides equally.

# Topics for further research:

* Criticisms of privacy-as-control approach in data protection
* Advantages and disadvantages of PETs in data protection
* Impact of DPbD on data subject rights
* Trade-offs between confidentiality and data subject rights in DPbD
* Interpretation of FIPs and GDPR provisions by data controllers
* Risks and benefits of DPbD strategies for large data controllers

# Report location:

<https://www.fullpicture.app/item/35352674fe45d7937044740af4577361>