The Possibilities of Data Resistance in a Digital Society

Kyle Beadle, University College London

The British Academy

Abstract

In our digital society, marginalised and vulnerable populations are unequally at risk of discrimination, surveillance, and lack of representation from the collection, analysis, and usage of their data. Instead of submitting to these consequences of our digital society, data resistance, or the subversive and productive act of responding to the power of corporate and governmental data practices, offers a way out. This paper presents acts of data resistance from across the globe to argue that a *good* digital society mirrors a *good* democratic society—one that supports individual and collective agency, autonomy, and empowerment, strengthens democratic values and promotes equality and justice, and stimulates market competition. This paper concludes with three brief policy provocations: imposing a data tax, enabling participatory governance of data regulation, and establishing self-sovereign identity, all of which build upon the work of activists, academics, and artists dedicated to creating a better digital society.

***Keywords*:** data resistance; privacy harms; participatory governance

Introduction

The possibilities of marginalised and vulnerable populations are constrained by privacy-violating algorithms and data practices. Individuals belonging to these populations, such as LGBTQ+,[1] refugee,[2] and racial minority populations,[3] face unique privacy violations beyond those of the general population. LGBTQ+ dating apps are used to arrest queer people[4], period-tracking apps may lead to the conviction of women seeking abortions[5] and religious minorities are being tracked through Muslim prayer apps.[6] To protect themselves from being stereotyped by behavioural data,[7] arrested because of discriminatory policing practices,[8] and struggling to live under welfare fraud algorithms,[9] marginalised[10] and vulnerable[11] individuals use privacy tools such as the Tor browser,[12] ad blockers,[13] and end-to-end encryption.[14] These data resistance practices empower individuals to reclaim control over their digital identities and online experiences.[15] Data resistance shapes a *good* digital society[16] by supporting individual and collective agency, autonomy, and empowerment, strengthening democratic values and promoting equality and justice, and stimulating market competition.

Building on Baaz et al.'s definition of resistance, data resistance is an act performed by data subjects responding to the power of corporate and governmental data practices.[17] Included in data resistance is algorithmic resistance, or the acts of responding to algorithms.[18] While all data subjects, or 'the identified or identifiable living individual to whom personal data relates,'[19] are constrained by the aggregation, analysis, and application of personal data for the use of corporate profit and government observation, this paper focuses on the experiences of marginalised and vulnerable populations. UK Aid Match defines marginalisation as 'both a process, and a condition, that prevents individuals or groups from full participation in social, economic and political life,' and that, 'people can be marginalised due to multiple factors: sexual orientation, gender, geography, ethnicity,

1 Ellis, J.R. (2022) Blurred consent and redistributed privacy: owning LGBTQ identity in surveillance capitalism. In: *Diversity in Criminology and Criminal Justice Studies*. Emerald Publishing Limited. pp. 183–196.

2 Metcalfe, P. & Dencik, L. (2019) The politics of big borders: Data (in) justice and the governance of refugees. *First Monday*

3 Wäscher, T. (2020) Framing resistance against surveillance: Political communication of privacy advocacy groups in the "Stop Watching Us" and "The Day We Fight Back" campaigns. In: *Journalism, Citizenship and Surveillance Society*. Routledge. pp. 113–130.

4 Brandom, R. (2018) Designing for the crackdown. 25 April 2018. *The Verge*.

5 Hill, K. (2022) Deleting Your Period Tracker Won't Protect You. 30 June 2022. *The New York Times*.

6 ACLU (2013) The NYPD Muslim Surveillance Program.

7 Mayer, J.R. & Mitchell, J.C. (2012) Third-Party Web Tracking: Policy and Technology In: *2012 IEEE Symposium on Security and Privacy*. May 2012 San Francisco, CA, USA, IEEE. pp. 413–427.

8 Arora, P. (2019) General data protection regulation—A global standard? Privacy futures, digital activism, and surveillance cultures in the Global South. *Surveillance & Society*. 17 (5), 717–725.

9 Burgess, M., Schot, E. & Geiger, G. (2023) This Algorithm Could Ruin Your Life, *WIRED*.

10 Lerner, A., He, H.Y., Kawakami, A., Zeamer, S.C. & Hoyle, R. (2020) Privacy and activism in the transgender community. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 2020 pp. 1–13.

11 Tanczer, L.M., López-Neira, I. & Parkin, S. (2021) 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of Gender-Based Violence*. 5 (3), 431–450.

12 The Tor Project Inc. (n.d.) *The Tor Project* [Accessed: 6 March 2024].

13 Wills, C.E. & Uzunoglu, D.C. (2016) What ad blockers are (and are not) doing. In: *2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*. 2016 IEEE. pp. 72–77.

14 Greenberg, A. (2014) Hacker Lexicon: What is End-To-End Encryption? 25 November 2014. *Wired*.

15 Youmans, W.L. & York, J.C. (2012) Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of Communication*. 62 (2), 315–329.

16 Dufva, T. & Dufva, M. (2019) Grasping the future of the digital society. *Futures*. 107, 17–28.

17 Baaz, M., Lilja, M., Schulz, M. & Vinthagen, S. (2016) Defining and Analyzing "Resistance": Possible Entrances to the Study of Subversive Practices. *Alternatives: Global, Local, Political*. 41 (3), 137–153; Milan, S. & Velden, L. Van Der (2016) The Alternative Epistemologies of Data Activism. *Digital Culture & Society*. 2 (2), 57–74; Milioni, D.L. & Papa, V. (2022) The oppositional affordances of data activism. *Media International Australia*. 183 (1), 44–59.

18 Ettlinger, N. (2018) Algorithmic affordances for productive resistance. Big Data & Society. 5 (1), Cobbe, J. (2021) Algorithmic Censorship by Social Platforms: Power and Resistance. *Philosophy & Technology*. 34 (4), 739–766; DeVito, M.A., Gergle, D. & Birnholtz, J. (2017) 'Algorithms ruin everything': #RIPTwitter, Folk Theories, and Resistance to Algorithmic Change in Social Media. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. May 2017 Denver Colorado USA, ACM. pp. 3163–3174; Heemsbergen, L., Treré, E. & Pereira, G. (2022) Introduction to algorithmic antagonisms: Resistance, reconfiguration, and renaissance for computational life. *Media International Australia*. 183 (1), 3–15; Shelby, R., Rismani, S., Henne, K., Moon, Aj., Rostamzadeh, N., Nicholas, P., Yilla-Akbari, N., Gallegos, J., Smart, A., Garcia, E. & Virk, G. (2023) Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction. In: *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*. August 2023 Montreal QC Canada, ACM. pp. 723–741.

19 U.K. Information Commissioner's Office (n.d.a) Legal definitions. *Information Commissioner's Office*.

religion, displacement, conflict, or disability. Poverty is both a consequence and a cause of being marginalised.'[20] Even though everyone in a digital society is exposed to privacy-violating data practices and algorithms, marginalised and vulnerable populations are more exposed to the harms these socio-technical systems produce. In consequence, data resistance is mainly led by these marginalised and vulnerable populations.[21]

Behind the study of data resistance lie larger questions about our digital society. A digital society is a datafied society or a world in which, 'digital data enable not only near-real-time monitoring of aspects of human society but also of nature thanks to the increasing connection of data production, processing, modelling and sharing.'[22] Questions of agency, equality, and justice in a datafied society begin the second an individual interacts with an information system. Is data extracted from people equally? How accurate does data need to be about an individual? What can an individual withhold from data collection? Corporations argue that unused data is worthless, and their digital services infuse data with value. When does data extraction become exploitative? How much data is too much? What is an individual's data worth? How does it change value when aggregated with others' data? What compensation do individuals receive for their data? Is the compensation fair concerning the value their data creates? Participation is the central theme of these questions. Who gets to participate in a digital society? Where does a person get to participate in a digital society? How much can a single person participate in a digital society? Arguing for data resistance within a digital society means empowering individuals to answer these questions for themselves, ensuring them that someone represents their interests if they choose not to answer them, and holding accountable those that violate their interests. In essence, a good digital society mirrors a good democratic society.[23]

Supporting individual and collective agency, autonomy, and empowerment

Agency, autonomy, and empowerment are central in a good datafied society where data mining practices expand surveillance[24] and social sorting.[25] According to a 2022 UK Government survey, 52% of respondents stated they have little to no knowledge of how personal data is utilised and gathered about them in day-to-day life.[26] Without comprehension of corporate and government data practices, over 60% of respondents reported feeling a lack of control over their data.[27] Agency in a datafied world is collectives' and individuals' abilities to manifest their capacity to act *within, upon* and *in concert with* structures that reduce individuals' actions to data.[28] Algorithmic decision-making and current data practices additionally weaken individual and collective autonomy by obscuring processes,[29] controlling data flows,[30] and constraining available products and services.[31] Therefore, a datafied society that supports autonomy enables the agency of collectives and individuals to express ownership over the collection, storage, and usage of their data. These possibilities are withheld from individuals and collectives because algorithmic affordances,[32] economic incentives,[33] and platform centralisation[34] do not provide alternatives.

Specifically, transgender people face being outed by automatic gender recognition,[35] black and Indigenous people of color experience unequal medical treatment by diagnostic algorithms,[36] and people with lower socioeconomic status encounter more predatory financial practices by loan approval algorithms.[37] Marginalised and vulnerable populations are therefore unable to act upon their self-determination if our datafied society hinders their individual, financial, and medical agency. As a result, empowerment in a datafied society reinforces agency and autonomy by providing collectives and individuals with the social,

20 U.K. Aid Match (2020) Defining marginalised – the Foreign, Commonwealth & Development Office's 'Leaving no one behind' agenda.

21 Karizat, N., Delmonaco, D., Eslami, M. & Andalibi, N. (2021) Algorithmic Folk Theories and Identity: How TikTok Users Co-Produce Knowledge of Identity and Engage in Algorithmic Resistance. *Proceedings of the ACM on Human-Computer Interaction*. 5 (CSCW2), 1–44.

22 Gstrein, O.J. & Beaulieu, A. (2022) How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*. 35 (1).

23 Balkin, J.M. (n.d.) Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society. *NEW YORK UNIVERSITY LAW REVIEW*. 79.

24 Andrejevic, M. & Gates, K. (2014) Big Data Surveillance: Introduction. *Surveillance & Society*. 12 (2), 185–196.

25 Lyon, D. (2003) *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press.

26 Centre for Data Ethics and Innovation (2022) Public attitudes to data and AI: Tracker survey.

27 Centre for Data Ethics and Innovation (2022) Public attitudes to data and AI.

28 Kennedy, H., Poell, T. & Van Dijck, J. (2015) Data and agency. *Big Data & Society*. 2 (2).

29 Gillespie, T. (2014) The relevance of algorithms. *Media technologies: Essays on communication, materiality, and society*. 167 (2014), 167.

30 Bergé, J.-S., Grumbach, S. & Zeno-Zencovich, V. (2018) The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance. *European Journal of Comparative Law and Governance*. 5 (2), 144–178.

31 Gal, M.S. (2018) Algorithmic challenges to autonomous choice. *Mich. Tech. L. Rev.* 25, 59; Danaher, J. (2019) The Ethics of Algorithmic Outsourcing in Everyday Life. In: *Algorithmic Regulation*. Oxford University Press. pp. 98–118; Dogruel, L., Facciorusso, D. & Stark, B. (2022) 'I'm still the master of the machine.' Internet users' awareness of algorithmic decision-making and their perception of its effect on their autonomy. *Information, Communication & Society*. 25 (9), 1311–1332.

32 Milioni, D.L. & Papa, V. (2022) The oppositional affordances of data activism. 44–59.

33 Vincent, N., Li, H., Tilly, N., Chancellor, S. & Hecht, B. (2021) Data Leverage: A Framework for Empowering the Public in its Relationship with Technology Companies. In: *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. March 2021 Virtual Event Canada, ACM. pp. 215–227.

34 Iiadis, A., & Ford, H. (2023). Fast facts: Platforms from personalization to centralization. *Social Media+ Society.*

35 Keyes, O. (2018) The misgendering machines: Trans/HCI implications of automatic gender recognition. *Proceedings of the ACM on human-computer interaction*. 2 (CSCW), 1–22.

36 Obermeyer, Z., Powers, B., Vogeli, C. & Mullainathan, S. (2019) Dissecting racial bias in an algorithm used to manage the health of populations. Science. 366 (6464), 447–453.

37 Eubanks, V. (2018) *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press; Hampton, L.M. (2021) Black feminist musings on algorithmic oppression.

political, economic, and technical tools to enable their data resistance. By highlighting and presenting the practices which individuals and collectives use to reclaim agency, autonomy, and empowerment, I argue for the importance of data resistance in a digital society.

Individual data resistance

At an individual level, data resistance fosters self-determination as it empowers users to seize control of their digital identities and online experiences.[38] In compiling a list of fifteen cases of everyday algorithmic auditing, Shen et al. argue that ordinary users effectively detect the hidden operations of popular platforms such as Google Search, TikTok, and YouTube.[39] One example they examine further is racial bias in Twitter's cropping algorithm.[40] When large photos are posted on Twitter, the website will present only a section of the photo to fit within their design while allowing users to see the full photo by clicking on it. However, users in 2020 found that Twitter's cropping algorithm would only crop out darker-skinned people in favour of lighter-skinned people. In running these experiments, individual users became aware of the underlying mechanisms on Twitter that concealed darker-skinned users.[41]

Beyond platform affordances, Pybus et al. research project *Our Data Ourselves* additionally reveals the role of hacktivists (i.e., politically motivated hackers) in augmenting individual agency over data practices.[42] By developing and distributing an Android app that mines data from users' downloaded social media apps, they reveal the security vulnerabilities of platforms, inform users of the extent their data is accumulated, and dismantle the control platform's exercise on user data. On the one hand, these examples show just two of the many techniques users deploy to regain agency in a data-driven world.[43] On the other hand, the examples highlight how individual acts of resistance are also often situated within broader, collective movements.

Collective data resistance

At a societal level, data resistance highlights ongoing injustices and supplies the tools necessary for solidarity.[44] Corporate algorithmic decision-making and data practices seek to isolate users from one another, as Bonini et al highlight in their analysis and observation of how 68 food delivery workers use instant messaging apps.[45] Therefore, data resistance is necessary to initiating and maintaining solidarity in a datafied society. Focusing on the Open Knowledge Foundation Germany (OKF DE), Stefan Baack reiterates the importance of a 'transparent and collaborative form of governance' to many open data activists.[46] Baack reports that the OKF DE acknowledges the different technical and social expertise necessary for the various tasks of collecting, distributing, and interpreting open data from corporations and governments, and argues that the open data movement encourages participation and collaboration.

Furthermore, surveillance is a collective issue which requires collective opposition. Big data scholar Kazansky found that developers and security educators collectively employed anticipatory techniques of 'threat modelling' and 'risk assessment' to develop advice and strategies to resist surveillance.[47] These methods empower collectives to consider the impact of data surveillance within their contexts because surveillance presents different risks to black and LGBTQ+ individuals than it does to disabled people—and these contexts can also overlap. By organising themselves according to how algorithmic decision-making and data practices affect them, these collectives, whether food delivery drivers, open-source activists, or developers and educators, appropriate the tools and techniques used against them to regain agency, autonomy, and empowerment within a digital society.

38 Kapsch, P.H. (2022) Exploring user agency and small acts of algorithm engagement in everyday media use. *Media International Australia*. 183 (1), 16–29.

39 Shen, H., DeVos, A., Eslami, M. & Holstein, K. (2021) Everyday Algorithm Auditing: Understanding the Power of Everyday Users in Surfacing Harmful Algorithmic Behaviors. *Proceedings of the ACM on Human-Computer Interaction*. 5 (CSCW2), 1–29.

40 Yee, K., Tantipongpipat, U. & Mishra, S. (2021) Image cropping on twitter: Fairness metrics, their limitations, and the importance of representation, design, and agency. Proceedings of the ACM on human-computer interaction. 5 (CSCW2), 1–24.

41 Shen, H., DeVos, A., Eslami, M. & Holstein, K. (2021) Everyday Algorithm Auditing. 1-29.

42 Pybus, J., Coté, M. & Blanke, T. (2015) Hacking the social life of Big Data. *Big Data & Society*. 2 (2).

43 Xie, X., Du, Y. & Bai, Q. (2022) Why do people resist algorithms? From the perspective of short video usage motivations. *Frontiers in Psychology*. 13; Fouquaert, T. & Mechant, P. (2022) Making curation algorithms apparent: a case study of 'Instawareness' as a means to heighten awareness and understanding of Instagram's algorithm. *Information, Communication & Society*. 25 (12), 1769–1789; Velkova, J. & Kaun, A. (2021) Algorithmic resistance: media practices and the politics of repair. *Information, Communication & Society*. 24 (4), 523–540.

44 Milan, S. (2015) From social movements to cloud protesting: the evolution of collective identity. *Information, Communication & Society*. 18 (8), 887–900.

45 Bonini, T., Treré, E., Yu, Z., Singh, S., Cargnelutti, D. & López-Ferrández, F.J. (2023) Cooperative affordances: How instant messaging apps afford learning, resistance and solidarity among food delivery workers. *Convergence: The International Journal of Research into New Media Technologies*.

46 Baack, S. (2015) Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data & Society*. 2 (2), 205395171559463.

47 Kazansky, B. (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society*. 8 (1).

Strengthening democratic values and promoting equality and justice

Data resistance protects democratic values such as freedom of speech, expression, and association by preventing surveillance and censorship.[48] Data gathering technologies, such as CCTV, GPS tracking, and wiretapping, cause a chilling effect on freedom of speech. Yet, while the smartphone democratises these capabilities, enabling anyone to hold government officials accountable, facilitating the safety of protestors, and encouraging the creation of journalism, it also extends surveillance ever closer to our physical bodies. Data resistance techniques, such as the mobile phone application 'InformaCam,' analysed by Van der Velden, allow individuals to reclaim democratic values by supporting journalists and protestors.[49] InformaCam resists datafication in two ways, firstly by directly involving users in 'investigatory practices through code' by which users respond to 'unequal distribution of power over data,' as argued by Van der Velden.[50] Secondly, the practice allows users to delete the metadata, such as location, time, and device type, associated with their smartphone camera—empowering journalists and protestors to take and share photos without fear of being located. Data resistance tools, such as 'InformaCam,' strengthen democratic values by enabling anyone to resist datafication and seize control of their personal data regardless of their position in a datafied society.

Data resistance and the freedom of expression

Personal security tools, such as such as 'InformaCam,' can only exist when supported by strong values for freedom of association that make possible groups[51] dedicated to anonymity and privacy. For example, the Chaos Computer Club (CCC)[52] is Europe's largest hacker group with a mission of deconstructing surveillance technology and building alternative technologies to support data security and privacy.[53] The MyData activist group in Finland additionally combines technical skills and digital human rights to improve 'the fair use of personal data.'[54] The group, founded in 2017, quickly expanded globally and critically examines the role of technical measures in data activism while petitioning for stronger data governance politically.[55] Finally, the Electronic Disturbance Theater 2.0 (EDT 2.0), a group of hacktivists and artists, created the 'Transborder Immigrant Tool' which helps people crossing the Mexican-American border find safe routes and water.[56] Data practices are intentionally obfuscated to prevent individuals from understanding the true extent to which they are tracked and monetised. By refusing to be kept in individual data silos, the CCC, Guardian Project, MyData, and the EDT assert their collective power to resist existing structures, protect marginalised and vulnerable populations, and preserve the freedom of association.

Promoting equality and justice with data resistance

Whether resisting the introduction of algorithms in educational assessments or advocating for the implementation of protective algorithms, resisting data means opposing discriminatory decision-making and promoting equal opportunity. Algorithmic systems reproduce existing social biases while imposing past outcomes on future possibilities. Taking to social media is just one way of resisting these algorithmically enforced biases, such as #FuckTheAlgorithm analysed by Benjamin.[57] The hashtag was developed following the backlash to the 2020 OfQual scandal in which the administrator of national exams in the United Kingdom announced that students' previous coursework would be used to establish their marks algorithmically instead of a traditional exam. As a result, students were judged not on how they could perform but how they, and their classmates from that same school, performed in the past, resulting in unexpected underperformance at historically BAME schools. The use of #FuckTheAlgorithm amplified the backlash and illuminated the sociotechnical structures which impose marginalisation.

However, some algorithmic systems do shield individuals from harm. On the Chinese social media app, Zihu, gay men perceive algorithms which filter content to user preferences as their 'protectors.'[58] Zhao argues, in their analysis of the practice, that by only recommending LGBTQ+ content to LGBTQ+ people, algorithms protect marginalised groups by not recommending their posts to non-queer users and by shielding them from outside group hate.[59] LGBTQ+ people on Zihu fit the algorithm to their needs and construct their own coherent social media experience in parallel to heteronormative ones. In confronting the imposition of algorithms through a viral social media campaign and appropriating filter algorithms as protection mechanisms, data resistors affirm the need for everyone to receive equal status, equal rights, and equal opportunities despite 'neutral' algorithms that claim to remove human bias.

48 Treré, E. (2016) The Dark Side of Digital Politics: Understanding the Algorithmic Manufacturing of Consent and the Hindering of Online Dissidence. *IDS Bulletin*. 41 (1), 127–138.

49 Van Der Velden, L. (2015) Forensic devices for activism: Metadata tracking and public proof. *Big Data & Society*. 2 (2).

50 Van Der Velden, L. (2015) Forensic devices for activism.

51 Guardian Project (n.d.) *Guardian Project*. [Accessed: 6 March 2024].

52 The Chaos Computer Club (n.d.) *The Chaos Computer Club*. [Accessed: 6 March 2024].

53 Kubitschko, S. (2015) The Role of Hackers in Countering Surveillance and Promoting Democracy. *Media and Communication*. 3 (2), 77–87.

54 MyData Global (n.d.) *MyData*. [Accessed: 6 March 2024].

55 Lehtiniemi, T. & Ruckenstein, M. (2019) The social imaginaries of data activism. *Big Data & Society*. 6 (1).

56 Züger, T., Milan, S. & Tanczer, L.M. (2015) FCJ-192 Sand in the Information Society Machine: How Digital Technologies Change and Challenge the Paradigms of Civil Disobedience. *The Fibreculture Journal*. (26 2015: Entanglements–Activism and Technology).

57 Benjamin, G. (2022) #FuckTheAlgorithm: algorithmic imaginaries and political resistance. In: *2022 ACM Conference on Fairness, Accountability, and Transparency*. June 2022 Seoul Republic of Korea, ACM. pp. 46–57.

58 Zhao, L. (2023) Filter Bubbles? Also Protector Bubbles! Folk Theories of Zhihu Algorithms Among Chinese Gay Men. *Social Media + Society*. 9 (2).

59 Zhao, L. (2023) Filter Bubbles?

Stimulating market competition

Data resistance also encourages individual control and portability of an individual's data, incentivising competition among online services as they seek to differentiate themselves based on their privacy protections.[60] Data portability, 'allows individuals to obtain and reuse their personal data for their own purposes across different services,' and is a right granted in Article 20 of the EU General Data Protection Regulation.[61] Additionally, individuals can access their data through subject access requests which compels data controllers to hand over an individual's data within one month of the request.[62] Data resistance encourages the use of these two legal instruments to move data among services and to understand what data is stored on any given individual. With this knowledge, individuals can make more informed decisions within the digital market.

Usability of data portability

Understanding how to reclaim control of one's data, through data portability, is the first step in stimulating market competition for online services.[63] One way of comprehending data portability is by measuring the complexity of individual perceptions. An interview and survey study conducted by Jamieson and Yamashita found that most respondents were either neutral or more likely to use smaller online services if proper data portability measures were implemented in the larger platforms, such as Facebook, Google, and Microsoft.[64] However, an overwhelming 60% of their participants reported that they were not likely to stop using their currently used platforms even if data portability allowed them to transfer their data elsewhere.[65] On one hand, these results suggest that, despite data portability, individuals do not consider there to be any viable alternatives to Facebook, Google, and Microsoft services. On the other hand, these results prove that the ability to import data from larger services to smaller services will be necessary for smaller services to gain a foothold in the digital market.

Data portability in practice

Furthermore, it is necessary to examine how digital services implement data portability to understand how they relate to regulation and provide choice to individuals. Online services do not always allow an individual's entire, personal data to be easily exported. In a longitudinal study from 2015 to 2019, Kröger et al. found that only an average of 33% of app vendors sufficiently responded to subject access requests with customer data.[66] Additionally, while many online services offer data exports, realizing data imports is less common. In a study of 182 online services, Syrmoudis et al. found that 74.2% of services offer some way of exporting data while 76.8% of services offer no data import options.[67]

One challenge for data portability is the lack of standardised data formats where instead each digital service maintains its own, unique definitions and data structures. This challenge only gets exacerbated among Internet of Things devices which capture personal data that is more difficult to structure, such as audio recordings, body data and location data.[68] There is still much to do regarding individual data portability, especially in the wake of GDPR, but the slow movement of digital services is still promising as the small, decentralised web, in the form of Mastodon and other ActivityPub-based applications, pushes market leaders to open up.[69]

Market effects of data portability

Furthermore, investigating the impact of data portability legislation on current markets is the second step in capturing how data resistance energises the free market for online services.[70] Firstly, data portability may reduce barriers for new market entrants. Lam et al. found, in their economic simulation of data portability, that current legislation increases the barrier to entry for new market competitors, but only because current legislation does not go far enough in requiring all, quality collected data to be transferable. They argue that it is necessary to 'broaden the range of portable data' and 'force data sharing' to lower barriers.[71]

60 Engels, B. (2016) Data portability among online platforms. *Internet Policy Review.* 5 (2).

61 U.K. Information Commissioner's Office (n.d.c) *Right to data portability* [Accessed: 6 March 2024].

62 U.K. Information Commissioner's Office (n.d.b) *Right of access*. Right of access [Accessed: 6 March 2024].

63 Zwiebelmann, Z. & Henderson, T. (2021) Data Portability as a Tool for Audit. In: *Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers.* September 2021 Virtual USA, ACM. pp. 276–280 [Accessed: 16 August 2024].

64 Jamieson, J. & Yamashita, N. (2023) Escaping the Walled Garden? User Perspectives of Control in Data Portability for Social Media. *Proceedings of the ACM on Human-Computer Interaction.* 7 (CSCW2), 1–27 [Accessed: 16 August 2024].

65 Jamieson, J. & Yamashita, N. (2023) Escaping the Walled Garden?

66 Kröger, J.L., Lindemann, J. & Herrmann, D. (2020) How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android Apps. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security.* 2020 pp. 1–10.

67 Syrmoudis, E., Mager, S., Kuebler-Wachendorff, S., Pizzinini, P., Grossklags, J. & Kranz, J. (2021) Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. *Proceedings on Privacy Enhancing Technologies.* 2021 (3), 351–372. [Accessed: 16 August 2024].

68 Turner, S., Quintero, J.G., Turner, S., Lis, J. & Tanczer, L.M. (2020) The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*

69 David, E. (2024) *Threads' API is coming in June*. 1 March 2024. The Verge.

70 Krämer, J. (2021) Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations. *Journal of Competition Law & Economics.* 17 (2), 263–308. [Accessed: 16 August 2024]; Wohlfarth, M. (2019) Data Portability on the Internet: An Economic Analysis. *Business & Information Systems Engineering.* 61 (5), 551–574; Krämer, J., Senellart, P. & de Streel, A. (2020) *ECONOMIC IMPLICATIONS AND REGULATORY CHALLENGES.*

71 Lam, W.M.W. & Liu, X. (2020) Does data portability facilitate entry? *International Journal of Industrial Organization.* 69, 102564.

Secondly, data portability may encourage innovation from market competitors. In an analysis of Spotify, Ramos et al. found that the introduction of Apple Music as a market competitor increased the amount Spotify spent on research and development (R&D), and they argue that R&D spending is likely to grow as data portability increases the likelihood of individuals switching services.[72] While the effects are currently small, data portability legislation in Europe is changing global market competition. International data resistance must continue to push legislators to extend the requirements of data portability and hold digital services accountable for violating the law.

Challenges of data resistance

Although data resistance unearths a myriad of possibilities for our digital society, it also comes with challenges. One indirect challenge is the rise of hate speech, racism, and extremism that comes with the anonymous use of digital services. In this case, the autonomy (free speech) that digital privacy allows clashes with a need for democracies to protect themselves from disinformation and extremism. Firstly, focusing on privacy as the issue does not hold digital services accountable for their part in allowing and spreading disinformation. Facebook particularly profits from highly polarising content as higher engagement leads to higher advertising pay-outs for the platform.[73] The company formerly known as Twitter also stopped enforcing its policy on coronavirus misinformation in 2022[74] and fired a third of their global trust and safety team in 2023.[75] Anonymity and privacy do not lead to disinformation and extremism, a lack of social media platform policies does.[76] Secondly, data resistance does not argue for total online anonymity. Instead, its proponents argue that users should have a say in the collection and use of their data.[77] Online services should minimise data collection and enable user discretion regarding data processing. If not, data resistors argue that users should be empowered to use their strategies and tools to reclaim their digital agency.[78] As a result, this section only focuses on the countering arguments against privacy-enhancing technologies (the tools of data resistance) and increasing awareness of the digital divide (people unable to resist) which may prevent marginalised and vulnerable populations from engaging in data resistance.

Unfortunately, the tools and strategies of resistance, Tor browser,[79] ad blockers,[80] and end-to-end encryption,[81] mentioned in this paper are also used by criminals and terrorist organisations. End-to-end encryption (E2EE), a tool that encourages freedom of speech by preventing unauthorised access to telephone calls, text messages, and personal data, is used to hide child abuse.[82] Europol also argues that encryption impedes criminal investigations.[83] However, in their analysis of 25,366 Dutch court judgments from 2015-2020, Hartel and Van Wegberg found that prosecutors are just, 'as successful in convicting offenders who rely on E2EE as those who do not,' suggesting that encryption does not obstruct criminal justice.[84] Encrypted messaging apps even prevent women from unjust prosecution[85] for receiving abortions,[86] an act of bodily autonomy that is legal or decriminalised in 67 countries.[87]

The Dark Web is additionally mischaracterised as a haven for illegal drug sales and online hate.[88] These things do happen on the Dark Web,[89] but law enforcement officers are quickly catching up.[90] Users of the Dark Web even see it as 'not intrinsically criminogenic' and rather use it as a tool to further their freedom of expression.[91] The social stigma around the Dark Web and end-to-end encryption should not discourage data activists. Instead of outlawing these tools, policymakers should encourage their responsible use and advertise the ways data activists use these tools to shape a better society.

Another challenge to data resistance is the digital divide or, 'the gap between those who have and do not have access to computers and the Internet.'[92] The term expanded over time to include the quality of internet access and individuals' education in communication technology.[93] Data resistance

72 Ramos, E.F. & Blind, K. (2020) Data portability effects on data-driven innovation of online platforms: Analyzing Spotify. *Telecommunications Policy*. 44 (9), 102026.

73 Lauer, D. (2021) Facebook's ethical failures are not accidental; they are part of the business model. *AI and Ethics*. 1 (4), 395–403.

74 BBC (2022) *Twitter ends Covid misinformation policy under Musk*. 30 November 2022. BBC.

75 Brewster, T. (2024) *Musk's X Fired 80% Of Engineers Working On Trust And Safety, Australian Government Says*. 10 January 2024. Forbes.

76 Hao, K. (2021) *How Facebook and Google fund global misinformation*. 20 November 2021. MIT Technology Review.

77 Redden, J. (2018) The harm that data do. *Scientific American*. 319 (5), 76.

78 Treré, E. (2016) The Dark Side of Digital Politics. 127–138.

79 The Tor Project Inc. (n.d.) *The Tor Project*.

80 Wills, C.E. & Uzunoglu, D.C. (2016) What ad blockers are (and are not) doing. pp. 72–77.

81 Greenberg, A. (2014) *Hacker Lexicon*.

82 McAleenan, K.K., Barr, W.P., Dutton, P. & Patel, P. (2019) *Open letter from the Home Secretary alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg*.

83 Koomen, M. (2019) The encryption debate in the European Union. *Carnegie Endowment for International Peace*.

84 Hartel, P. & Van Wegberg, R. (2023) Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. *Crime Science*. 12 (1), 5.

85 Martin, Z.C., Riedl, M.J. & Woolley, S.C. (2023) How pro- and anti-abortion activists use encrypted messaging apps in post- Roe America. *Big Data & Society*. 10 (2).

86 Kelly, H., Hunter, T. & Abril, D. (2022) Seeking an abortion? Here's how to avoid leaving a digital trail. 26 June 2022. *The Washington Post* [Accessed: 6 March 2024].

87 Centre for Reproductive Rights (n.d.) The World's Abortion Laws. [Accessed: 6 March 2024].

88 Jardine, E. (2015) The Dark Web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series*. (21).

89 Europol (2023) *288 dark web vendors arrested in major marketplace seizure*. 2 May 2023.

90 Greenberg, A. (2022) *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. Doubleday & Co Inc.

91 Mirea, M., Wang, V. & Jung, J. (2019) The not so dark side of the darknet: a qualitative study. *Security Journal*. 32 (2), 102–118.

92 Van Dijk, J.A.G.M. (2006) Digital divide research, achievements and shortcomings. *Poetics*. 34 (4–5), 221–235.

93 Lythreatis, S., Singh, S.K. & El-Kassar, A.-N. (2022) The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*. 175, 121359.

still requires comprehensive technical knowledge and connection to digitally active communities which limits and excludes those with unequal access to information technology. A study by Gran et al. into awareness of algorithms found that there are three large divides, an age divide where younger respondents were more aware of algorithms than older respondents, a gender divide where male-identifying respondents were more aware of algorithms than female-identifying respondents, and an education divide where more traditionally educated respondents were more aware of algorithms than less educated respondents.[94] These results support previous results by Cotter and Reisman et al. who argue more people will recognise the damaging effects of algorithms as more people encounter them.[95] Overcoming these divides to both educate the unaware and include the unaware will be important for data resistance given that all individuals are affected by privacy-violating algorithms and data practices regardless of their awareness.

Conclusion and policy provocations

Even though the examples presented in this paper show activists around the world resisting privacy-violating algorithms and data practices, it is important to note that individual and collective data resistance must not be the only way government and corporate power is challenged. Extensive public regulation is needed to effectively deal with the problems of our digital society. The UK Online Safety Act, European Union Digital Services Act, Digital Markets Act and General Data Protection Regulation (GDPR) are all steps in the right direction. However, more regulatory action is required globally that is informed by data resistance and promotes the principles and strategies of data resistance.

It is beyond the scope of this paper to present a fully developed policy proposal, but policy action is required to support data resistance and to create a more equitable landscape that does not rely on the unpaid labour of marginalised and vulnerable populations. Instead, I present three brief, policy provocations: imposing a data tax, introducing participatory governance to data regulation, and establishing digital identity sovereignty. The first two provocations, imposing a data tax and introducing participatory governance to data regulation, apply prior policy successes to a datafied society while the third provocation, establishing digital identity sovereignty, is thoroughly supported by data activists and computer security experts.

Imposing a data tax

Privacy-violating algorithms and data practices are negative externalities of the data economy. Negative externalities are an economic concept that captures the cost of one party making another party worse off—particularly regarding environmental economics and the societal cost of greenhouse gases.[96] Legal scholar Omri Marian argues that data creates monetary value which remains uncaptured by current taxation systems; 'the analysis, manipulation, and utilisation of large quantities of dispersed data' provides new value to corporations beyond basic collection methods.[97] In consequence, the negative externality of these practices is the lack of compensation being provided to the individuals whose data build this excess value. Adam Thimmsesch, in their analysis of the United States tax system, additionally found that current tax instruments prevent data practices from being taxed.[98]

Therefore, to collect lost taxes and to incentivise more equal data practices, a new tax should be considered for corporations and governments that collect, analyse, manipulate, and utilise individual data as their main business model. A data tax would not be a fine, it would be proportional to the company size and the amount of profits the digital service derives from a user's data. The tax would be applied to the entire digital economy, not just one company as a fine would. A tax would also be an addition to existing and future regulations. Europe's GDPR does not prevent the collection and usage of personal data, it regulates it. An additional data tax would be imposed on the digital economy for simply collecting and processing data. The funds collected from these data taxes could go to ensuring compliance with data regulations.

Enabling participatory governance of data regulation

Additionally, the creation of data regulations should bring everyone affected by the data economy into the discussion.[99] Participatory governance, or 'the democratic mechanisms which are intended to involve citizens in public policy-making processes,' and deliberative democracy, or 'the idea that legitimate law-making [arises] from the public deliberation of citizens', are two answers to this.[100] Participatory governance of data regulation is necessary to design regulation which does not violate individual and collective freedoms. When Barcelona began to experiment with technology to transform

94 Gran, A.-B., Booth, P. & Bucher, T. (2021) To be or not to be algorithm aware: a question of a new digital divide? *Information, Communication & Society*. 24 (12), 1779–1796.

95 Cotter, K. (2020) *Algorithmic Knowledge Gaps: A New Dimension of (Digital) Inequality*.; Reisman, D., Schultz, J., Crawford, K. & Whittaker, M. (2018) Algorithmic impact assessments: A practical framework for public agency. AI Now. 9.

96 Sandmo, A. (2024) *Optimal Taxation in the Presence of Externalities.*

97 Marian, O. (2021) Taxing Data. BYU L. *Rev.* 47, 511.

98 Thimmesch, A.B. (2016) Transacting in data: Tax, privacy, and the new economy. *Denv*. L. Rev. 94, 145.

99 Reisman, D., Schultz, J., Crawford, K. & Whittaker, M. (2018) Algorithmic impact assessments.

100 Smith, G. (2019) Reflections on the theory and practice of democratic innovations. In: S. Elstub & O. Escobar (eds.). *Handbook of Democratic Innovation and Governance.* Edward Elgar Publishing. p.

itself into a smart city, they created a digital participatory platform for citizens, called Decidim,[101] that resulted in over 70% of the city government's agenda deriving from proposals argued for by online and offline citizens.[102]

Deliberative democracy is another mechanism of citizen inclusion,[103] such as in the example of the Danish Board of Technology which runs citizen meetings which incorporate citizens' views on 'how to protect public health and the environment in the face of uncertainty about the risks of a technology, innovation, or product.'[104] Implementations of democratic innovations are abundant around the world,[105] and appropriating them for more inclusive data governance will create data regulations that incorporate and support the experience, techniques, and strategies of data resistors. Since these democratic innovations welcome all citizens, their implementation will also empower diverse voices to govern our digital society.

Establishing self-sovereign identity

Finally, individuals should have more control over their data and what happens to it. Digital sovereignty is a wide-ranging concept[106] that encompasses national sovereignty over data captured within their nation,[107] collective control over data captured from indigenous populations,[108] and individual ownership over their data.[109] The latter, self-sovereign identity, intends to synthesise various identity systems from digital services to allow individuals to control access to their identity across the entire digital economy.[110] Unlike the ad-hoc methods of resistance that activists use to reclaim their data after collection, establishing self-sovereign identity pre-emptively solidifies the principles of data resistance through cryptography.

Databox[111] and Solid[112] are two current technologies that empower users to manage their personal data. The Databox is 'a personal networked device…[which] is configured to be able to access a user's personal data from a variety of sources… [and] serves as a platform upon which the processing of personal data can be done locally.'[113] The Databox would then be able to interact with digital services, such as music and social media platforms while being completely in control of their personal data. Similarly, Solid 'lets individuals and groups store their data securely in decentralised data stores called Pods' which 'its owners control which people and applications can access it.'[114] A growing list of applications allow owners of Solid Pods to message one another, manage their health records, and track their note-taking.[115] Supporting the development of self-sovereign identity technologies and compelling digital services to adopt them will empower individuals to securely manage and selectively share their data with trusted parties while retaining the ability to revoke access or delete their data at any time.

Final thoughts

Increased individual and collective agency, autonomy, and empowerment, strengthened democratic values, equality and justice, and stimulated market competition are all possibilities of a *good* digital society. These prospects are only made possible by supporting data resistance which enables citizens to resist privacy-violating algorithms and data practices. Our digital society is fuelled by the collection, analysis, and usage of digital citizens' data, and marginalised and vulnerable populations are unequally at risk of the resulting discrimination, surveillance, and lack of representation. While data-driven societies expose all members of the public to algorithms and data practices that violate privacy, marginalised and vulnerable groups are more susceptible to the harms of these socio-technical systems. However, these issues are not unique to our digital society, they are reflections of our real-life one. Data resistance offers a way out by surfacing inequalities, subverting datafication, and producing alternatives within the digital economy. Encouraging data resistance technically, socially, and politically will not only create a good *digital* society but a good *democratic* one.

Acknowledgements

The author is grateful to Leonie Tanczer for the discussions and feedback that shaped this discussion paper. This work was also supported by the British Academy's Public Policy Team dedicated to the theme of Digital Society and the UK EPSRC grant EP/S022503/1.

101 Ajuntament de Barcelona (n.d.) *Decidim Barcelona*. [Accessed: 6 March 2024].
102 Bria, F. (2019) *BUILDING DIGITAL CITIES FROM THE GROUND UP BASED AROUND DATA SOVEREIGNTY AND PARTICIPATORY DEMOCRACY: THE CASE OF BARCELONA*.
103 Setälä, M., Smith, G. & others (2018) Mini-publics and deliberative democracy. *The Oxford handbook of deliberative democracy*. 300–314.
104 Palsberg, A., Gram, S., Drivdadal, L.E., Van der Sluijs, J.P., Damianova, Z., Kazorev, V., Declich, G., Edelenbosch, R., Verhoef, P. & Tijs Sikma (2020) *Citizens' values and opinions in relation to Precaution and Innovation*.
105 Smith, G. (2021) *Can democracy safeguard the future?* John Wiley & Sons.
103 Setälä, M., Smith, G. & others (2018) Mini-publics and deliberative democracy. *The Oxford handbook of deliberative democracy*. 300–314.
104 Palsberg, A., Gram, S., Drivdadal, L.E., Van der Sluijs, J.P., Damianova, Z., Kazorev, V., Declich, G., Edelenbosch, R., Verhoef, P. & Tijs Sikma (2020) *Citizens' values and opinions in relation to Precaution and Innovation*.
105 Smith, G. (2021) *Can democracy safeguard the future?* John Wiley & Sons.
106 Amoore, L. (2018) Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography*. 42 (1), 4–24.
107 Tan, K.L., Chi, C.-H. & Lam, K.-Y. (2024) Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. *ACM Computing Surveys*. 56 (3), 1–36.
108 Kukutai, T. & Taylor, J. (2016) *Indigenous data sovereignty: Toward an agenda*. ANU press.
109 Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021) Data sovereignty: A review. *Big Data & Society*. 8 (1).
110 Preukschat, A. & Reed, D. (2021) *Self-sovereign identity*. Manning Publications.
111 Amar, Y., Haddadi, H. & Mortier, R. (2016) Privacy-aware infrastructure for managing personal data. In: *Proceedings of the 2016 ACM SIGCOMM Conference*. 2016 pp. 571–572.
112 Solid Project (n.d.) *Solid*. Solid Project. [Accessed: 29 March 2024].
113 Amar, Y., Haddadi, H. & Mortier, R. (2016) Privacy-aware infrastructure. pp. 571–572.
114 Solid Project (n.d.) *Solid*.
115 Solid Project (n.d.) *Solid*.

References

ACLU (2013) The NYPD Muslim Surveillance Program.

Ajuntament de Barcelona (n.d.) Decidim Barcelona. [Accessed: 6 March 2024].

Amar, Y., Haddadi, H. & Mortier, R. (2016) Privacy-aware infrastructure for managing personal data. In: Proceedings of the 2016 ACM SIGCOMM Conference. 2016 pp. 571–572.

Amoore, L. (2018) Cloud geographies: Computing, data, sovereignty. Progress in Human Geography. 42 (1), 4–24.

Andrejevic, M. & Gates, K. (2014) Big Data Surveillance: Introduction. Surveillance & Society. 12 (2), 185–196.

Arora, P. (2019) General data protection regulation—A global standard? Privacy futures, digital activism, and surveillance cultures in the Global South. Surveillance & Society. 17 (5), 717–725.

Baack, S. (2015) Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. Big Data & Society. 2 (2).

Baaz, M., Lilja, M., Schulz, M. & Vinthagen, S. (2016) Defining and Analyzing "Resistance": Possible Entrances to the Study of Subversive Practices. Alternatives: Global, Local, Political. 41 (3), 137–153.

Balkin, J.M. (n.d.) Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society. NEW YORK UNIVERSITY LAW REVIEW. 79.

BBC (2022) Twitter ends Covid misinformation policy under Musk. 30 November 2022. BBC.

Benjamin, G. (2022) #FuckTheAlgorithm: algorithmic imaginaries and political resistance. In: 2022 ACM Conference on Fairness, Accountability, and Transparency. June 2022 Seoul Republic of Korea, ACM. pp. 46–57.

Bergé, J.-S., Grumbach, S. & Zeno-Zencovich, V. (2018) The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance. European Journal of Comparative Law and Governance. 5 (2), 144–178.

Bonini, T., Treré, E., Yu, Z., Singh, S., Cargnelutti, D. & López-Ferrández, F.J. (2023) Cooperative affordances: How instant messaging apps afford learning, resistance and solidarity among food delivery workers. Convergence: The International Journal of Research into New Media Technologies.

Brandom, R. (2018) Designing for the crackdown. 25 April 2018. The Verge.

Brewster, T. (2024) Musk's X Fired 80% Of Engineers Working On Trust And Safety, Australian Government Says. 10 January 2024. Forbes.

Bria, F. (2019) BUILDING DIGITAL CITIES FROM THE GROUND UP BASED AROUND DATA SOVEREIGNTY AND PARTICIPATORY DEMOCRACY: THE CASE OF BARCELONA.

Burgess, M., Schot, E. & Geiger, G. (2023) This Algorithm Could Ruin Your Life, WIRED.

Centre for Data Ethics and Innovation (2022) Public attitudes to data and AI: Tracker survey.

Centre for Reproductive Rights (n.d.) The World's Abortion Laws. [Accessed: 6 March 2024].

Cobbe, J. (2021) Algorithmic Censorship by Social Platforms: Power and Resistance. Philosophy & Technology. 34 (4), 739–766.

Cotter, K. (2020) Algorithmic Knowledge Gaps: A New Dimension of (Digital) Inequality.

Danaher, J. (2019) The Ethics of Algorithmic Outsourcing in Everyday Life. In: Algorithmic Regulation. Oxford University Press. pp. 98–118.

David, E. (2024) Threads' API is coming in June. 1 March 2024. The Verge. [Accessed: 6 March 2024].

DeVito, M.A., Gergle, D. & Birnholtz, J. (2017) 'Algorithms ruin everything': \#{RIPTwitter}, Folk Theories, and Resistance to Algorithmic Change in Social Media. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. May 2017 Denver Colorado USA, ACM. pp. 3163–3174.

Van Dijk, J.A.G.M. (2006) Digital divide research, achievements and shortcomings. Poetics. 34 (4–5), 221–235.

Dogruel, L., Facciorusso, D. & Stark, B. (2022) 'I'm still the master of the machine.' Internet users' awareness of algorithmic decision-making and their perception of its effect on their autonomy. Information, Communication & Society. 25 (9), 1311–1332.

Dufva, T. & Dufva, M. (2019) Grasping the future of the digital society. Futures. 107, 17–28.

Ellis, J.R. (2022) Blurred consent and redistributed privacy: owning LGBTQ identity in surveillance capitalism. In: Diversity in Criminology and Criminal Justice Studies. Emerald Publishing Limited. pp. 183–196.

Engels, B. (2016) Data portability among online platforms. Internet Policy Review. 5 (2).

Ettlinger, N. (2018) Algorithmic affordances for productive resistance. Big Data & Society. 5 (1), 205395171877139.

Eubanks, V. (2018) Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

Europol (2023) 288 dark web vendors arrested in major marketplace seizure. 2 May 2023.

Fouquaert, T. & Mechant, P. (2022) Making curation algorithms apparent: a case study of 'Instawareness' as a means to heighten awareness and understanding of Instagram's algorithm. Information, Communication & Society. 25 (12), 1769–1789.

Fung, A. (2009) Empowered participation: Reinventing urban democracy. Princeton University Press.

Gal, M.S. (2018) Algorithmic challenges to autonomous choice. Mich. Tech. L. Rev. 25, 59.

Gillespie, T. (2014) The relevance of algorithms. Media technologies: Essays on communication, materiality, and society. 167 (2014), 167.

Gran, A.-B., Booth, P. & Bucher, T. (2021) To be or not to be algorithm aware: a question of a new digital divide? Information, Communication & Society. 24 (12), 1779–1796.

Greenberg, A. (2014) Hacker Lexicon: What is End-To-End Encryption? 25 November 2014. Wired.

Greenberg, A. (2022) Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency. Doubleday & Co Inc.

Gstrein, O.J. & Beaulieu, A. (2022) How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology. 35 (1), 3.

Guardian Project (n.d.) Guardian Project. [Accessed: 6 March 2024].

Hampton, L.M. (2021) Black feminist musings on algorithmic oppression. arXiv preprint arXiv:2101.09869.

Hao, K. (2021) How Facebook and Google fund global misinformation. 20 November 2021. MIT Technology Review.

Hartel, P. & Van Wegberg, R. (2023) Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. Crime Science. 12 (1), 5.

Hill, K. (2022) Deleting Your Period Tracker Won't Protect You. 30 June 2022. The New York Times.

Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021) Data sovereignty: A review. Big Data & Society. 8 (1).

Jamieson, J. & Yamashita, N. (2023) Escaping the Walled Garden? User Perspectives of Control in Data Portability for Social Media. Proceedings of the ACM on Human-Computer Interaction. 7 (CSCW2), 1–27.

Jardine, E. (2015) The Dark Web dilemma: Tor, anonymity and online policing. Global Commission on Internet Governance Paper Series. (21).

Kapsch, P.H. (2022) Exploring user agency and small acts of algorithm engagement in everyday media use. Media International Australia. 183 (1), 16–29.

Karizat, N., Delmonaco, D., Eslami, M. & Andalibi, N. (2021) Algorithmic Folk Theories and Identity: How TikTok Users Co-Produce Knowledge of Identity and Engage in Algorithmic Resistance. Proceedings of the ACM on Human-Computer Interaction. 5 (CSCW2), 1–44.

Kazansky, B. (2021) 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data & Society. 8 (1).

Kelly, H., Hunter, T. & Abril, D. (2022) Seeking an abortion? Here's how to avoid leaving a digital trail. 26 June 2022. The Washington Post. [Accessed: 6 March 2024].

Kennedy, H., Poell, T. & Van Dijck, J. (2015) Data and agency. Big Data & Society. 2 (2).

Keyes, O. (2018) The misgendering machines: Trans/HCI implications of automatic gender recognition. Proceedings of the ACM on human-computer interaction. 2 (CSCW), 1–22.

Koomen, M. (2019) The encryption debate in the European Union. Carnegie Endowment for International Peace.

Krämer, J. (2021) Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations. Journal of Competition Law & Economics. 17 (2), 263–308.

Krämer, J., Senellart, P. & de Streel, A. (2020) ECONOMIC IMPLICATIONS AND REGULATORY CHALLENGES.

Kröger, J.L., Lindemann, J. & Herrmann, D. (2020) How do app vendors respond to subject access requests? A longitudinal privacy study on iOS and Android Apps. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020 pp. 1–10.

Kubitschko, S. (2015) The Role of Hackers in Countering Surveillance and Promoting Democracy. Media and Communication. 3 (2), 77–87.

Kukutai, T. & Taylor, J. (2016) Indigenous data sovereignty: Toward an agenda. ANU press.

Lam, W.M.W. & Liu, X. (2020) Does data portability facilitate entry? International Journal of Industrial Organization. 69, 102564.

Lauer, D. (2021) Facebook's ethical failures are not accidental; they are part of the business model. AI and Ethics. 1 (4), 395–403.

Lehtiniemi, T. & Ruckenstein, M. (2019) The social imaginaries of data activism. Big Data & Society. 6 (1).

Lerner, A., He, H.Y., Kawakami, A., Zeamer, S.C. & Hoyle, R. (2020) Privacy and activism in the transgender community. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020 pp. 1–13.

Lyon, D. (2003) Surveillance as social sorting: Privacy, risk, and digital discrimination. Psychology Press.

Lythreatis, S., Singh, S.K. & El-Kassar, A.-N. (2022) The digital divide: A review and future research agenda. Technological Forecasting and Social Change. 175, 121359.

Marian, O. (2021) Taxing Data. BYU L. Rev. 47, 511.

Martin, Z.C., Riedl, M.J. & Woolley, S.C. (2023) How pro- and anti-abortion activists use encrypted messaging apps in post-Roe America. Big Data & Society. 10 (2).

Mayer, J.R. & Mitchell, J.C. (2012) Third-Party Web Tracking: Policy and Technology. In: 2012 IEEE Symposium on Security and Privacy. May 2012 San Francisco, CA, USA, IEEE. pp. 413–427.

McAleenan, K.K., Barr, W.P., Dutton, P. & Patel, P. (2019) Open letter from the Home Secretary alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg.

Metcalfe, P. & Dencik, L. (2019) The politics of big borders: Data (in) justice and the governance of refugees. First Monday.

Milan, S. (2015) From social movements to cloud protesting: the evolution of collective identity. Information, Communication & Society. 18 (8), 887–900.

Milan, S. & Velden, L. Van Der (2016) The Alternative Epistemologies of Data Activism. Digital Culture & Society. 2 (2), 57–74.

Milioni, D.L. & Papa, V. (2022) The oppositional affordances of data activism. Media International Australia. 183 (1), 44–59.

Mirea, M., Wang, V. & Jung, J. (2019) The not so dark side of the darknet: a qualitative study. Security Journal. 32 (2), 102–118.

MyData Global (n.d.) MyData. [Accessed: 6 March 2024].

Obermeyer, Z., Powers, B., Vogeli, C. & Mullainathan, S. (2019) Dissecting racial bias in an algorithm used to manage the health of populations. Science. 366 (6464), 447–453.

Palsberg, A., Gram, S., Drivdadal, L.E., Van der Sluijs, J.P., Damianova, Z., Kazorev, V., Declich, G., Edelenbosch, R., Verhoef, P. & Tijs Sikma (2020) Citizens' values and opinions in relation to Precaution and Innovation.

Preukschat, A. & Reed, D. (2021) Self-sovereign identity. Manning Publications.

Pybus, J., Coté, M. & Blanke, T. (2015) Hacking the social life of Big Data. Big Data & Society. 2 (2).

Ramos, E.F. & Blind, K. (2020) Data portability effects on data-driven innovation of online platforms: Analyzing Spotify. Telecommunications Policy. 44 (9), 102026.

Redden, J. (2018) The harm that data do. Scientific American. 319 (5), 76.

Reisman, D., Schultz, J., Crawford, K. & Whittaker, M. (2018) Algorithmic impact assessments: A practical framework for public agency. AI Now. 9.

Sandmo, A. (2024) Optimal Taxation in the Presence of Externalities.

Setälä, M., Smith, G. & others (2018) Mini-publics and deliberative democracy. The Oxford handbook of deliberative democracy. 300–314.

Shen, H., DeVos, A., Eslami, M. & Holstein, K. (2021) Everyday Algorithm Auditing: Understanding the Power of Everyday Users in Surfacing Harmful Algorithmic Behaviors. Proceedings of the ACM on Human-Computer Interaction. 5 (CSCW2), 1–29.

Smith, G. (2021) Can democracy safeguard the future? John Wiley & Sons.

Smith, G. (2019) Reflections on the theory and practice of democratic innovations. In: S. Elstub & O. Escobar (eds.). Handbook of Democratic Innovation and Governance. Edward Elgar Publishing. p.

Solid Project (n.d.) Solid. Solid Project [Accessed: 29 March 2024].

Syrmoudis, E., Mager, S., Kuebler-Wachendorff, S., Pizzinini, P., Grossklags, J. & Kranz, J. (2021) Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. Proceedings on Privacy Enhancing Technologies. 2021 (3), 351–372.

Tan, K.L., Chi, C.-H. & Lam, K.-Y. (2024) Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. ACM Computing Surveys. 56 (3), 1–36.

Tanczer, L.M., López-Neira, I. & Parkin, S. (2021) 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. Journal of Gender-Based Violence. 5 (3), 431–450.

The Chaos Computer Club (n.d.) The Chaos Computer Club. [Accessed: 6 March 2024].

The Tor Project Inc. (n.d.) The Tor Project. [Accessed: 6 March 2024].

Thimmesch, A.B. (2016) Transacting in data: Tax, privacy, and the new economy. Denv. L. Rev. 94, 145.

Treré, E. (2016) The Dark Side of Digital Politics: Understanding the Algorithmic Manufacturing of Consent and the Hindering of Online Dissidence. IDS Bulletin. 41 (1), 127–138.

Turner, S., Quintero, J.G., Turner, S., Lis, J. & Tanczer, L.M. (2020) The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. New Media & Society.

U.K. Aid Match (2020) Defining marginalised – the Foreign, Commonwealth & Development Office's 'Leaving no one behind' agenda.

U.K. Information Commissioner's Office (n.d.a) Legal definitions. Information Commissioner's Office.

U.K. Information Commissioner's Office (n.d.b) Right of access. Right of access [Accessed: 6 March 2024].

U.K. Information Commissioner's Office (n.d.c) Right to data portability. [Accessed: 6 March 2024].

Van Der Velden, L. (2015) Forensic devices for activism: Metadata tracking and public proof. Big Data & Society. 2 (2), 205395171561282.

Velkova, J. & Kaun, A. (2021) Algorithmic resistance: media practices and the politics of repair. Information, Communication & Society. 24 (4), 523–540.

Vincent, N., Li, H., Tilly, N., Chancellor, S. & Hecht, B. (2021) Data Leverage: A Framework for Empowering the Public in its Relationship with Technology Companies. In: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. March 2021 Virtual Event Canada, ACM. pp. 215–227.

Wäscher, T. (2020) Framing resistance against surveillance: Political communication of privacy advocacy groups in the "Stop Watching Us" and "The Day We Fight Back" campaigns. In: Journalism, Citizenship and Surveillance Society. Routledge. pp. 113–130.

Wills, C.E. & Uzunoglu, D.C. (2016) What ad blockers are (and are not) doing. In: 2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb). 2016 IEEE. pp. 72–77.

Wohlfarth, M. (2019) Data Portability on the Internet: An Economic Analysis. Business & Information Systems Engineering. 61 (5), 551–574.

Xie, X., Du, Y. & Bai, Q. (2022) Why do people resist algorithms? From the perspective of short video usage motivations. Frontiers in Psychology. 13, 941640.

Yee, K., Tantipongpipat, U. & Mishra, S. (2021) Image cropping on twitter: Fairness metrics, their limitations, and the importance of representation, design, and agency. Proceedings of the ACM on human-computer interaction. 5 (CSCW2), 1–24.

Youmans, W.L. & York, J.C. (2012) Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. Journal of Communication. 62 (2), 315–329.

Zhao, L. (2023) Filter Bubbles? Also Protector Bubbles! Folk Theories of Zhihu Algorithms Among Chinese Gay Men. Social Media + Society. 9 (2).

Züger, T., Milan, S. & Tanczer, L.M. (2015) FCJ-192 Sand in the Information Society Machine: How Digital Technologies Change and Challenge the Paradigms of Civil Disobedience. The Fibreculture Journal. (26 2015: Entanglements–Activism and Technology).

Zwiebelmann, Z. & Henderson, T. (2021) Data Portability as a Tool for Audit. In: Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers. September 2021 Virtual USA, ACM. pp. 276–280.