

Introduction to the Minitrack on Privacy, Trust, and Governance in the Data-driven Economy

Ofe, Hosea; Sandberg, Johan; Rudmark, Daniel; de Reuver, Mark

DOI

[10.24251/HICSS.2023.527](https://doi.org/10.24251/HICSS.2023.527)

Publication date

2023

Document Version

Final published version

Citation (APA)

Ofe, H., Sandberg, J., Rudmark, D., & de Reuver, M. (2023). *Introduction to the Minitrack on Privacy, Trust, and Governance in the Data-driven Economy*. 4326-4327. Paper presented at 56th Annual Hawaii International Conference on System Sciences, HICSS 2023, Virtual, Online, United States.
<https://doi.org/10.24251/HICSS.2023.527>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Introduction to the Minitrack on Privacy, Trust, and Governance in the Data-driven Economy

Hosea Ofe
Delft University of
Technology

h.a.Ofe@tudelft.nl

Johan Sandberg
Umeå University

johan.sandberg@umu.se

Daniel Rudmark
University of Gothenburg
RISE Research Institutes
of Sweden

daniel.rudmark@ait.gu.se

Mark de Reuver
Delft University of
Technology

g.a.dereuver@tudelft.nl

1. Minitrack Purpose

The increasingly essential and strategic role of data as a raw material for social and economic activities exposes firms to new opportunities and challenges. As organizations seek novel ways of organizing and innovating to enhance competitiveness by leveraging data, more insights and guidance on how to approach this transformation are essential. However, even though large-scale analytics can provide unprecedented insights into, e.g., consumer behavior, firms need to govern these value creation opportunities in ways where stakeholder privacy is ensured and trust among involved parties is maintained. Such governance processes involve complex, dynamic power relationships with unpredictable outcomes (Ofe and Sandberg, 2023). Consequently, we project far-reaching implications for business models, frameworks, public policy, and governance structures within the data-driven economy.

The purpose of this minitrack is to draw attention to a spectrum of socio-technical implications of privacy, trust, and governance in the data-driven economy. Our aim with this minitrack is to provide opportunities for researchers to articulate and examine boundaries on phenomena of privacy, trust, and governance implications as organizations increasingly rely on data for sustaining their competitiveness.

2. Minitrack Papers

The papers of this inaugural minitrack have a common focus on organizations' response to pressures for increased privacy and they exhibit the breadth of its sources (legislators, users, and employees). In total, three papers, all empirical, were accepted for presentation.

Digital technologies are double-edged in that they can enable transparency but also be used for surveillance and oppression. Developers must thus carefully consider how to design trustworthy digital services, especially if these services are related to political processes or whistleblowing. This minitrack's first paper, *Building Digital Trust to Protect Whistleblowers - A Blockchain-based Reporting Channel*, Asprion, Grieder, and Grimberg (2023), examines how technological affordances can be used to

increase trustworthiness. Based on findings from a design science research endeavor, the authors explore requirements for trustworthy reporting services, examine how blockchain can help meet these requirements, and suggest design implications through a prototypical solution.

Regulation can have unpredictable and paradoxical outcomes, as shown by the second paper *Does Data Privacy Regulation Only Benefit Contracting Parties? Evidence from International Digital Product Market*. Li, Lee, Raghu, and Shi (2023) find that the introduction of GDPR benefited the competitive position of non-EU app developers. The authors show that, after GDPR implementation, the proportion of non-EU-based apps in top app chart lists has increased significantly, while EU-based apps have reduced. Possibly, European citizens are more open-minded and willing to use foreign digital goods after the rollout of GDPR. The paper contributes to the ongoing debate on privacy protection regulation and its implications for businesses and consumers in our society.

We live in a data economy where new logics of value generation and accumulation emerges (Zuboff, 2015). In this environment, privacy is a key concern for academics and society. Consumers often respond to privacy violations in paradoxical ways. These responses are examined in the third paper, *When and Why Consumers Respond to Online Privacy Violations*. Tran, Reich and Yuan (2023) report findings from three studies on consumer responses to privacy violations. From the studies, the authors conceptualize three types of privacy violations. For each type, consumer responses can largely be explained by differences in variability in industry-specific privacy practices.

3. Concluding remarks

On a broader scale, we see a complex interplay of platform business models, consumer privacy, and regulation. Following the success of the GDPR, a range of EU regulations has been created, such as the Digital Market Act and the Data Act. Within this arena, societal goals are competing: harnessing platform power, protecting consumer privacy, and realizing a single market for data and AI. Fascinating research questions await in this field full of opportunities to do natural experiments, with regulatory interventions, business

model innovation, and societal concerns co-evolving. Add to the mix new technological paradigms, such as privacy-preserving technologies, and we may be in for more unexpected and paradoxical outcomes.

4. References

Asprion, P., Grieder, H., and Grimberg, F. (2023). Building Digital Trust to Protect Whistleblowers - A Blockchain-based Reporting Channel. In *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Li, Z., Lee, G., Raghu, T. S., and Shi Z. (2023). Does Data Privacy Regulation Only Benefit Contracting Parties? Evidence from International Digital Product Market. In

Proceedings of the 56th Hawaii International Conference on System Sciences.

Ofe, H. A., & Sandberg, J. (2023). The emergence of digital ecosystem governance: An investigation of responses to disrupted resource control in the Swedish public transport sector. *Information Systems Journal*, 33(2). <https://doi.org/10.1111/isj.12404>

Tran, C., Reich, B., and Yuan, H. (2023). When and Why Consumers Respond to Online Privacy Violations. In *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, 30(1), 75-89.