Multi-Party Computation as a Data Sharing Solution for Compliance Monitoring An Exploratory Study in the Domain of Battery Circularity

Agahari, Wirawan; Rukanova, Boriana; Ubacht, Jolien; Tan, Yao Hua

Publication date
2024

Document Version
Final published version

Published in
CEUR Workshop Proceedings

Multi-Party Computation as a Data Sharing Solution for Compliance Monitoring: An Exploratory Study in the Domain of Battery Circularity

Wirawan Agahari[1,2,*], Boriana Rukanova[1], Jolien Ubacht[1] and Yao-hua Tan[1]

[1] *Delft University of Technology, Jaffalaan 5, 2628 BX, Delft, the Netherlands*
[2] *Tilburg University, Warandelaan 2, 5037 AB, Tilburg, the Netherlands*

Abstract

Monitoring the circular economy (CE) transition requires data sharing and collaboration between public and private actors. However, businesses are reluctant to share data with authorities for monitoring purposes due to fear of losing control over sensitive data. The emerging technology Multi-Party Computation (MPC), which enables collaborative data analysis while maintaining data control, could address barriers in business-to-government (B2G) data sharing and collaboration. This ongoing research aims to explore the potential of MPC in facilitating B2G data sharing and collaboration for CE monitoring under the conditions of inter-organizational trust and data control. Drawing on a B2G data sharing framework, our initial findings suggest that MPC can benefit authorities in accessing sensitive business data, while businesses can benefit from controlling shared data for compliance reporting. As MPC can be deployed in various architectures, the next research steps are to examine links between variants of MPC architectures and different data-sharing solutions.

Keywords

business-to-government, data sharing, privacy-enhancing technologies, multi-party computation, circular economy monitoring, batteries

1. Introduction

The transition towards a circular economy (CE)—a regenerative system designed to minimize resource usage, waste, and emissions through narrowing, slowing, and closing material loops [1, 2]—is a high priority for governments around the world. Policies like the European Green Deal [3] to stimulate the CE transition are being implemented, but public organizations lack the means to monitor the effects of these policies due to business data being scattered across multiple actors in their own IT systems [4, 5]. In addition, given that

Proceedings EGOV-CeDEM-ePart conference, September 1-5, 2024, Ghent University and KU Leuven, Ghent/Leuven, Belgium
* Corresponding author.
w.agahari@tudelft.nl; w.agahari@tilburguniversity.edu (W. Agahari); b.d.rukanova@tudelft.nl (B. Rukanova); j.ubacht@tudelft.nl (J. Ubacht); y.tan@tudelft.nl (Y. Tan)
0000-0001-8588-8421 (W. Agahari); 0000-0003-0254-5787 (B. Rukanova); 0000-0002-1269-7189 (J. Ubacht); 0000-0002-5930-5138 (Y. Tan)

businesses consider their data as commercially sensitive, they are reluctant to share their data without assurances over data sovereignty and control [6, 7]. Therefore, a mechanism is needed to enhance inter-organizational trust and control in business-to-government (B2G) data sharing and collaboration for CE monitoring [8, 9].

Using Privacy-Enhancing Technologies (PETs)—technological artifacts to protect sensitive data while maintaining its functionality [10, 11]—can overcome barriers in B2G data sharing and collaboration. One of these PETs is Multi-Party Computation (MPC), which enables joint computation between multiple stakeholders to generate meaningful insights from various data sources while maintaining data control and respecting confidentiality [12-14]. Although MPC is traditionally viewed as a privacy technology, its potential goes beyond that and can also be seen as a data collaboration tool under the conditions of inter-organizational trust and data control [15].

Public-private data sharing and collaboration is a nascent topic in the Information Systems (IS) and e-government domains [8, 9], and empirical evidence is scarce on how this type of data collaboration can be realized to enhance CE monitoring [5, 16]. This calls for research into how CE monitoring can be realized through public-private data sharing and collaboration. Despite the uptake of MPC research that unravels its potential to address data sharing in the context of societal challenges [17, 18], the potential impact of MPC in the CE context is lacking. Combining the two knowledge gaps, our main objective in this paper is to explore the potential contribution of MPC in facilitating B2G data sharing and collaboration for CE monitoring under the conditions of inter-organizational trust and data control.

2. Research design

We conducted an exploratory case study in the context of the DATAPIPE project[1] that aims to support Dutch authorities in fulfilling their new responsibilities in CE monitoring. The authorities need information to establish whether companies comply with legal CE requirements. One of their challenges is assuring that the data and the claims companies provide on using recycled content are correct.

We selected the case of monitoring recycled battery content as mandated by the new EU battery regulation that entered into force in August 2023 [19]. According to this regulation, battery manufacturers must provide documentation regarding the share of recycled content used in their new batteries. This recycled content (i.e., raw materials that were not mined but obtained from recycling) concerns elements such as cobalt, lithium, nickel, and lead that are recovered from battery manufacturing waste or post-consumer waste. The initial EU targets for recycled content are set at a minimum of 16% cobalt, 85% lead, 6% lithium, and 6% nickel, which will increase over time [19].

[1] https://www.tudelft.nl/tbm/onderzoek/projecten/datapipe-project

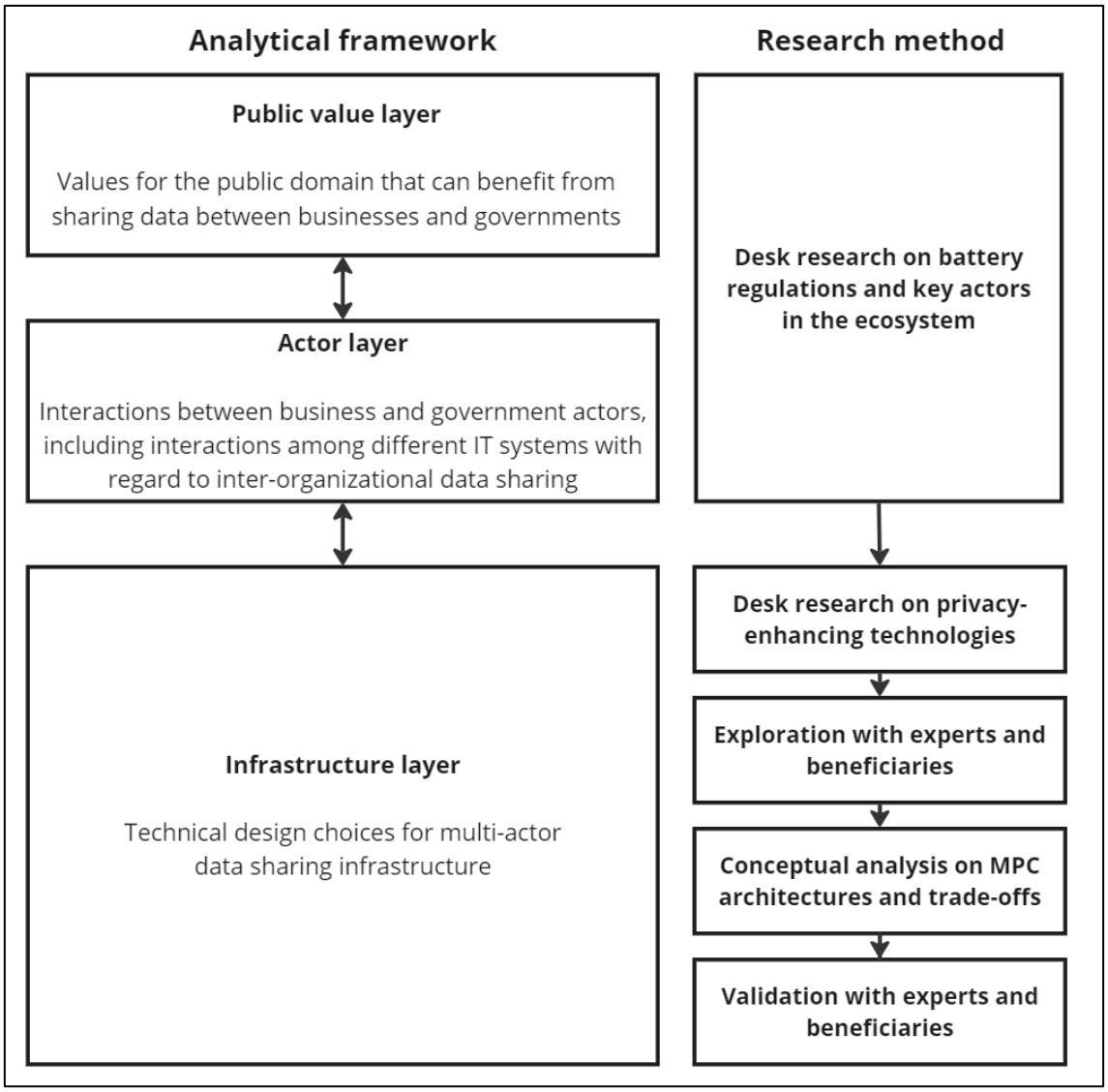

Figure 1. An analytical framework for business-to-government data sharing for public value creation and the corresponding research methods

For the case analysis, we use a framework for investigating B2G data sharing for public value creation developed by [8] (see the left side of Figure 1). This analytical framework consists of three layers: the actor layer, the public value layer, and the infrastructure layer. This high-level framework has previously been used in similar cases for CE monitoring to show the relationship between choices made at the three levels and how they can be aligned [8, 20]. The public value layer examines the public values that can be realized through B2G data sharing and collaboration. The actor layer addresses the business and government actors involved in the CE monitoring context, their internal information systems, and their interactions. The infrastructure layer represents the technical design choices for the multi-actor data-sharing infrastructure. Because of our objective to explore the potential

contribution of MPC in facilitating B2G data sharing and collaboration for CE monitoring, our focus in this paper is on the infrastructure layer.

In examining each layer, we employed various research methods (see the right side of Figure 1). For the public value and actor layers, we conducted desk research to review scientific papers, reports, legal documents, and regulations concerning battery regulations. For the infrastructure layer, we created an overview of different PETs that can contribute to lowering the barriers to B2G data sharing and collaboration. We evaluated this overview in an online session with a technology innovation expert from Dutch customs. After this session, we focussed on MPC as a promising technology to explore its potential use for commercially sensitive invoice data for cross-validation. Subsequently, we further conceptually analyzed different MPC architecture models as part of data sharing architecture and possible trade-offs in the context of CE monitoring. We presented our analyses at weekly meetings with the project team and regular progress meetings with the project beneficiaries for discussion, validation, and feedback.

3. Multi-Party Computation (MPC)

MPC is a cryptographic technique where two or more data owners jointly compute datasets, which results in a meaningful output without revealing the input provided by each data owner [21]. It works by encrypting and splitting the input data into multiple parts, which are then distributed to multiple computational nodes. Subsequently, these nodes compute partial results based on the encrypted data they received, which are then recombined to obtain the final results. A simple example of MPC is the millionaire's problem [13], in which the net worth of two millionaires is securely compared to determine who is the richest without disclosing their net worth to each other.

MPC is useful in a distributed computing scenario where multiple data owners would like to collaborate by computing a function together with their own datasets to obtain valuable insights without giving away their sensitive information [15]. This way, organizations can ensure they keep control of their sensitive data while simultaneously creating value from the relevant data. MPC has been implemented in various real-life applications, including health risk prediction [24], fraud detection [25], economic inequalities [18], and reporting sexual offenders [26]. With the growing attention on MPC and PETs in general from academics and policymakers [27, 28], we can expect a growing number of innovative use cases in the coming years [29].

MPC can be deployed in three architecture models [22, 23]. In the decentralized model, computational nodes are installed locally in data providers and requesters. This model has a low trust requirement as no additional party is involved in the computation, but it requires more resources and effort to set up. Meanwhile, in the centralized single cloud model, one cloud provider is involved as an additional party to set up computational nodes. While this model can reduce the burden for data providers and requesters, it compromises security robustness and trust requirements due to a single third party as a potential point of failure. The third architecture addresses this issue, namely the centralized multiple clouds model. In this model, computational nodes are deployed by multiple independent cloud providers (instead of only one cloud provider) to lower the complexity while maintaining sufficient

robustness and trust requirements, as each cloud provider is independent and ideally would not collude.

4. Preliminary results

We visualize our preliminary results in Figure 2, which is derived based on the analytical framework of B2G data sharing and collaboration for public value creation introduced in Figure 1. The remainder of this section describes our initial analysis of each layer. However, given our focus on exploring the relevance of MPC in facilitating B2G data sharing and collaboration for CE monitoring, we emphasize our analysis of the infrastructure layer.

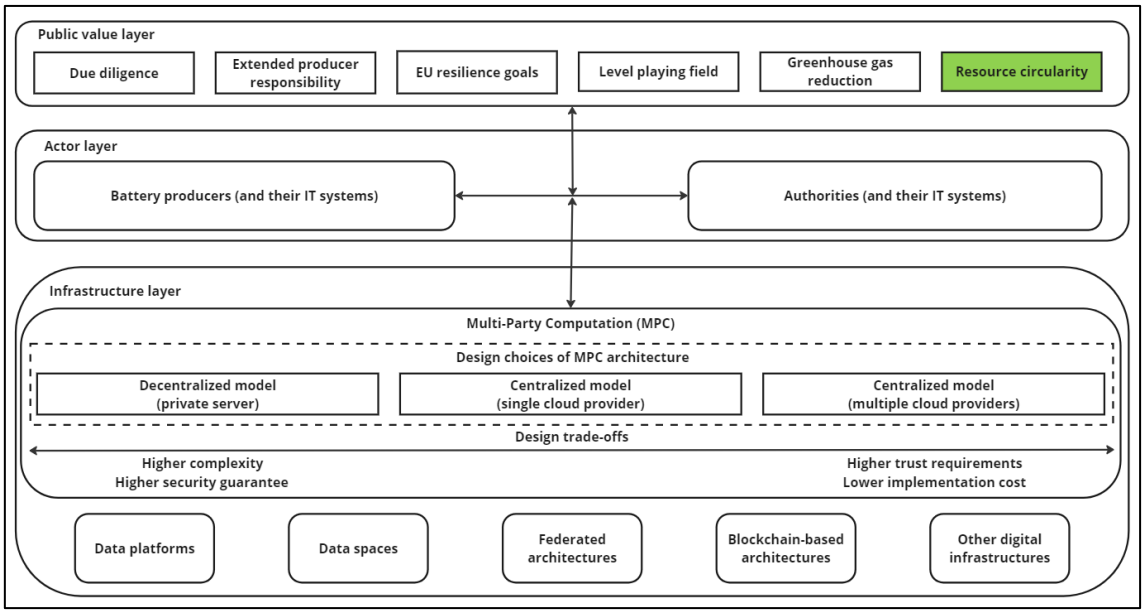

Figure 2: Initial analysis of MPC-enabled B2G data sharing and collaboration for CE monitoring

4.1. Public value and actor layers

For the public value layer, we explore relevant public values that fit within our context of CE, particularly CE monitoring. Our starting point is the conceptualization by [20], who presented six CE-related public values: (1) due diligence, (2) extended producer responsibility, (3) EU resilience goals, (4) creating a level playing field in the EU, (5) reducing greenhouse gas emissions, and (6) resource circularity. Given that the ultimate goal of CE monitoring is to ensure that circularity principles are adhered to while utilizing critical resources, we select **resource circularity** as our key public value for our context (see the top layer of Figure 2).

This public value is relevant if we zoom in on the specific case of battery regulation, as it obliges battery producers to produce new batteries partly based on recycled content extracted from old/used batteries. While it can be argued that other public values, such as due diligence and extended producer responsibility could also be relevant, we limit the

scope of this paper to focus only on resource circularity as a broad public value that fits with our context. Thus, the remainder of the analysis will take into account resource circularity as a public value while looking at the potential of MPC in facilitating B2G data sharing and collaboration for CE monitoring.

Meanwhile, for the actor layer, we incorporate relevant actors that play a role in monitoring CE policies to ensure resource circularity. In this regard, we include those who perform monitoring of CE policies (i.e., public institutions/policymakers) and those who perform activities that might have implications on circularity and, therefore, relevant to be monitored (i.e., private sector/businesses). Given our focus, we chose to emphasize the involvement of two main actors, namely **the monitoring authorities** and **the battery producers** (see the middle layer of Figure 2)**.** Both actors are important and relevant to be included in our analysis, as the new battery regulation requires authorities to monitor recycled content in battery manufacturing. In turn, battery manufacturers are forced to align their objectives with the battery regulation in their manufacturing process and consider the mandatory recycling content target.

Further examining the relationship between the public value layer and the actor layer, it is imperative that realizing the public value of resource circularity requires public-private data collaboration between battery producers and authorities. However, some barriers and tensions could arise between those actors. First, from a technical standpoint, both authorities and battery producers have their own digital systems that may not be interoperable, making it challenging to orchestrate data sharing between them. Second, even if both systems are interoperable, battery producers would want to protect their sensitive and confidential data, such as recipes with exact material composition and battery chemistry, to maintain their competitive advantage. Thus, the tension between realizing the public value of resource circularity and protecting sensitive data needs to be addressed.

4.2. Infrastructure layer

Moving to the infrastructure layer, our focus is to investigate how **MPC can play a role in the infrastructure layer** to facilitate B2G data sharing and collaboration for CE monitoring in the battery domain. Specifically, MPC is seen as a possible means to address one of the data sharing barriers mentioned in section 4.1.: to address the tension between realizing the public value of resource circularity and protecting sensitive business data. We position MPC as a component on the infrastructure layer, in addition to the required technical infrastructural components, such as e.g. a blockchain solution. As our focus in this paper is on the potential impact of MPC, we assume other infrastructural components to be constant.

To conceptualize the relevance of MPC for CE monitoring in the battery domain, we looked back again at battery regulation as a basis of our case analysis. The battery regulation mandates that authorities monitor whether each battery produced by battery producers contains the minimum required recycled content (see Section 2). The issue, then, is how battery producers can share relevant data needed by authorities for monitoring recycled content in new batteries without compromising control over sensitive business data.

For their monitoring task, authorities are not interested in the details of the complete battery recipe or the exact percentage of recycled content in the battery. Instead, they are only interested in checking whether the recycled content in the battery is above or below

the minimum recycled content. This scenario is where MPC can be highly relevant, as authorities can access parts of the battery composition data from battery producers required for monitoring recycled content, which is typically difficult due to its sensitive nature. MPC use can also benefit battery producers by keeping their input data private, meaning they do not need to reveal all details of the battery recipes to show their compliance with the recycled content requirements.

4.2.1. Using MPC for B2G data sharing and collaboration in CE monitoring

We conceptualize four steps regarding how MPC can facilitate B2G data sharing and collaboration for monitoring recycled content (see Figure 3). For simplicity, we limit the scope of our use case to focus on the interaction between one battery producer (battery producer A) and one government authority. Further, our discussion in this sub-section focuses on a decentralized model as a baseline scenario for MPC architecture deployment (see Section 3). We will discuss other MPC architecture options in sub-section 4.2.2.

As a first step, battery producer A internally prepares the recycled content data in new batteries based on the battery bill-of-materials (Step 1: prepare data). In our example, the percentage of recycled content in new batteries produced by battery producer A is 10% cobalt, 89% lead, 8% lithium, and 3% nickel. Next, battery producer A locally encrypts the input data using a dedicated MPC platform installed in their information system (Step 2: secure data), meaning that authorities cannot see the original input data. After that, battery producer A uploads the encrypted data via the MPC platform. Then, the computational nodes perform the MPC protocol to analyze whether the recycled content in new batteries produced by battery producer A is equal to or higher than the mandatory recycled content target (Step 3: start MPC), which is set at a minimum of 16% cobalt, 85% lead, 6% lithium, and 6% nickel [19] (see also Section 2). The computational nodes can only perform the computation and cannot see the input data, as it is already encrypted. Finally, the MPC protocol generates computation results that authorities receive as simple yes/no answers (Step 4: share results).

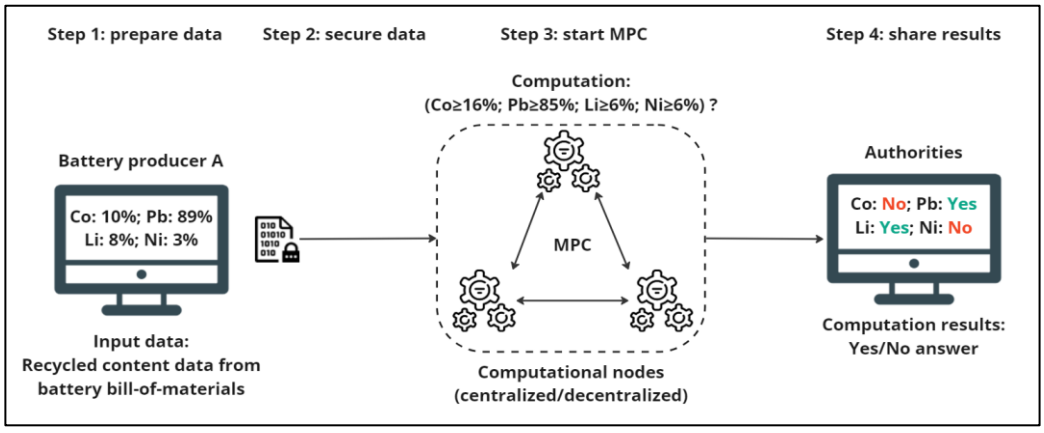

Figure 3: Conceptualization of MPC use for monitoring recycled content in new batteries

In our example, the computation results indicate that battery producer A has not reached the mandatory recycled content target for Cobalt (Co) and Nickel (Ni). Thus, authorities can take further action to ensure that battery producer A (and other battery producers) can fulfill the minimum target mandated by the regulation. It is important to note that authorities only learned that the composition of recycled Cobalt and Nickel is still below the minimum level and nothing else, including the actual percentage of these elements and the complete battery recipes. Thus, using MPC to monitor recycled content can facilitate B2G data sharing and collaboration to generate meaningful insights while respecting the confidentiality of sensitive business data and ultimately creating public value of resource circularity.

4.2.2. Design trade-offs in implementing MPC for CE monitoring

As introduced in Section 3, the underlying computational nodes for executing MPC (see Step 3 in Figure 3) can be deployed in three architectural designs: (1) **the decentralized model** (i.e., computational nodes are placed at the premise of battery producer A and the authorities); (2) **the centralized single cloud model** (i.e., one cloud provider sets up computational nodes); and (3) **the centralized multiple clouds model** (i.e., multiple computational nodes deployed by multiple independent cloud providers). Each design choice of MPC architecture poses design trade-offs regarding resource complexity, security guarantee, trust requirements, and implementation costs. We illustrate these design trade-offs at the bottom layer of Figure 2.

On the one hand, the decentralized model can offer a stronger guarantee as computation is done at the premises of battery producer A and the authorities. The trust requirement in this model is also lower since no third party is involved in the computation process. However, this model requires more effort and implementation costs as battery producer A and the authorities must prepare their computing infrastructure. On the other hand, the centralized single cloud model might reduce the implementation costs and address complexity issues since a third party will deploy computation nodes centrally. However, there is a risk that the security guarantee is compromised, leading to a higher need for trust in the process. The centralized multiple clouds model can be an alternative that balances security guarantees, trust requirements, complexity, and implementation costs. While computing nodes are still deployed centrally, it is deployed by multiple third parties that are independent and unrelated, which offers higher security guarantees and trust requirements than the second model without placing the burden on authorities and battery producer A to deploy the computing server themselves.

5. Discussions, conclusions and outlook

In this ongoing research, we explored the potential of MPC in facilitating B2G data sharing and collaboration for CE monitoring, focusing on a specific context of monitoring recycled content in new batteries. Our initial analysis shows that implementing MPC can address barriers to B2G data sharing and collaboration in CE monitoring, which is challenging due to concerns about the confidentiality and competitiveness of sensitive data owned by businesses. MPC poses a new approach to sharing data by executing joint computation to

provide relevant insights for authorities on regulatory compliance without revealing anything about sensitive battery data provided by battery producers. As a result, authorities can access valuable data that is otherwise difficult to obtain from battery producers due to their reluctance to share commercially sensitive data. At the same time, battery producers can still share relevant data for compliance monitoring while maintaining control and confidentiality, as only computation results are generated. Thus, we argue that MPC can address tensions between public and private actors in the actor layer, particularly between compliance monitoring for circularity and protecting sensitive data. Ultimately, by addressing those tensions, MPC can contribute to realizing resource circularity as a public value in the context of CE monitoring.

Our findings also suggest that it is crucial to consider various design trade-offs when implementing MPC as there are variations in MPC architectures, which might include introducing new entities. The design trade-offs in the infrastructure layer must be assessed in terms of their effects on the willingness of battery producers to participate and whether they contribute to realizing resource circularity as a public value. Likewise, as the various design options for implementing MPC on the technical layer can influence the public value layer, public authorities can establish reasoning about the benefits they see in using MPC for improving their CE monitoring capabilities, given specific technical design choices of MPC.

This ongoing research provides three main contributions. First, we make a theoretical contribution by understanding the potential of MPC (as an emerging technology) in the novel domain of CE monitoring (to contribute to resource circularity) with the framework of [8] as a tool to establish this understanding. This contribution is essential because MPC represents a novel and radical data-sharing approach that underlines the importance of computation results as opposed to the underlying details of data [30]. Second, we contribute to translating the generic MPC architectures to the specific case of CE monitoring in the battery domain. As such, we add a new application domain where MPC can be of potential value next to domains like health [24], finance [25], and crime prevention [26]. This way, we enhance the richness of MPC use cases and how MPC can be relevant in addressing a multitude of societal problems, which can boost its adoption by businesses and public organizations. Third, we demonstrate the capabilities of MPC to support data sharing under conditions of inter-organizational trust and control. In this regard, we illustrate the potential generalizability of our initial findings for other cases in which both conditions are essential to address concerns of businesses when they share their data with other stakeholders like governments.

There are various possible avenues for further exploration and next steps. For instance, our focus in this paper is on monitoring one company, and the next steps can expand this by monitoring all battery producers in one particular country or even at the EU level. This way, we can obtain macro insights on the level of compliance of all producers at the national and EU level. Also, examining various CE monitoring use cases beyond monitoring recycled content in new batteries can be interesting. This would include cases like upstream data aggregation for battery carbon footprint declarations or performance readiness in achieving the CE transition target. Such cases represent a different public value, which involves more actors and requires a different technical architecture. Taking this path as a

next step will enrich our understanding of the dynamics of B2G data sharing and collaboration in the context of CE monitoring.

Other potential avenues can be to expand the infrastructure layer further by incorporating various technical solutions like a centralized platform, data spaces, or other distributed data sharing architectures such as blockchain-based architectures. We can even explore the relevance of other PETs beyond MPC, like homomorphic encryption, differential privacy, federated learning, and zero-knowledge proof in the context of CE monitoring. By making the architecture of the complex multi-actor data sharing environment explicit, we can further examine the link and associated trade-offs between various technical solutions and MPC architectures (and even different PETs).

Acknowledgments

This research was partially funded by the DATAPIPE project, which has received funding from the European Union's Technical Support Instrument (TSI) programme under grant agreement No 101094495. Ideas and opinions expressed by the authors do not necessarily represent those of all partners.

References

[1] Ellen MacArthur Foundation, The New Plastics Economy: Rethinking the future of plastics, 2016. URL: https://ellenmacarthurfoundation.org/the-new-plastics-economy-rethinking-the-future-of-plastics

[2] M. Geissdoerfer, P. Savaget, N. M. P. Bocken, E. J. Hultink, The Circular Economy – A new sustainability paradigm?, Journal of Cleaner Production (2017), 143, 757–768.

[3] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Green Deal, COM(2019) 640 final, 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0640&from=EN

[4] A. Kofos, J. Ubacht, B. Rukanova, G. Korevaar, N. Kouwenhoven, Y.-H. Tan, Circular economy visibility evaluation framework, Journal of Responsible Technology (2022), 10, 100026.

[5] B. Rukanova, Y.-H. Tan, R. Hamerlinck, F. Heijmann, and J. Ubacht, Digital Infrastructures for Governance of Circular Economy: A Research Agenda, in: EGOV-CeDEM-EPart-*, 2021, pp. 191–198.

[6] M. Jarke, B. Otto, S. Ram, Data Sovereignty and Data Space Ecosystems, Business & Information Systems Engineering (2019), 61(5), 549–550.

[7] F. Lauf, S. Scheider, J. Bartsch, P. Herrmann, M. Radic, M. Rebbert, A. T. Nemat, C. S. Langdon, R. Konrad, A. Sunyaev, S. Meister, Linking Data Sovereignty and Data Economy: Arising Areas of Tension, in: Wirtschaftsinformatik 2022 Proceedings, 2022. URL: https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/19

[8] B. Rukanova, S. van Engelenburg, J. Ubacht, Y.-H. Tan, M. Geurts, M. Sies, M. Molenhuis, M. Slegt, D. van Dijk, Public value creation through voluntary business to government

information sharing enabled by digital infrastructure innovations: A framework for analysis, Government Information Quarterly (2023), 40(2), 101786. doi: 10.1016/j.giq.2022.101786

[9] I. Susha, B. Rukanova, A. Zuiderwijk, J. R. Gil-Garcia, M. Gasco Hernandez, Achieving voluntary data sharing in cross sector partnerships: Three partnership models, Information and Organization (2023), 33(1), 100448.

[10] J. J. Borking, C. Raab, Laws, PETs and other technologies for privacy protection, Journal of Information, Law and Technology (2001), 1, 1–14.

[11] J. Heurix, P. Zimmermann, T. Neubauer, S. Fenz, A taxonomy for privacy enhancing technologies, Computers & Security (2015), 53, 1–17.

[12] J. I. Choi, K. R. B. Butler, Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities, Security and Communication Networks (2019), 2019, 1368905.

[13] A. C. Yao, How to generate and exchange secrets, in: 27th Annual Symposium on Foundations of Computer Science (Sfcs 1986), 1986, pp. 162–167. doi:10.1109/SFCS.1986.25.

[14] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, Y. Tan, Secure Multi-Party Computation: Theory, practice and applications, Information Sciences (2019), 476, 357–372.

[15] W. Agahari, H. Ofe, M. de Reuver, It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing, Electronic Markets (2022), 1–26.

[16] R. Zeiss, A. Ixmeier, J. Recker, J. Kranz, Mobilising information systems scholarship for a circular economy: Review, synthesis, and directions for future research, Information Systems Journal (2021), 31(1), 148–183.

[17] A. Bestavros, A. Lapets, M. Varia. User-centric distributed solutions for privacy-preserving analytics, Communications of the ACM (2017), 60(2), 37–39.

[18] A. Lapets, F. Jansen, K. D. Albab, R. Issa, L. Qin, M. Varia, A. Bestavros, Accessible Privacy-Preserving Web-Based Data Analysis for Assessing and Addressing Economic Inequalities, in: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies, 2018, pp. 1–5. doi:10.1145/3209811.3212701.

[19] European Parliament and the Council of the European Union, Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC, 2023. URL: https://eur-lex.europa.eu/eli/reg/2023/1542/oj

[20] B. Rukanova, J. Ubacht, B. Turner, Y.-H. Tan, J. Schmid, E. Rietveld, and W. Hofman, A Framework for Understanding Circular Economy Monitoring: Insights from the Automotive Industry, in: Proceedings of the 24th Annual International Conference on Digital Government Research, 2023, pp. 544–555. doi:10.1145/3598469.3598530.

[21] A. C. Yao, Protocols for secure computations, in: 23rd Annual Symposium on Foundations of Computer Science (Sfcs 1982), 1982, pp. 160-164. doi: 10.1109/SFCS.1982.38.

[22] W. Agahari, R. Dolci, M. de Reuver, Business model implications of privacy-preserving technologies in data marketplaces: The case of multi-party computation, ECIS 2021 Research Papers, 2021. URL: https://aisel.aisnet.org/ecis2021_rp/59
[23] G. Alter, B. H. Falk, S. Lu, R. Ostrovsky, Computing Statistics from Private Data, Data Science Journal (2018), 17(0), Article 0. doi:10.5334/dsj-2018-031.
[24] G. Spini, E. Mancini, T. Attema, M. Abspoel, J. de Gier, S. Fehr, T. Veugen, M. van Heesch, D. Worm, A. De Luca, R. Cramer, P. M. A. Sloot, New Approach to Privacy-Preserving Clinical Decision Support Systems for HIV Treatment, Journal of Medical Systems (2022), 46(12), 84.
[25] A. Sangers, M. van Heesch, T. Attema, T. Veugen, M. Wiggerman, J. Veldsink, O. Bloemen, and D. Worm, Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection, in: I. Goldberg and T. Moore (Eds.), Financial Cryptography and Data Security, Springer International Publishing, 2019, pp. 605–623. doi:10.1007/978-3-030-32101-7_35.
[26] A. Rajan, L. Qin, D. W. Archer, D. Boneh, T. Lepoint, M. Varia, Callisto: A Cryptographic Approach to Detecting Serial Perpetrators of Sexual Misconduct, in: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies, 2018, pp. 1–4. doi:10.1145/3209811.3212699.
[27] OECD, Emerging privacy-enhancing technologies: Current regulatory and policy approaches (No. 351), 2023. URL: https://www.oecd-ilibrary.org/content/paper/bf121be4-en
[28] World Economic Forum, Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows, 2023. URL: https://www.weforum.org/whitepapers/data-free-flow-with-trust-overcoming-barriers-to-cross-border-data-flows/
[29] Gartner, Gartner Says Digital Ethics is at the Peak of Inflated Expectations in the 2021 Gartner Hype Cycle for Privacy, 2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-09-30-gartner-says-digital-ethics-is-at-the-peak-of-inflate
[30] M. W. Van Alstyne, A. Lenart. Using data and respecting users, Communications of the ACM (2020), 63(11), 28–30.