Bourgeus, August; Vandercruysse, Laurens (2024): Reinvigorating Consent: Exploring New Paradigms for Privacy and Data Sharing. In: Proceedings of the 22nd European Conference on Computer-Supported Cooperative Work: The International Venue on Practice-centered Computing on the Design of Cooperation Technologies - Exploratory papers, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591), DOI: 10.48340/ecscw2024_ep08

Reinvigorating Consent: Exploring New Paradigms for Privacy and Data Sharing

August Bourgeus[a] & Laurens Vandercruysse[b]
[a]*imec-SMIT, Vrije Universiteit Brussel. Pleinlaan 9 – 1050 Brussels, Belgium*
[b]*Department of Applied Economics, Vrije Universiteit Brussel. Pleinlaan 5 – 1050 Brussels, Belgium*
august.bourgeus@vub.be

Abstract. This paper examines the inadequacies of the notice-and-consent paradigm in personal data processing, which fails to distribute data economy benefits fairly and degrades data privacy. We explore alternative frameworks like group privacy and contextual integrity that propose a communal and contextual approach to data privacy decisions. Critiquing the consent model for overlooking data externalities and the influence of cognitive biases, we argue against the de facto overreliance on individual consent under the General Data Protection Regulation (GDPR). Instead, we advocate for a revised model that integrates group privacy strategies and contextual norms with strategic, selective deployment of active consent. This proposed approach emphasises the balance between individual autonomy, group interests, and communal privacy norms, aiming to empower users with meaningful engagement in consent decisions. We discuss the potential of this model to enhance data privacy in the context of the evolving European Union data spaces and the personal data market.

Copyright 2024 held by Authors, DOI 10.48340/ecscw2024_ep08
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, contact the Authors.

Introduction

In this paper, we explore the evolving landscape of data privacy through the lens of the notice-and-consent paradigm, a foundational concept in data protection that requires users to be informed about how their data will be used, and to consent to these practices explicitly, e.g. by ticking a box. Despite being widely adopted, this paradigm has faced significant criticism for failing to ensure genuine user understanding and control, which is exacerbated by the complexity of modern data ecosystems. It has long been claimed that the notice-and-consent paradigm for personal data processing has failed to produce a balanced distribution of data economy benefits, leading to further eroding data privacy[1] levels. As a result, alternative normative theories for governing access to personal data have been developed. Group privacy (Floridi, 2017) and contextual integrity (Nissenbaum, 2009) conceptualise data privacy, and the decision as to whether or not personal data processing is desirable, as something group-based/communal. Consent is often sketched as a pragmatic, though misguided, attempt to solve a collective action problem by attributing individual rights to citizens (Sloan & Warner, 2013). Further criticisms include that the consent paradigm makes abstraction of data externalities (J. P. Choi et al., 2019) as well as the fact that cognitive biases and limitations impede rational decision-making in the data context (Kröger et al., 2021).

Article 4(11) of the General Data Protection Regulation defines consent as being actively, freely given, specific, informed, and unambiguous (The European Parliament and the Council of the European Union, 2016). However, the bar for consent to be meaningful is arguably higher and requires consent to be significant. It is possible for consent to be valid under GDPR sensu stricto, though not meaningful per se. Issues such as information asymmetries and the growing complexity of data ecosystems make privacy self-management impractical. While we agree that consent has its limits, we argue here that the overreliance on consent as a legal basis for processing personal data gets in the way of meaningful consent.

In contrast to scholars propagating doing away with notice-and-consent in its entirety, we think employing a combination of group logics - and institutions - for managing privacy in combination with targeted use of notice-and-consent can produce better outcomes for citizens. This model should incorporate individual autonomy, shared privacy norms and collaborative governance to truly empower users, allowing them to focus on important consent decisions for meaningful engagement. Taking into consideration the deployment of the various data spaces

[1] We will focus on data privacy as privacy and personal data protection are two distinct rights (González Fuster, 2014).

at the European Union level and the emergence of personal data markets, an operationalisation of the combination of these ideas imposes itself.

Our contribution lies in demonstrating the limitations of the current paradigm, while proposing a novel governance framework that balances individual consent with collective privacy considerations, and, finally, providing a starting point for the practical implementation of this model.

Background

The Problem with the Consent Paradigm

Over the past decades, privacy self-management (by consent) has been a central tenet of EU data privacy legislation. It is worth noting that while there are alternative legal bases for processing personal data, consent has emerged as the most popular one, with tech companies promoting its use. Although privacy self-management may seem to promote values such as liberalism and individualism, it often fails to succeed in empowering individuals for three main reasons.

First, existing obstacles to informed and rational privacy choices result from human limitations, bounded rationality and modern data processing (Acquisti et al., 2020; Kröger et al., 2021). As data ecosystems grow in complexity, expecting individuals to manage their privacy settings across a myriad of platforms becomes unrealistic. Consent is repeatedly requested and at inappropriate times, leading to a decrease in active user participation and consent rates (H. Choi et al., 2018). Research indicates that data subjects often lack sufficient knowledge to make informed decisions about disclosing personal information (Acquisti et al., 2020; Park, 2013; Weinshel et al., 2019). The explanations provided in privacy policies are insufficient for users to comprehend the outcomes of their consent. Their overwhelming length and complexity (Kröger et al., 2021; Luger & Rodden, 2014; Obar & Oeldorf-Hirsch, 2020), leads to passive acceptance of privacy terms and conditions rather than informed decision-making. This causes many users to inadvertently give permissions without comprehending the full implications of their choices, including aggregation and inference risks. Crabtree et al. (2017) who investigated privacy in a networked world, claim concerns center on maintaining control over personal and others' data privacy, managing unauthorized intrusions from the online world, and navigating the impact of networked interactions on personal relationships. The consequences for individuals can be challenging to trace, as they may occur gradually or over time due to multiple data transactions (Lazaro & Le Métayer, 2015; Solove, 2013).

Second, modern data collection and processing creates significant information asymmetries. These asymmetries inhibit data subjects from making informed

privacy choices due to an unfair distribution of opportunities in terms of understanding, knowledge, prediction, and risk assessment (Mantalero, 2014). Information asymmetries mean that access to relevant information is different for different actors. These asymmetries are exacerbated by advancements in information technology that make data practices less visible, making individuals unsure about how much information they share (Acquisti et al., 2013). Information asymmetries become more complex with the growth of online services, policy updates, and users' tendency to disregard these agreements (Bashir et al., 2015).

Third, the current individual-centric consent model fails to address the communal impacts of data sharing and privacy decisions (Fairfield et al., 2015). Data externalities are particularly interesting here, as highlighted by Choi, Jeon, and Kim (2018), who illustrate the discrepancy between individual consent and communal outcomes. Their research demonstrates that even with individual consent, collective privacy can be compromised beyond what is socially optimal due to information externalities and user coordination failures. Moreover, Lovato et al. (2022) emphasise the inadequacy of traditional consent frameworks within digital environments, where a single user's consent can inadvertently expose connected individuals' data (Fairfield et al., 2015; Lovato et al., 2022). When a group of people shares a feature or a combination of features, it is possible to make inferences about them, which is referred to as inferential privacy (Loi & Christen, 2020). Additionally, individual consent decisions may not lead to optimal social outcomes, with privacy risks being both minor and scattered yet significant over time.

While consents under these three reasons could still be formally recorded as valid under GDPR, it is evident that these consents are hardly meaningful.

Alternative Paradigms

Various theories have advocated for an improved personal data ecosystem beyond the privacy self-management model. In what follows, we will introduce theories that could facilitate meaningful consent and go beyond the individual, like contextual integrity (Nissenbaum, 2009) and group privacy (Floridi, 2017; Taylor et al., 2017).

Nissenbaum's privacy as Contextual Integrity (CI) emphasises the importance of the appropriateness of information flows rather than solely relying on individual preferences. In CI, privacy is evaluated based on the contextual alignment of information sharing, where specific spheres, encompassing contexts and intended purposes, establish the guidelines for when and how different actors can access data. CI serves as a critical departure from traditional privacy approaches, offering a robust foundation for evaluating information practices based on the collective understanding and norms of a given context. CI has

already been applied in various contexts and formats. Recently, Kumar et al. (2024) defined a roadmap for applying the CI framework in qualitative privacy research in the CSCW field.

Nissenbaum and Solove advocate that privacy and consent decisions must be contextually grounded, recognising that shared perceptions within different environments significantly influence privacy expectations (Nissenbaum, 2019; Solove, 2023). During a conference, a visitor may agree to have their photo taken and shared within the community but may not want the same photo to be used for commercial purposes. This approach underscores that privacy norms and consent mechanisms should be derived from the collective situational awareness and agreed-upon standards within distinct contexts, rather than the isolated preferences of individuals. Multiple studies support this view, illustrating that privacy expectations inherently vary in line with the situational parameters defined by CI (Apthorpe et al., 2018; Martin & Nissenbaum, 2015; Zhang et al., 2022).

Networked privacy (Lampinen, 2015) and group privacy (Floridi, 2017; Taylor et al., 2017) pave the way for alternative models. (Floridi, 2017) argued that groups may have privacy rights that are not reducible to those of their individual members. For example, activist or political groups must protect their strategies, communications, and identities. Exposing such information can threaten their goals and safety, highlighting a collective privacy right tied to their operational integrity and advocacy efforts (Jia & Baumer, 2022; Suh et al., 2018). The focus on group privacy advances the discussion by advocating for the internalisation of information externalities discussed in the previous section and promoting collective decision-making, thereby challenging the traditional individualistic approach. This shift towards group privacy involves developing mechanisms that empower groups to determine their data sharing and privacy standards rather than solely relying on individuals.

The principles of CI and group privacy might be practically facilitated by establishing data intermediaries (von Ditfurth & Lienemann, 2022). Data collective intermediaries like data cooperatives allow their members to have more control over their individual data and to use this data in the interest of their community or the commons (Bietti et al., 2021). Such a system should align with the specific values that a user embodies, and relevant stakeholders should be included in the ownership model. Another example is a data collaborative (Susha et al., 2017), which is a partnership between a private sector entity and a public sector, civil society, or academia entity to use private data for the public good and benefit of society.

CI and group privacy propose interesting perspectives, though they fall short of operationalisation. Seeing the developments at the EU level, there is an imminent need for a revised governance framework for personal data processing, taking into account the learnings from the limitations of consent and the merits of a

contextual group-based view on privacy, while at the same time respecting the individual autonomy of the citizen in deciding what happens with their data and to participate in the data economy.

In what follows, we will present how we think such a model could look like – we will be basing some of the conjectures on the Solid-wave in Flanders, where the government is investing in the development of a personal data ecosystem where citizens exercise control over personal data via a decentralised container, based on the Solid specification.

A Revised Model

We propose a revised model that, while retaining the foundation of individual consent, is significantly enhanced by incorporating contextual cues and group norms into the personal data governance ecosystem. The revised model could be described as a type of semi-automated consent model (Gomer et al., 2014). It aims to address the dynamic nature of privacy expectations by enabling individuals to set consent preferences that are sensitive to different contexts and align with the collective norms of groups they belong to or identify with.

Following CI, it could be acceptable for data controllers to obtain consent only once for various operations as long as they are within the reasonable expectations of the data subject. The GDPR, in Article 6(4), permits the continued processing of personal data for purposes that align with the original collection purpose without requiring new consent. Such expectations can be derived by applying the contextual integrity framework. Adding these expectations to the current paradigm would incorporate both individual sovereignty and automated decisions based on individual preferences and communal values. The revised model aligns with the EU's efforts on data spaces and data strategy (Susha et al., 2017). We maintain a role for active consent, but only in important privacy decisions. The level of importance attached to the consent decision could vary based on the context, the sensitivity of the information, and the potential consequences of information misuse. To illustrate, people or their caregivers may desire greater authority over the sharing of their medical data because such information is personal and carries the risk of being misused. Likewise, when seeking a loan, a person may require more active consent due to the wide variance in what information flow is deemed acceptable and the absence of community norms.

Group privacy theory argues for data privacy rights for groups that are distinct from those at the individual level. In practice, managing group privacy will necessitate setting up institutions for deliberation and decision-making at the group level. Also, at this level, CI could inform deriving group-based norms to limit the necessary engagement of individual citizens while allowing them to 'vote' in more contested group consent matters.

The implementation of a semi-automated consent system could potentially enable meaningful consent. By using CI and group privacy, we can derive acceptable information flows that data subjects could automatically consent to, but this is not fully covered. Difficult or ambiguous information flows still require human oversight. Semi-automated consent mechanisms or intermediaries can work as agents for the data subject to manage their daily consent and privacy decisions.

Following the enactment of the Data Governance Act (DGA), there has been a notable increase in the advocacy for the deployment of data intermediaries. Janssen & Singh (2022) define data intermediaries as entities that "serve as mediators between those wishing to make their data available and those seeking to leverage such data." Examples of such intermediaries include clearinghouses, service catalogues, and data cleaners. As an example, the Flemish government has established a data utility company, a public-private entity, to foster data-sharing ecosystems. They offer services such as infrastructure provision, ecosystem auditing, and standardisation (Digitaal Vlaanderen, n.d.). Such intermediaries could also act as consent intermediaries (Lehtiniemi & Kortesniemi, 2017). Lehtiniemi & Kortesniemi (2017, pp. 10) argue that: “intermediaries could be leveraged to develop tools to mitigate obstacles, helping people understand the decisions they make, better evaluate their consequences, and simplify the decisions themselves.”

A technology of interest that has recently received much traction is Solid (Sambra et al., 2016). Solid allows individuals to store their data in personal online data stores (pods) and manage access through granular consent tools. Integrating this technology with the revised consent model facilitates a more nuanced consent process, where individuals can automate their privacy preferences based on predefined contexts and community standards. Using Solid to obtain consent has been researched by (Florea & Esteves, 2023), who investigated a technical and legal approach to consent. We argue that coding privacy norms or rules into a system as access control policies forms a promising approach, worthy of further exploration and research. This approach not only streamlines consent management for data subjects but also aligns with broader social and ethical norms, reflecting the shift towards more informed and context-aware data practices. Solid as a web standard/ interoperable technology should also facilitate setting up data collaboratives, etc., as lack of interoperability is one of the premier hindrances for these institutions to scale (Susha, 2020). In Flanders, the northern part of Belgium, the government has funded a research project to investigate the challenges and opportunities of Solid-enabled Personal Data Store (PDS) ecosystems to improve information flows while safeguarding privacy for citizens. The government-funded PDS-based data ecosystem is attempting to make this work with an eye on allowing citizens to play an active role. Integrating our proposed adaptations could facilitate the shift towards a more

inclusive, transparent, and user-controlled data environment. These developments could facilitate the shift to a semi-automated consent model.

In the revised model, a data subject could manage preferences via a dashboard that can be shared with a group. A primary layer of safeguards can be applied for common, socially acceptable information flows, supplemented with a top layer of personalised preferences.

Conclusion & Future Research

In conclusion, the revised model represents a transformative step in personal data governance, combining individual preferences with the nuances of context and group norms. The integration of Solid and the role of data intermediaries illustrate a practical, user-centred approach that aligns with legislative standards like the GDPR and DGA. As long as individuals' privacy choices are falsely painted and perceived as expressions of their freedom and autonomy, there will be little resistance to the status quo. However, future research should focus on several tracks to refine and validate this semi-automated consent model.

First, communal privacy norms need to be derived, which can be programmed into systems as policies. Such policies can reserve active consent for specific instances, but requiring too much effort will adversely affect empowerment. Hence, research on which consents can be automated is necessary. Besides, research is needed to investigate whether the principles and applications of CI, typically considered at the individual level, need to be adapted when these intermediaries are involved, reflecting the potentially different dynamics and privacy concerns at play.

Second, while data intermediaries are the subject of extensive research (Bietti et al., 2021; Janssen & Singh, 2022; Susha et al., 2017; von Ditfurth & Lienemann, 2022), they remain sparsely implemented in real-world settings. Exploring the practical manifestations of novel ecosystems built around these intermediaries is crucial. The concept of data intermediaries often remains obscure to companies and data subjects alike, underscoring the need for research into their adoption and assessing how effectively they balance individual and collective governance approaches. Their development and implementation could ease some of the group privacy concerns while catering to demands for norm-based unburdening of data subjects. However, research is needed on how these group institutions should be managed.

Third, further development of standards, ontologies, and integration of technologies like Solid is needed. Interoperability is key to making the system work for data subjects and avoiding a winner-take-all network effect that leads to insurmountable power asymmetries in the data ecosystem.

Last, exploring a semi-automated consent system's interface and user journey is of considerable importance. Future research should focus on ensuring the remaining consents in the data governance models are genuinely meaningful. This entails investigating strategies for enhancing user understanding and consent quality - what makes consent meaningful, and how can this be achieved? Addressing dark patterns that mislead or manipulate users into providing consent unwittingly and increasing literacy is another vital area. Additionally, research should explore the mechanisms for enhanced enforcement of consent regulations to ensure user decisions are respected and protected.

Although revised consent models provide enhanced protection against tracking and surveillance, they can also introduce new privacy risks and complexities, such as the involvement of additional third parties and the need for disclosing more information. Additionally, these systems require some level of understanding for proper selection and operation, which is something to consider when designing such systems.

Acknowledgments

This research was supported by SolidLab Vlaanderen (Flemish Government, EWI and RRF project VV023/10)

References

Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15 seconds: The limits of privacy transparency and control. *IEEE Security and Privacy*, *11*(4), 72–74. https://doi.org/10.1109/MSP.2013.86

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, *30*(4), 736–758. https://doi.org/10.1002/jcpy.1191

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(2), 1–23. https://doi.org/10.1145/3214262

Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1–10. https://doi.org/10.1002/pra2.2015.145052010043

Bietti, E., Etxeberria, A., Mannan, M., & ... (2021). Data Cooperatives in Europe: a legal and empirical investigation. *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*. https://openfuture.eu/wp-content/uploads/2022/03/Data_Cooperatives_Europe-group2.pdf

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Governance of Platform Markets in the "Big Data" Era. *Journal of Public Economics*, *173*, 113–124.

Crabtree, A., Tolmie, P., & Knight, W. (2017). Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work: CSCW: An International Journal*, *26*(4–6), 453–488. https://doi.org/10.1007/s10606-017-9276-y

Digitaal Vlaanderen. (n.d.). *The Flemish Data Utility Company*. Retrieved February 25, 2024, from https://www.vlaanderen.be/digitaal-vlaanderen/athumi-het-vlaams-datanutsbedrijf/the-flemish-data-utility-company

Fairfield, J. A. T., Engel, C., Regan, P., Hirsch, D., Hoofnagle, C. J., Hartzog, W., Bambauer, J., Froomkin, M., Seaman, C., Hu, M., Kaminski, M., Candeub, A., Jost, J., & Lastowka, G. (2015). Privacy as a public good. *Duke Law Journal*, *65*, 385.

Florea, M., & Esteves, B. (2023). Is Automated Consent in Solid GDPR-Compliant? An Approach for Obtaining Valid Consent with the Solid Protocol. *Information (Switzerland)*, *14*(12), 631. https://doi.org/10.3390/info14120631

Floridi, L. (2017). Group Privacy: A Defence and an Interpretation. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group Privacy* (pp. 83–100). Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_5

Gomer, R., Schraefel, M. C., & Gerding, E. (2014). Consenting agents: Semi-autonomous interactions for ubiquitous consent. *UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 653–658. https://doi.org/10.1145/2638728.2641682

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Vol. 16). Springer International Publishing. https://doi.org/10.1007/978-3-319-05023-2

Janssen, H., & Singh, J. (2022). Data intermediary. *Internet Policy Review*, *11*(1), 1–9. https://doi.org/10.14763/2022.1.1644

Jia, H., & Baumer, E. P. S. (2022). Birds of a feather: Collective privacy of online social activist groups. *Computers & Security*, *115*, 102614. https://doi.org/10.1016/j.cose.2022.102614

Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). The myth of individual control: Mapping the limitations of privacy self-management. *SSRN Electronic Journal*, *...*(...), 106705. https://doi.org/10.2139/ssrn.3881776

Kumar, P., Zimmer, M., & Vitak, J. (2024). A Roadmap for Applying the Contextual Integrity Framework in Qualitative Privacy Research. *Proceedings of the ACM on Human-Computer Interaction*, *8*(April). https://doi.org/10.1145/3653710

Lampinen, A. (2015). Networked privacy beyond the individual: Four perspectives to sharing. *Critical Alternatives - Proceedings of the 5th Decennial Aarhus Conference, CA 2015*, *October 2015*, 25–28. https://doi.org/10.7146/aahcc.v1i1.21300

Lazaro, C., & Le Métayer, D. (2015). Control over personal data: True remedy or fairytale? *SCRIPTed*, *12*(1). https://doi.org/10.2966/scrip.120115.3

Lehtiniemi, T., & Kortesniemi, Y. (2017). Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data and Society*, *4*(2), 1–11. https://doi.org/10.1177/2053951717721935

Loi, M., & Christen, M. (2020). Two Concepts of Group Privacy. *Philosophy and Technology*, *33*(2), 207–224. https://doi.org/10.1007/s13347-019-00351-0

Lovato, J. L., Allard, A., Harp, R., Onaolapo, J., & Hébert-Dufresne, L. (2022). Limits of Individual Consent and Models of Distributed Consent in Online Social Networks. *ACM International Conference Proceeding Series*, 2251–2262. https://doi.org/10.1145/3531146.3534640

Luger, E., & Rodden, T. (2014). The value of consent: Discussions with designers of ubiquitous computing systems. *2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014*, 388–393. https://doi.org/10.1109/PerComW.2014.6815237

Mantalero, A. (2014). Social control, transparency, and participation in the big data world. *Journal of Internet Law*, *17(10)*, 23–29.

Martin, K. E., & Nissenbaum, H. (2015). Measuring Privacy: Using Context to Expose Confounding Variables. *SSRN Electronic Journal*, *January*. https://doi.org/10.2139/ssrn.2709584

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law*, *20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information Communication and Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Sambra, A. V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., & Berners-Lee, T. (2016). *Solid: A Platform for Decentralized Social Applications Based on Linked Data*.

Sloan, R. H., & Warner, R. (2013). Beyond Notice and Choice: Privacy, Norms, and Consent. *SSRN Electronic Journal*, *January*. https://doi.org/10.2139/ssrn.2239099

Solove, D. J. (2013). *INTRODUCTION : PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA Author (s): Daniel J . Solove Source : Harvard Law Review , MAY 2013 , Vol . 126 , No . 7 (MAY 2013), pp . 1880-1903 Published by : The Harvard Law Review Association Stable URL : https://*. *126*(7), 1880–1903. https://doi.org/https://ssrn.com/abstract=2171018

Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *SSRN Electronic Journal*, *118*(4), 1081–1138. https://doi.org/10.2139/ssrn.4322198

Suh, J. J., Metzger, M. J., Reid, S. A., & El Abbadi, A. (2018). Distinguishing group privacy from personal privacy: The effect of group inference technologies on privacy perceptions and behaviors. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW). https://doi.org/10.1145/3274437

Susha, I. (2020). Establishing and implementing data collaborations for public good: A critical factor analysis to scale up the practice. *Information Polity*, *25*(1), 3–24. https://doi.org/10.3233/IP-180117

Susha, I., Janssen, M., & Verhulst, S. (2017). Data collaboratives as a new frontier of cross-sector partnerships in the age of open data: Taxonomy development. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2017-Janua*, 2691–2700. https://doi.org/10.24251/hicss.2017.325

Taylor, L., Floridi, L., & van der Sloot, B. (2017). *Group Privacy: New Challenges of Data Technologies*. https://doi.org/10.2966/scrip.140117.131

The European Parliament and the Council of the European Union. (2016). *GDPR - 32016R0679 - EN - EUR-Lex*. EUR-Lex. http://data.europa.eu/eli/reg/2016/679

von Ditfurth, L., & Lienemann, G. (2022). The Data Governance Act: – Promoting or Restricting Data Intermediaries? *Competition and Regulation in Network Industries*, *23*(4), 270–295. https://doi.org/10.1177/17835917221141324

Weinshel, B., Wei, M., Mondal, M., Choi, E., Shan, S., Dolin, C., Mazurek, M. L., & Ur, B. (2019). Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing. *Proceedings of the ACM Conference on Computer and Communications Security*, 149–166. https://doi.org/10.1145/3319535.3363200

Zhang, S., Shvartzshnaider, Y., Feng, Y., Nissenbaum, H., & Sadeh, N. (2022). Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates. In *ACM International Conference Proceeding Series* (Vol. 1, Issue 1). Association for Computing Machinery. https://doi.org/10.1145/3531146.3533222