ADVANCES IN KNOWLEDGE ORGANIZATION
Proceedings of International ISKO Conference - ISSN: 0938-5495 - 2026 - São Paulo

Data Colonialism and the Myth of Consent: Toward Informational Self-Determination and Digital Justice

Jonas Ferrigolo Melo

CITCEM, Portugal

Moisés Rockembach

CEIS20 / University of Porto, Portugal

Abstract

In the contemporary digital economy, accepting privacy policies has become a daily gesture that is rarely questioned, even though it lies at the heart of the massive exploitation of personal data. This study investigates the effectiveness of informed consent, questioning whether it guarantees autonomy or if it is merely a formality in the era of datafication. The objective was to analyze the myth of consent from the perspective of data colonialism, highlighting how digital platform interfaces function as instruments of informational expropriation. Using the Quivy and Van Campenhoudt model, the study combined a systematic review with empirical research involving 237 participants on an experimental website. The results reveal the myth of consent: although 97% of respondents expressed great concern for their data, 87.8% accepted the terms immediately. Only 5.5% consulted the privacy policy, spending just 29 seconds on a document that would require approximately 25 minutes to read. The study concludes that, as currently implemented, informed consent has significant limitations in ensuring informational self-determination, often functioning as a mechanism to legitimize data extraction within the context of surveillance capitalism and data colonialism.

1.0 Introduction

Contemporary society is experiencing a paradigmatic transformation driven by datafication, a process through which an ever-broader range of human life is converted into quantifiable, economically exploitable data. This phenomenon constitutes a new phase of capitalism, marked by the intensive exploitation of behavioral information produced by individuals in their interactions with digital technologies (Zuboff 2019; Srnicek 2017; Cohen 2018).

Within this economic model, digital platforms continuously capture behavioral traces, transforming everyday activities into analyzable, monetizable data, enabling the construction of predictive systems capable of anticipating and influencing individual decisions (Zuboff 2019; West 2019). As a consequence, the platformization of society reorganizes practices of consumption and communication and establishes new asymmetries of power (Hayashi et al. 2025) between individuals, technological

corporations, and states. In this context, processes traditionally associated with Knowledge Organization, such as classification, indexing, metadata production, and cataloguing, become central components of the data economy, since they structure how information is represented, retrieved, categorized, and operationalized within algorithmic systems. As Bair (2005) argues, indexers have an ethical responsibility to maintain honesty and accuracy in the representation of resources, avoiding distortions caused by careless or minimal cataloguing. In the context of datafication, these representational practices are no longer merely technical procedures, but sociotechnical mechanisms that shape visibility, knowledge production, and informational power.

To better understand the depth of these transformations, the concept of data colonialism has been proposed to describe the systematic appropriation of human life in the form of data, reproducing historical logics of domination associated with colonialism (Couldry and Mejias 2019; Thatcher et al. 2016; Costa and Melo 2022). Analogous to historical colonialism, data colonialism transforms social experience into a resource for the digital economy.

In this context, Moura (2024, 515) argues that classification systems and algorithmic codes are not neutral; rather, they often incorporate what is described as a colonial "narcissistic pact," which silences differences and reinforces hegemonic regulatory norms. The apparent universal neutrality of these systems frequently conceals the political economy of knowledge production and its effects on the hierarchy of subjects. Thus, datafication operates as a technical process and also as a political and economic mechanism that reorganizes relations of power and dependency on a global scale (Kwet 2019; Mumford 2022).

This phenomenon is intensified by the actions of large technological corporations (Big Techs), which control digital infrastructures and data ecosystems on a planetary scale (Couldry and Mejias 2019). The result is the consolidation of a regime of accumulation based on the continuous exploitation of human experience, often described as surveillance capitalism (Zuboff 2019).

At the center of this extractivist architecture lies informed consent, adopted by legislation such as the European GDPR and the Brazilian LGPD, as the foundation for the autonomy of data subjects. In practice, however, this mechanism is often reduced to a formal procedure marked by informational asymmetries, legal complexity, and manipulative interfaces (Obar and Oeldorf-Hirsch 2020; Utz et al. 2019).

The so-called "myth of consent" refers to the situation in which users accept Terms of Service and Privacy Policies automatically, without reading or understanding them. Individuals are confronted with interfaces that offer limited choices, frequently structured as "accept or abandon the service," which generates coercive or structurally induced consent (Degeling et al. 2018; Schaub et al. 2015). In this scenario, informational autonomy becomes a legal fiction, while data extraction remains widely naturalized.

In this context, this article analyzes the myth of consent from the perspective of data colonialism, investigating user behavior and the architecture of consent managers on

websites to demonstrate the limitations of the current informed consent model. Furthermore, it proposes a critical and decolonial reflection on possible paths toward the construction of a model of self-determination and digital justice capable of returning to individuals greater control over their datafied existences.

2.0 Methods

The investigation was structured based on the methodological model proposed by Quivy and Van Campenhoudt (1992), which organizes the scientific process into three fundamental acts: rupture, construction, and verification. This model was adopted because it allows a systematic and reflexive approach to the research problem, promoting the articulation between theoretical grounding, empirical analysis, and the validation of results.

The rupture stage aimed to define the research problem and break with superficial interpretations regarding digital consent. To this end, initial research questions were formulated regarding user behavior related to privacy policies and consent managers, such as whether individuals actually read privacy policies, whether they understand the data being collected, and whether the consent provided is unequivocal. Within this stage, a systematic literature review was conducted using scientific articles indexed in the Web of Science and Scopus databases to identify the main theoretical debates on data colonialism, surveillance capitalism, and digital governance. This review enabled the construction of the investigation's conceptual framework, grounded in the work of Couldry and Mejias (2019), Zuboff (2019), Kwet (2019), and Mumford (2022).

The construction stage involved the first contact with the empirical objects of the investigation. Consent managers and privacy policies from widely accessed websites across different geographical contexts were analyzed; from this analysis, information was extracted to compose the verification stage.

The verification stage consisted of developing data-collection instruments to analyze user behavior when interacting with a simulated consent system. To empirically investigate the dynamics of informed consent in digital environments, an experimental consent manager integrated into a website specifically designed for this investigation was developed. This digital environment simulated an everyday interaction with online platforms, allowing the observation of participants' real behavior when faced with a typical mechanism for collecting consent to the processing of personal data.

The website was structured as a controlled environment for behavioral experimentation, in which participants were exposed to a consent manager without knowing that their behaviors were being monitored. To record the interaction in detail, the Hotjar software was used, allowing the mapping of movements, clicks, and navigation patterns while participants browsed the site, realistically simulating the experience of users on internet pages that require consent for data collection and the use of cookies.

Upon accessing the website's homepage, participants were immediately confronted with a pop-up consent manager, a model commonly used on contemporary websites. The interface offered three options: i) read the privacy policy; ii) edit cookie preferences; and iii) accept the terms and proceed. Clicks on the consent manager, access to the policy text, and responses to an online questionnaire about digital privacy were recorded.

The design of the consent manager simulated typical patterns of the digital economy, highlighting quick acceptance as the most direct alternative and allowing observation of whether participants would interact reflectively or reproduce the usual behavior of automatic acceptance. For this purpose, a fictitious privacy policy was created with deliberately intrusive examples of data collection and sharing, including financial information, consumption habits, unrestricted sharing with third parties, and sensitive data.

Participants were recruited through an open online invitation disseminated via digital platforms, email distribution lists, and in-person academic events. Because the experimental website was publicly accessible during the data collection period, participation was voluntary and open to any interested individual. Participants were informed that the study concerned digital privacy and online data practices; however, they were not informed that their interaction behavior with the consent manager would be monitored, since awareness of this aspect could interfere with the spontaneity of their responses and compromise the behavioral observation component of the investigation.

Upon accessing the questionnaire hosted on Google Forms, participants were first presented with an informed consent form describing the objectives of the study, the voluntary nature of participation, the anonymity of responses, and the use of the collected data exclusively for academic purposes. Only after agreeing to the consent form could participants proceed to the questionnaire. The entire research protocol, including the behavioral observation procedures, was reviewed and approved by the Ethics Committee of the University of Porto.

During navigation on the experimental website, the system recorded users' click flow, including the type of action performed (accept, manage, or access the policy), time spent on pages, navigation paths, and temporal records. Subsequently, participants completed a questionnaire regarding demographic profile, frequency of internet use, perceptions of digital privacy, reading habits concerning privacy policies, and perceived control over personal data. The responses were automatically stored for statistical analysis and cross-referenced with the behavioral interaction data collected during the experiment.

The correspondence between navigation records and questionnaire responses was established through date and time stamps, enabling the identification of behavioral patterns. The average time between accessing the site and completing the questionnaire was approximately 11 minutes and 10 seconds, with a standard deviation of 9 minutes and 35 seconds. This procedure enabled the consolidation of a final sample of 237 participants, ensuring that the observed behavioral data matched the participants' reported responses.

The use of this experimental consent manager had as its main objective comparing users' actual behavior with their declared perceptions of privacy and consent. By integrating behavioral data and self-reported responses, the study sought to highlight possible discrepancies between discourse and practice, providing empirical evidence for the critical discussion on the so-called "myth of consent" in the context of data colonialism. In this way, the experimental environment enabled observation of how consent interfaces, often presented as instruments of autonomy and control, may, in practice, operate as mechanisms of information capture embedded within the extractivist logic of the data economy, reinforcing the power structures characteristic of surveillance capitalism.

3.0 Results

The investigation included a sample of 237 participants, predominantly residents of Portugal (65%) and Brazil (31.2%), with smaller representations from countries such as Angola, Spain, Cape Verde, and Germany. Regarding the age profile, there was a predominance of young people and adults, with 56.5% of respondents aged 18 to 34, followed by 32.9% in the 35 to 54 age group. The educational level of the sample is high, demonstrating that the automatic acceptance of consent does not result from a lack of formal education: 46% hold postgraduate degrees (master's or doctorate), and 38.4% have completed undergraduate degrees. These data reinforce that, even among a highly educated public with full digital integration (99.6% access the internet daily), autonomy is suppressed by the extractivist design of interfaces.

Upon accessing the research website, participants were immediately presented with the consent manager, which offered three options: (1) access to the Privacy Policy; (2) the "manage cookies" button; and (3) the "agree and close" button. The passive click flow shows a strong tendency toward immediate consent. Of the 237 recorded accesses, 87.8% of participants (208 users) directly selected the option "agree and close," authorizing the processing of their personal data without adjusting their privacy settings. Only 12.2% of participants (29 users) chose to access the "manage cookies" option to customize their data collection preferences. Among these participants, the following distribution of choices was observed: 8.9% of the total sample (21 participants) rejected all categories of cookies; 2.5% (6 participants) accepted all categories of cookies; and 0.8% (2 participants) configured specific preferences. Among the two participants who selectively customized their permissions, one authorized exclusively the cookies classified as "analytical," while the other allowed "analytical," "performance," and "functional" cookies, rejecting only the "advertising" category.

Access to the privacy policy was even less frequent. Only 5.5% of the sample (13 participants) clicked on the document link. Among these users, 43.8% reached the end of the page, which, at first glance, suggests deeper reading of the document. However, the analysis of the time spent on the page suggests otherwise. Considering that the privacy policy contains approximately 6,150 words and that the average reading speed for adults is estimated at 238 words per minute (Brysbaert 2019), approximately 25 minutes and 50 seconds would be required to complete the reading. However, the median time spent on

the page was only 29 seconds, which corresponds to about 1.9% of the time required for a full reading of the document. This pattern suggests that most participants likely only skimmed the page quickly or scrolled to the end without engaging in effective reading.

Furthermore, when considering the total time spent by the 13 participants on the page, a total of 6 minutes and 17 seconds is observed, which would not even be sufficient for a single person to complete the document. This result reinforces the hypothesis that privacy policies are largely ignored or only superficially consulted by users.

After interacting with the consent manager, participants were directed to the questionnaire. Regarding internet use frequency, 99.6% of respondents reported using it several times a day, while 0.4% reported using it at least once a week, confirming the high level of digital integration in the sample.

To understand participants' perceptions of privacy, they were asked to list words or ideas associated with the term. Participants predominantly associated the concept of privacy with the protection of personal information and the individual dimension of the right to privacy. The terms most frequently mentioned were "information," "right," "individual," "personal," and "private," suggesting that participants understand privacy as a right linked to the protection of personal data and the individual sphere. Other words appeared with intermediate frequency, such as "intimate," "sharing," "authorization," "data," "discretion," "reserved," "restriction," "security," and "confidentiality," indicating a perception of privacy as a mechanism for controlling the flow of information. Less frequent mentions were also recorded, such as "anonymity," "confidentiality," "protection," and "secret," in addition to individual associations such as "power," "manipulation," "autonomy," "safeguard," and "peace of mind," revealing the multidimensional nature of the concept of privacy.

When asked about the importance of different dimensions of privacy, on a scale from 1 (not important at all) to 7 (very important), a strong concentration of responses was observed at the highest levels. Among the evaluated items, the following stood out: not being disturbed in the domestic environment, which presented the highest concentration of responses at the maximum level of the scale; being able to share confidential information with trusted individuals, with a predominance of responses at levels 6 and 7; and having moments completely alone, also with a strong concentration in the upper categories.

When invited to reflect on a typical day involving various digital activities, such as social networking, online shopping, urban mobility, and digital services, participants demonstrated a generalized sense of low control over the collection and use of their personal data. In total, 69.7% of participants indicated that they have little or no control over the information collected about them; 43.5% declared having "not much control"; 26.2% stated they have "no control"; 26.6% reported having "some control" over their data; and only 3.8% stated that they have "a lot of control" over the collection and use of their information.

Finally, participants were asked about possible changes to their digital habits to avoid tracking of their online activities. The results indicated a relatively balanced division: 52.3%

of participants stated that they had not changed their digital habits, maintaining the same patterns of internet and mobile device use; 47.7% declared that they had already modified their behavior, adopting strategies to reduce exposure to tracking.

4.0 Analysis and Discussion

The empirical results of this investigation reveal a structural contradiction between the normative valuation of privacy and the effective behavior observed in relation to interfaces, reinforcing the critiques of Zuboff (2019) and Srnicek (2017) regarding the datafication economy. The high rate of automatic acceptance (87.8%) demonstrates that informed consent functions less as a mechanism of autonomy and more as an instrument of legal legitimation for the massive collection of data, operating under what has been termed the "myth of consent." This dynamic constitutes a pillar of surveillance capitalism, in which "behavioral surplus" is converted into commercial assets through an architecture of invisible extraction.

The discrepancy between the 97% of participants who value privacy and the average time of only 29 seconds dedicated to reading the privacy policy reveals that informational autonomy is, in practice, a legal fiction. As Obar and Oeldorf-Hirsch (2020) point out, the complexity of these documents makes informed decision-making impractical. This phenomenon is further aggravated by dark patterns, design strategies that induce compliance and reduce the likelihood of critical reflection, turning agreement into a product of the interface rather than the result of conscious deliberation.

Among the strategies identified, decision convenience stands out, in which the consent manager presents acceptance of the terms as the fastest and most direct alternative for continuing navigation. This tactic is reinforced by visual prominence, which highlights the "agree and close" button to the detriment of privacy options, and by the fragmentation of choices, which imposes a multi-click journey on those who wish to restrict data collection or customize cookies. In addition, the use of a manipulative interface, typically configured as pop-ups that interrupt access, establishes a limited binary choice between accepting the terms or abandoning the service, consolidating what can be characterized as coercive or structurally induced consent. This process of capture, which naturalizes the expropriation of everyday experience, directly resonates with the concept of data colonialism proposed by Couldry and Mejias (2019), in which human life is annexed as raw material to digital capital.

The perception of 69.7% of the sample regarding the lack of effective control over their data reflects the power asymmetry inherent in this new regime of accumulation. This vulnerability manifests as infrastructural coercion: to access essential services managed by Big Techs, the user is forced to accept asymmetric terms, under the penalty of being excluded from digitized social life. Analogous to the Requirement of the Spanish Empire cited by de las Casas (1951), current policies formalize submission through opaque languages. As argued by Kwet (2019), this concentration of technological power

consolidates a digital neocolonialism that subjects individuals to a machinic servitude, in which their traces feed predictive systems of algorithmic governance.

Therefore, the results corroborate the need to transcend the individualistic logic of consent. As Noble (2018) and Mumford (2022) argue, effective protection in the era of datafication requires models grounded in informational sovereignty and digital justice, capable of redistributing control over information flows and limiting the extractivism of platforms. The problem, as evidenced, is not merely educational, but rather a question of political economy that requires a profound restructuring of sociotechnical infrastructures.

Moreover, the management of the complexity inherent to Big Data transcends the need for technical advances or semantic innovation; it demands a democratic strategy, grounded in human and social principles, to ensure that the excess of information does not culminate in the emptying of knowledge. It is essential to understand Big Data as a technosocial phenomenon (Francelin and Meschini 2025), in which the processing and analysis of large volumes of data are shaped by political choices, theoretical biases, and human decisions that act upon it.

The reframing of the issue of consent and policies in terms of an integrated ethical value, as well as the inclusion of the principles of informational justice in the design, brings the proposal closer to the discussions in the field of Knowledge Organization (Ridi 2013; Moura 2024; Hayashi et al. 2025; Tognoli 2025).

5.0 Conclusions

The present investigation began with the premise that informed consent, as operationalized on contemporary digital platforms, plays a central role in the governance of personal data processing, often presented as the primary instrument for guaranteeing user autonomy. By articulating the theoretical frameworks of surveillance capitalism and data colonialism with the empirical analysis of user behavior in the presence of an experimental consent manager, it was possible to critically examine how this mechanism functions in the everyday practice of digital interaction.

The results reveal a significant discrepancy between the importance individuals attribute to privacy and the way consent is effectively granted in digital environments. The high rate of immediate acceptance observed in the behavioral experiment, associated with the limited access to and reading of the privacy policy, demonstrates that consent rarely results from informed deliberation. On the contrary, it materializes in a context marked by complex interfaces, cognitive overload, and informational asymmetry, in which the user's decision tends to be guided by convenience and platform design structures.

These empirical findings reinforce the critiques present in the literature regarding the so-called "myth of consent," according to which individual authorization functions less as an instrument of informational self-determination and more as a mechanism for the legal formalization of data collection. Inserted within the broader context of the datafication

economy, consent becomes part of a sociotechnical infrastructure that enables the systematic capture of personal information and its conversion into economic value.

From the perspective of data colonialism, this dynamic reveals a contemporary form of appropriation of human experience. The transformation of everyday activities into flows of monetizable data demonstrates that social life has become an integral part of the accumulation chains of informational capitalism. In this scenario, privacy governance ceases to be merely a matter of individual protection and becomes a matter of structural power, informational control, and digital sovereignty.

The analysis developed throughout the study demonstrates that the current model of consent presents important limitations in addressing these asymmetries. Although it remains a relevant component of data protection legislation, its isolated application proves insufficient in the face of the technical and economic complexity that characterizes the contemporary digital ecosystem. The effective protection of data subjects, therefore, requires broader approaches capable of acting not only on individual behavior but also on technological infrastructures, platform business models, and information governance regimes.

In this sense, the results point to the need to adopt regulatory and sociotechnical strategies that promote greater transparency, limit data collection, hold platforms accountable, and strengthen informational self-determination. Initiatives aimed at critical data education, the development of more ethical digital architectures, and the construction of participatory models of internet governance are also fundamental to addressing the challenges posed by the surveillance economy.

Like any empirical investigation, this study presents some limitations. The analysis focused primarily on the technological, informational, and structural dimensions of the phenomenon, privileging perspectives from information science and critical technology studies. Although the observed behavior is strongly related to factors such as cognitive heuristics, social influence, and decision-making processes, aspects derived from social psychology could have been explored to understand the subjective motivations that influence users' decisions when faced with consent interfaces.

Thus, future research may expand this interdisciplinary approach by investigating in greater detail the interactions between interface design, human behavior, and risk perception, as well as by analyzing how cultural, educational, and contextual factors influence individuals' relationships with digital privacy. Comparative studies across different geographical contexts, particularly between countries of the Global North and the Global South, may also deepen understanding of the political and economic implications of data colonialism.

By empirically highlighting the tensions between formal consent and effective autonomy in the digital environment, this research contributes to the contemporary debate on digital justice, data governance, and informational self-determination. In a context in which social life becomes increasingly datafied, rethinking the mechanisms for controlling the circulation of personal information is an essential step toward building a more democratic,

transparent, and public-interest–oriented digital society. Ultimately, consent in the digital economy is not an act of freedom, but a bureaucratic rite of passage that formalizes the expropriation of everyday life under the appearance of legality, requiring an urgent transition from a focus on individual autonomy to the guarantee of collective digital justice.

AI usage statement: The authors used Grammarly and Claude to review the English translation of this manuscript, as the authors are non-native English speakers. These tools were used only for language editing (grammar, clarity, and word choice), not for generating content or ideas. The authors reviewed all changes and take full responsibility for the final text.

Acknowledgements

This work is funded by national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., under the project UIDB/04059/2020 (CITCEM).

References

Bair, Sheila A. 2005. “Toward a Code of Ethics for Cataloging.” Technical Services Quarterly 23, no. 1: 13–26.

Brysbaert, Marc. 2019. “How Many Words Do We Read per Minute? A Review and Meta-Analysis of Reading Rate.” Journal of Memory and Language 109: 104047.

Cohen, Julie E. 2018. “The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy.” Philosophy & Technology 31: 213–233. https://doi.org/10.1007/s13347-017-0258-2.

Costa, Camila Mattos da, and Jonas Ferrigolo Melo. 2022. “Debates exploratórios sobre o colonialismo de dados.” In IX Encontro da ULEPICC-Brasil: As Tramas do Imperialismo no Século XXI, Londrina, November 22–25, 2022. https://doity.com.br/anais/9ulepiccbr/trabalho/252889.

Couldry, Nick, and Ulises A. Mejias. 2019. “Data Colonialism: Rethinking Big Data’s Relation to the Contemporary Subject.” Television & New Media 20: 336–349. https://doi.org/10.1177/1527476418796632.

Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2018. “We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy.” arXiv preprint arXiv:1808.05096. https://arxiv.org/abs/1808.05096.

Francelin, Marivalde Moacir, and Fabio Orsi Meschini. 2025. “Knowledge Organization and the Technological Challenges of the Big Data Era.” Knowledge Organization 52, no. 2: 40017. https://doi.org/10.31083/KO40017.

Hayashi, Maria Cristina Piumbato Innocentini, Marcia Regina da Silva, Camila Carneiro Dias Rigolin, and Júlia Fernandes Marcelo. 2025. “Ética algorítmica e interseccionalidade na Organização do Conhecimento com Inteligência Artificial.” In Desafios Éticos na Organização do Conhecimento II, edited by Fernanda Ribeiro, 99–112. Vol. 2. Porto: Faculdade de Letras da Universidade do Porto. https://doi.org/10.21747/978-989-9320-00-0/des.

Kwet, Michael. 2019. “Digital Colonialism: US Empire and the New Imperialism in the Global South.” Race & Class 60, no. 4: 3–26.

Las Casas, Bartolomé de. 1951. Historia de las Indias. Vol. 3. México: Fondo de Cultura Económica.

Moura, Maria Aparecida. 2024. “Information and Code Biases: Social Differentiation, Intersectionality and Decoloniality in Knowledge Organization Systems.” Knowledge Organization 51: 514–520. https://doi.org/10.5771/0943-7444-2024-7-514.

Mumford, Densua. 2022. “Data Colonialism: Compelling and Useful, but Whither Epistemes?” Information, Communication & Society 25: 1511–1516. https://doi.org/10.1080/1369118X.2021.1986103.

Noble, Safiya Umoja. 2018. Algorithms of Oppression: How Search Engines Reinforce Racism. New York: New York University Press.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2020. “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services.” Information, Communication & Society 23: 128–147. https://doi.org/10.1080/1369118X.2018.1486870.

Quivy, Raymond, and Luc Van Campenhoudt. 1992. Manual de investigação em ciências sociais. Lisboa: Gradiva.

Ridi, Riccardo. 2013. “Ethical Values for Knowledge Organization.” Knowledge Organization 40: 187–196. https://doi.org/10.5771/0943-7444-2013-3-187.

Schaub, Florian, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. “A Design Space for Effective Privacy Notices.” In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 1–17. Ottawa: USENIX Association. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub.

Srnicek, Nick. 2017. Platform Capitalism. Cambridge: Polity.

Thatcher, Jim, David O’Sullivan, and Dillon Mahmoudi. 2016. “Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data.” Environment and Planning D: Society and Space 34: 990–1006. https://doi.org/10.1177/0263775816633195.

Tognoli, Natália Bolfarini. 2025. “Access to Information and Social Justice: Pivotal Values for a Critical Knowledge Organization.” Informatio 30, no. 1: e203. https://doi.org/10.35643/info.30.1.8.

Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. "(Un)informed Consent: Studying GDPR Consent Notices in the Field." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 973–990. New York: Association for Computing Machinery. https://doi.org/10.1145/3319535.3354212.

West, Sarah Myers. 2019. "Data Capitalism: Redefining the Logics of Surveillance and Privacy." Business & Society 58: 20–41. https://doi.org/10.1177/0007650317718185.

Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books.