12: GOVERNANCE OF COMMUNAL DATA SHARING

CHIH-HSING HO [1] AND TYNG-RUEY CHUANG [2]

Introduction

The rapid development of the data economy calls for innovative research into its social and ethical impacts. When enormous opportunities emerge along with making use of vast amounts of data, challenges are generated and concerns arise around monopoly and market enclosure. Current legal and regulatory frameworks for data protection fail to address these devastating problems. By focusing on consent and the anonymisation of data, these legal techniques echo the neoliberal methods of governance which promise individual autonomy and choice as an advanced liberal strategy. This article proposes theoretical and computational approaches to the analysis of an alternative data sharing model, which is based on community participation in decision making and self-governance. We consider several examples, such as user data cooperatives and collaborative data projects, to further explore how a community is formed and how the governance of communal data sharing is being established. We will then develop frameworks for the governance of communal data sharing by combining common pool resource management and a socio-legal perspective on the commons.

Today we see many states as well as *private* initiatives to promote a *data*-driven industrial revolution across the globe. Data, said to be like oil a century ago, has been cast as a new type of resource fuelling an emerging, lucrative digital-era industry.[3] However, the wealth derived from this digital revolution is not being evenly distributed. According to a study by the Economist, all five of the most valuable listed companies in the world - Apple, Alphabet (Google's parent company), Amazon, Facebook and Microsoft are tech titans.[4] Digital wealth is being monopolized and concentrated in very few hands. Such dominance has led to such side effects as unfair competition, manipulation, routine intrusion of privacy, and the undermining of democracy.[5] These tech giants provide the infrastructure undergirding much of the data economy, and stand to gain the most from it. Although most of their services appear to be free, what underlies the transactions of the digital economy is an exchange of services for control over data. The challenges posed by capitalist accumulation of data raise the question: is this monopoly inevitable?

---

1 Assistant Research Fellow, Institute of European and American Studies, Academia Sinica, Taipei Taiwan; LLM (Columbia), JSM (Stanford), PhD in Law (LSE), Email: chihho@sinica.edu.tw (corresponding author).

2 Associate Research Fellow, Institute of Information Science, Academia Sinica, Taipei, Taiwan, PhD (NYU), Email: trc@iis.sinica.edu.tw.

3 'The world's most valuable resource is no longer oil, but data', *The Economist*, 6 May 2017.

4 'Tech firms hoard huge cash piles', *The Economist,* 3 June 2017.

5 An example can be illustrated by the Facebook scandal, see: Tam Adams, 'Facebook's week of shame: the Cambridge Analytica fallout', *The Guardian,* 24 March 2018, https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence.

How are we to imagine and create different systems, fairer systems featuring greater participatory control?

This article proposes theoretical and computational approaches to the analysis of an alternative data sharing model, which is based on community participation in decision making and self-governance. When we talk about 'community', we use this term in a non-conventional way. We try not to see community as a fixed group or a predefined collective identity. Rather, it refers to a set of ongoing engagement and practices of group making.[6] In other words, it is this dynamic process of community making - acts of mutual support, negotiation and experimentation, as David Bollier has argued - that are needed to build innovative systems to manage shared resources.[7] Along with these curiosities, we consider several examples, such as user data cooperatives[8] and collaborative data projects,[9] to further explore how a community is formed and how the governance of communal data sharing is being established. We will then develop frameworks for the governance of communal data sharing by combining common pool resource management and a socio-legal perspective on the commons.

Data for All? A Communal Approach

Historically, the governance of shared resources has challenged many great minds. For those who hold the view that competitive market promotes economic efficiency, the privatization of shared resources is one of the best ways to achieve their goal. As promoting efficiency is the core value under this endeavor, *how* the surplus is generated and *who* makes decision about its distribution are not central concerns of capitalists. That said, the social practice of commoning is a political-economic alternative to standard capitalist practice.[10] For commoners, what is more important is the *fair* conditions under which surplus is produced, and that the decision making about the surplus to be distributed involves those who take part in the process of production.[11] Applying the idea of the commons to the data economy, this participatory form of data sharing addresses the well-being of others through a process of democratizing ownership.[12] But the differences between the market and the commons go even beyond participation. Commoners need to communicate with one another to develop the norms, protocols or rules that govern access and the management of shared resources they co-own. In this process of commoning, all parties are stakeholders and are equally affected and bound by the governing rules they discuss, negotiate and then agree upon.

---

6 J.K Gibson-Graham et al, 'Cultivating Community Economies' (2017), https://thenextsystem.org/cultivating-community-economies: 5.

7 David Bollier, 'Commoning As A Transformative Social Paradigm', the Next System Project (2016).

8 For example, see Trebor Scholz and Nathan Schneider (eds), *Ours to hack and to own: The rise of platform cooperativism, a new vision for the future of work and a fairer internet*, New York: OR Books, 2017.

9 For more information on this, see: *2016 Workshop on Collaborative Data Projects,* held at Academia Sinica, Taipei, Taiwan, 8 Dec 2016, http://odw.tw/2016/.

10 Ibid.

11 J.K Gibson-Graham et al, p. 14.

12 David Bollier, 'Reclaiming the commons', *Boston Review* 27.3-4 (2002).

By taking responsibility and claiming entitlement to form and govern the common pool, commoners develop spaces of ethical and social connection. It is such ongoing social relationships that help build distinct communities in which commoners form their own subjectivities.

Current legal and regulatory frameworks for data protection fail to address the devastating problem of market enclosure. By focusing on consent and the anonymisation of data, these legal techniques echo the neoliberal methods of governance which promise individual autonomy and choice as an advanced liberal strategy. The Facebook-Cambridge Analytical scandal is one example of the inadequacy of these mechanisms in which trust was breached when Facebook failed to perform its role as a dutiful data controller by allowing Cambridge Analytical, a third party user, to access user data for very different purposes than that agreed to by data subjects who contributed their data only to access free services provided by Facebook. A communal data sharing model can be an alternative providing a bottom-up initiative to address these challenges.[13] However, how to set up this adequate model remains an issue yet to be solved. On the one hand, an effective system is required to encourage the establishing of incentives for data sharing within the community in a confidential and trustful manner. On the other hand, commoners have to recognise the need to differentiate between the degree of confidentiality within and outside of the communal boundaries. In this paper we will investigate and develop normative principles and computational frameworks to fully address these issues.

For communal data sharing, we refer to a communal approach of data management where members of a community voluntarily pool their data together to create a common pool for mutual benefits.[14] This common pool of data acts as a common resource of collective ownership to be accessed by third party users when properly aggregated and distilled according to its governance framework, which is initiated and agreed by all members of the community. Usually, three main actors are involved in data governance - data subjects, data controllers (and processors), and third party data users. Although data subjects contribute data, it is up to data controllers to decide how data is accessed and processed. In most cases, third party users who plan to access the data pool may hold very different, if not conflicting, interests from the data subjects. In reality, it becomes difficult for data subjects to trace and verify if data controllers have fulfilled their duties and the promises made prior to data collection.

What challenges this conventional model of data governance is that the three actors - data subjects, data controllers, and data users - do not share common views and interests on how they wish the data to be shared and reused. In practice, a common approach is for data controllers to anonymize personal data before the data to be released, and/or adopt restricted access model so that only certain users or queries are allowed to access data warehouses. However, this operation is not without limitations. As data science makes progress, thorough

13 Yves-Alexandre de Montjoye, Ce´sar A. Hidalgo, Michel Verleysen and Vincent D. Blondel, 'Unique in the crowd: The privacy bounds of human mobility', *Scientific Reports* 3 (2013): 1376.

14 Chao-Min Chiu, Meng-Hsiang Hsu and Eric T.G. Wang, 'Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories', *Decision Support Systems* 42.3 (December, 2006): 1872-1888.

anonymisation may not be possible when risks of re-identification remain.[15] As for restricting data access on a case-by-case basis, meeting the different expectations and requirements of data subjects and third party users challenges the possibility of stakeholders negotiating and agreeing to their data governing rules.

A Decentralized & Self-Governance Model

A communal approach to data sharing aims to create a decentralized model under which data subjects and data controllers are united rather than separated.[16] In other words, norms and principles for data use can be decided upon data subjects who are members of the community. Also, it is up to them to negotiate how their data shall be collected and used, as well as who can access to this communal data pool. Several notable experiments illustrate this kind of peer-based information production and sharing. Wikipedia,[17] OpenStreetMap,[18] and Social.Coop[19] are examples. They demonstrate that data can be aggregated, shared and managed by the peers themselves for the maximum of communal benefits. In addition, these initiatives also show that data management can be achieved from the bottom-up through grass root efforts.

Take Social.Coop as a case study. It is a social network platform operated through Mastodon,[20] a free and open-source software for microblogging. The operation of Mastodon is done via open protocols as its main purpose is to provide a decentralized alternative to commercial, monopolizing services in communication. Mastodon emphasizes a distributed and federated network of peer communication nodes. Attracted by its ethical design and non-commercial characteristic, Mastodon has been used by many communities to provide a service platform of no data advertising, mining and no walled gardens. Social.Coop follows these similar non-commercial and non-monopoly principles and operates itself as a co-operative microblogging service based on Mastodon. Its co-op operation emphasizes democratic principles of transparency and participation. In practice, it relies on several functional committees composed by members to establish a code of conduct and other policies in order to reach collective decisions for platform governance. All members of the Social.Coop are entitled to co-manage the platform where the community is served, and to take part in creating their own bylaws. The philosophy behind such self-governance model is to foster trust by means that increase data subjects' control over their data management based on their co-ownership.

Under this communal based, self-governance framework, the aggregated data becomes a common-pool resource. Its management is governed by community norms and bylaws set up by the peers who contribute to the data pool. Aggregation, distribution, and all other data management tasks can be facilitated by this open and transparent system. Further, all the

15 Latanya Sweeney, 'K-anonymity: A model for protecting privacy', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* 10.5 (October, 2002): 557-570.
16 Ibid.
17 Wikipedia, https://www.wikipedia.org/.
18 OpenStreetMap, http://www.openstreetmap.org/.
19 Social.Coop, https://social.coop/about.
20 Mastodon, https://mastodon.social/about.

source code of the entire information system of this communal design is open and free for everyone to review and improve upon. Based on these cases of communal data sharing, we will further propose norms, principles and techno designs to help lead to success of the communal data sharing model.

Governing the Data Commons

The Data Commons generates important benefits in terms of building civic trust and shared commitments. The question is how to govern such a commons to make it sustainable. This is perhaps the main challenge we would face while finding ways to protect not only the interests of individual members, but also the integrity of the community, namely the shared resource itself. David Bollier has studied the origins of free software and the Creative Commons licenses. He found that although commoners may assert different notions of social norms and community boundaries, there is one similarity among them, and that is the use of the commons to connect people.[21] For Bollier, a commons serves not only as a shared resource, but appeals to something very deep in humanity. How have commoners organized to build their commons, such as online communities, to improve data management and reclaim their common wealth remains an interesting question worthy of further study.

Garrett Hardin argued in his famous 1968 essay 'The Tragedy of the Commons'[22] that the commons is a failed management regime as when everything is free for the taking, the common resource will be overused. He proposed that the best solution to this tragedy is to allocate private property rights to the resource in question. However, what Hardin observed is not really a commons but an open, or we can say unlimited access, regime. The main difference between the two is that in a commons, commoners share a mutual interest to maintain their shared resources. This common expectation helps form a distinct community, which is lacking in the unlimited access regime in which people do not interact with one another and therefore there is no community consensus being formed. Later, economist Elinor Ostrom offered eight principles based on which she thinks that a commons can be governed in a more sustainable and equitable way.[23] These principles are proposed in order to address issues associated with the tragedy of the commons. Several questions were raised to be considered: what are mechanisms to incentivise sharing? What ways can benefits be fairly distributed? What are the methods to enforce the boundary of a group? What workable procedures are available to form censuses and decisions, among others?

21 David Bollier, *Viral Spiral: How the Commoners Built a Digital Republic of Their Own*, New York: The New Press, 2009.

22 Garrett Hardin, 'The Tragedy of the Commons', *Science* 162 (1968): 1243-1248

23 Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press, 1990.

Here are Ostrom's eight principles for the governance of a commons:[24]

1. Define clear group boundaries;
2. Match rules governing use of common goods to local needs and conditions;
3. Ensure that those affected by the rules can participate in modifying the rules;
4. Make sure the rule-making rights of community members are respected by outside authorities;
5. Develop a system, carried out by community members, for monitoring members' behavior;
6. Use graduated sanctions for rule violators;
7. Provide accessible, low-cost means for dispute resolution, and;
8. Build responsibility for governing the common resource in nested tiers from the lowest level up to the entire interconnected system.

After further analysis, it is found that these principles may well apply not only to classic common-pool resources (CPRs), which are made available to all by consumption but access to which are limited by high costs (e.g. fishing grounds and irrigation system), but also to intangible information resources, such as knowledge and data (e.g. software programs).[25] Free software, whose source code is distributed under licenses like the GNU General Public Licenses (GPL),[26] is an example of information commons. A GPL'ed software package can be used and improved upon by anyone, and the enhancements to the package are also free for all to reuse due to the copyleft nature of GPL. The GPL license can be viewed as a way to set up boundaries. GPL'ed software is free for all to use, and such freedom cannot be revoked. However, in general, data is not copyrightable. Although some jurisdictions have sui generis database rights, similar copyleft database licenses have been developed. For example, the Open Database License (ODbL)[27] has been used to set a boundary for OpenStreetMap datasets.

When individuals are willing to pool their data for mutual benefits, similar arrangements can be made to purposely restrict the information flow of the pool. While GPL and ODbL aim to ensure that improvements are free for all to reuse, the pool needs to remain within the community boundary unless other arrangements have been made. Issues such as how to formulate suitable data restriction polices, and how to effectively enforce them, are central to any data sharing community. In addition, due to the sensitivity of personal data, each individual may only want to share partial data to the pool, and/or to remain anonymous when sharing the data.

In addition, there are some proprietary structural designs being developed to improve cooperative legalities in the management of shared resources. A general asset lock is one example. It is often used in the common ownership to set out a number of conditions to prevent residual

24 Ibid.
25 Charlotte Hess and Elinor Ostrom (eds), *Understanding Knowledge as a Commons: From Theory to Practice*, Cambridge MA: MIT Press, 2006.
26 GNU General Public License, Version 3, http://www.gnu.org/licenses/gpl-3.0.en.html.
27 ODC Open Database License (ODbL) Summary, http://opendatacommons.org/licenses/odbl/summary/.

assets to be distributed amongst members when the organisation winds up.[28] But it also allows members to vote to change these provisions in the governing document to convert the nature of the organisation from a co-operative into a company. On the contrary, a statutory asset lock includes provisions in the governing document in a prescribed format to incorporate an organisation under specific legislation.[29] It sets out conditions so that assets can only be used for the benefit of the community on dissolution of the organisation or be transferred outside of a community interest company (CIC) when the prescribed requirements are satisfied.[30] These mechanisms of proprietary designs help not only address problems of the tragedy of the commons, but also provide a possible resolution for the sustainability of the commons.

Computational Methods

There are several computational methods that can be used to facilitate communal data sharing while maintaining confidentiality of data subjects. When members share their private data with others in a community, they often wish to ensure that their contributions are confidential, at least to some degree. For example, they may not want their identities to be revealed by other members in the same group. Even if, under certain circumstances, they have to reveal their identities to the group, they may not wish to disclose the same to those who are outside of the group. When members' data leaves the boundaries of the community for third party reuse, the data must be properly de-identified to keep the data subjects anonymous. In some cases, such de-identification efforts are futile, as even de-identified datasets can still reveal characteristics of the entire community that is harmful to every member of the group. For example, an anonymized dataset could reveal that many data subjects come from higher income groups (e.g. by their shopping habits and/or ZIP codes) or are susceptible to a particular disease (e.g. by the characteristics and/or areas of their upbringing).

These examples show that confidentiality is contextual and relative. A person may be more willing to trust others in her or his own community, but not feeling the same for those who are outside of the group. Data use within the group, therefore, shall be treated differently than that used outside of the community. When people form an ad hoc community to share personal information about themselves (e.g. drug abuse), a certain degree of anonymity is warranted; but they may still need ways to identify one another in the group just to be able to communicate with each other properly and in context. As for communication with others outside of the group, however, member anonymity must be maintained. Now, considering a situation where members can leave and join an ad hoc group freely and at any time, maintaining workable group boundaries turns out to be crucial if members are to be adequately protected.

---

28 For example, at the dissolution of the commons, commoners must pass assets on to another common ownership enterprise or choose to retain them within the sector, otherwise donate them to charity if either of these is not possible.

29 Alex Nicholls, https://www.sciencedirect.com/science/article/pii/S0361368209000798#!, 'Institutionalizing Social Entrepreneurship in Regulatory Space: Reporting and Disclosure by Community Interest Companies', *Accounting, Organisations and Society* 35.4 (2010): 394-415.

30 Rory Ridley-Duff, 'Communitarian Perspectives on Social Enterprise', *Corporate Governance: An International Review* (March 2007).

Likewise, there is a need to call for suitable methods for auditing the communal data sharing system. While maintaining confidentiality, members of a community would still want to ensure that their data is, and will always be, incorporated accurately and in full into the communal data pool. In addition, they need ways to validate that other members' contributions are authentic.[31] When the communal data pool is considered to be common resources, the community may want to keep track of contributions from its members and to make sure that members access the resource accordingly. This communal data pool needs to be used wisely by people both within and outside of the group. We shall also emphasize that in many scenarios, auditability needs to be achieved when data are anonymised.

Here we list several computational methods that can be used for trustful group communications. Many of these methods involve parties who would like to cooperate anonymously to produce verifiable outcomes. A typical scenario, for example, is to ask a group of strangers to form a consensus without meeting face-to-face, and that each be able to verify later that a certain consensus has been reached without knowing the opinions offered by others. Below we exemplify three areas of this promising research.

- **Secure multiparty computation** is a subfield of cryptography that aims to provide methods for multiple parties to jointly compute a function over their private values without revealing them.[32] For example, two employees can use a private equality test to see if they are paid the same while not revealing the amount of one's own salary. There are several methods for such a test. Methods for secure multiparty computation have been used for privacy-preserving data mining.

- **Open-audit e-voting** is with regard to developing protocols and systems for online voting in which each voter gains assurance that his or her vote was correctly cast, and any observer can verify that all cast votes were properly counted. Helios[33] is a protocol and a Web-based system for open-audit voting.[34] It is shown that one can set up an election on the Web using Helios, and invite voters to cast a secret ballot, compute a tally, and generate a validity proof for the entire process. In many cases, a group can use secret ballot voting to aggregate sensitive information and to form consensus, such as selecting a leader to the group while not revealing the preference of anyone involved.

- **User-centric online services** let Web users keep their personal data in their own devices and/or on storage servers that act as intermediaries to other online services. The data is likely stored encrypted. When user data is requested by a Web site, for example, while a user is logging into a social media site, encrypted user data is sent to the site on a need-to-know basis and decrypted. Sieve is such a system.[35] Dissent is a general protocol

31 Susan J. Eggers and Tor E. Jeremiassen, 'Eliminating False Sharing', *ICPP* (1991).

32 Carsten Baum et al, 'Publicly Auditable Secure Multi-Party Computation', *the 9th International Conference on Security and Cryptography for Networks, Lecture Notes in Computer Science,* vol. 8642, Springer, 2014.

33 Helios, https://heliosvoting.org/.

34 Ben Adida, 'Helios: Web-based Open-Audit Voting', *the 17th USENIX Security Symposium*, 2008.

35 Frank Wang et al, 'Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds',

offering provable anonymity and accountability for group communication .[36] It addresses the need to balance between provably hiding the identities of well-behaved users, while provably revealing the identities of disruptive users.

Confidentiality and auditability requirements are highly contextual. While these computational methods and systems are effective in their respective application domains, they may not meet the communication needs in a communal setting for data sharing. Many of the existing methods assume two kinds of actors: individuals and their adversaries. The assumption often is that every individual acts only for oneself. In a communal setting, there are various data sharing communities, and an individual can belong to many different groups. As each community may have its own data sharing policy (intra-group and inter-group), we anticipate that existing methods may require combination and/or use in layers to effectively address technical problems arising from communal sharing of personal data.

Here, we use a hypothetical example to further illustrate how the above computational methods can be used together to initiate and facilitate group communication concerning sensitive personal information. Suppose that there was an outbreak of disease in a population, but people were not willing to share their personal information. For those suspecting that they were exposed to similar hazards, they may be more willing to communicate with one another. Secure multiple-party computation methods can be developed to allow people to check whether they have a similar travel history - countries visited in last six months, for example, but without revealing where they went exactly. Open-audit e-voting methods will then allow these people to aggregate and share information without revealing their identities ('write in' one's major medical conditions and make tallies, for example). After the vote and tally, and based on the outcome, some people may be more willing to engage in group conversations (though remain private among themselves). In such a case, user-centric online services can be deployed to help host such conversations.

Conclusion

The rapid development of the data economy calls for innovative research into its social and ethical impacts. When enormous opportunities emerge along with making use of vast amounts of data, challenges are generated and concerns arise around monopoly and market enclosure. We need to ensure that the rapidly developing data economy evolves in fair and justifiable ways. In order to make possible this goal, it is crucial that an innovative, bottom-up and de-centralized data governance framework be designed, through which a trustful space arises such that all stakeholders are able to fruitfully engage and take responsibility for their communities.

13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, USA, 16-18 March 2016.

36 Ewa Syta et al, 'Security Analysis of Accountable Anonymity in Dissent', *ACM Transactions on Information and System Security* 17.1 (2014).

A communal data sharing model is established based on these principles. By forming a communal data pool, each member of the community is entitled to take her or his entitlement and participates in the collective decision-making on an equal footing. This involves also incorporating collective ownership in data governance frameworks. The central aspect of engagement facilitates communication among members of the community. Such initiative relies not only on an effective information system, but also on the process of commoning through which a collective identity is formed. In contrast to the conventional data protection framework paying primary attention to consent and data anonymisation, the communal data sharing model emphasizes the amount of control that individual subjects have over their data. It also deals with who may have access to data in the communal pool, and with whom such data may be shared. We therefore propose a communal data sharing model to help create fairer platforms for everyone who takes part in this brave new data-driven revolution.

Acknowledgements

This study is supported by Academia Sinica's three-year thematic project 'Socially Accountable Privacy Framework for Secondary Data Usage' under grant number AS-TP-106-M06. The authors would like to thank the editors and two anonymous reviewers for their constructive suggestions and comments.

References

Adams, Tam. 'Facebook's week of shame: the Cambridge Analytica fallout', *The Guardian,* 24 March 2018.

Adida, Ben. 'Helios: Web-based Open-Audit Voting', *USENIX security symposium*, 28 July-1 August 2008, https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf.

Angiuli, Olivia, Joe Blitzstein and Jim Waldo. 'How to de-identify your data', *Queue* 13 (8, September-October 2015): 20, https://dl.acm.org/citation.cfm?id=2838930.

Baum, Carsten, Ivan Damgård and Claudio Orlandi. 'Publicly Auditable Secure Multi-Party Computation', *International Conference on Security and Cryptography for Networks*, Springer, Cham, 3-5 September 2014, https://eprint.iacr.org/2014/075.pdf.

Bollier, David. 'Commoning as a transformative social paradigm'. *The Next System Project,* 2016, http://www.operationkindness.net/wp-content/uploads/David-Bollier.pdf.

_____. 'Reclaiming the commons', *Boston Review* 27 (3-4, 2002).

_____. *Viral Spiral: How the Commoners Built a Digital Republic of Their Own*, New York: The New Press, 2009, http://barcelonacomuns.pbworks.com/f/Viral+Spiral_How+the+Commoners+Built+a+Digital+Republic+of+Their+Own+%5Bdavid+bollier%5D.pdf.

Chiu, Chao-Min, Meng-Hsiang Hsu and Eric T.G. Wang. 'Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories', *Decision Support Systems* 42.3 (December 2006): 1872-1888.

De Montjoye, Yves-Alexandre, Ce´sar A. Hidalgo, Michel Verleysen and Vincent D. Blondel. 'Unique in the crowd: The privacy bounds of human mobility', *Scientific Reports* 3 (2013): 1376.

Eggers, Susan J. and Tor E. Jeremiassen. 'Page-level Affinity Scheduling for Eliminating False Sharing'. *ICPP* (1995), https://pdfs.semanticscholar.org/34fe/b586363fead853fa7e7d6dc5678d1159a8be.pdf?_ga=2.132910156.372523520.1542619879-1465787887.1542619879.

Garrett Hardin. 'The Tragedy of the Commons', *Science* 162 (1968): 1243-1248.

Gibson-Graham, J.K., Jenny Cameron, Kelly Dombroski, Stephen Healy and Ethan Miller. 'Cultivating Community Economies', 2017, https://thenextsystem.org/cultivating-community-economies.

GNU General Public License, Version 3, http://www.gnu.org/licenses/gpl-3.0.en.html.

Helios, https://heliosvoting.org/.

Hess, Charlotte and Elinor Ostrom (eds). *Understanding Knowledge as a Commons: From Theory to Practice*, Cambridge MA: MIT Press, 2006.

Kosba, Ahmed, Andrew Miller, Elaine Shi and Zikai Wen. 'Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts', *2016 IEEE Symposium on Security and Privacy (SP),* California, USA 22-26 May 2016, https://ieeexplore.ieee.org/document/7546538.

Lane, Julia, Victoria Stodden, Stefan Bender and Helen Nissenbaum (eds). *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Cambridge: Cambridge University Press, 2014.

Mastodon, https://mastodon.social/about.

Nicholls, Alex. 'Institutionalizing social entrepreneurship in regulatory space: Reporting and disclosure by community interest companies', *Accounting, Organizations and Society*, 35 (4, 2010): 394-415.

ODC Open Database License (ODbL) Summary, http://opendatacommons.org/licenses/odbl/summary/.

OpenStreetMap, http://www.openstreetmap.org/.

Ostrom, Elinor. *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press, 1990.

Ridley Duff, Rory. 'Communitarian perspectives on social enterprise', *Corporate governance: an international review,* 15.2 (2007): 382-392.

Satoshi, Nakamoto. 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008), https://bitcoin.org/bitcoin.pdf.

Scholz, Trebor and Nathan Schneider (eds). *Ours to hack and to own: The rise of platform cooperativism, a new vision for the future of work and a fairer internet*, New York: OR Books, 2017.

Social.Coop, https://social.coop/about.

Solon, Olivia. 'Facebook says Cambridge Analytica may have gained 37m more users' data', *The Guardian*, 4 April 2018.

Summers, Hannah and Nicola Slawson, 'Investigators complete seven-hour Cambridge Analytica HQ search', *The Guardian*, 24 March 2018.

Sweeney, Latanya. 'K-anonymity: A model for protecting privacy', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.5 (October 2002): 557-570.

Syta, Ewa, et al. 'Security analysis of accountable anonymity in Dissent', *ACM Transactions on Information and System Security (TISSEC),* 17.1 (2014): 4.

Tene, Omer and Jules Polonetsky. 'Big data for all: Privacy and user control in the age of analytics', *Nw. J. Tech. & Intell. Prop.* 11 (2013): xxvii.

'The world's most valuable resource is no longer oil, but data', *The Economist*, 6 May 2017.

'Tech firms hoard huge cash piles,' *The Economist,* 3 June 2017.

Wang Frank et al. 'Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds', *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation*, Santa Clara, CA, USA, 16-18 March 2016, https://www.usenix.org/sites/default/files/nsdi16_full_proceedings.pdf.

Wicks, Paul et al. 'Sharing health data for better outcomes on PatientsLikeMe', *Journal of medical Internet research,* 12.2 (June 2010), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2956230/.

Wikipedia, https://www.wikipedia.org/.

Wilkinson, Mark D et al. 'The FAIR Guiding Principles for scientific data management and stewardship', *Scientific Data* 3 (March 2016).

Workshop on Collaborative Data Projects, Academia Sinica, Taipei, Taiwan. 8 Dec 2016, http://odw.tw/2016/.

GOOD DATA

EDITED BY
ANGELA DALY,
S. KATE DEVITT
& MONIQUE MANN

Theory on Demand #29
Good Data

Editors: Angela Daly, S. Kate Devitt and Monique Mann

Copy editor: Harley Williams
Editorial assistant: Kayleigh Murphy

Funding: Queensland University of Technology Faculty of Law

Cover design: Katja van Stiphout
Design and EPUB development: Barbara Dubbeldam

Published by the Institute of Network Cultures, Amsterdam, 2019

ISBN 978-94-92302-27-4

Contact
Institute of Network Cultures
Phone: +3120 5951865
Email: info@networkcultures.org
Web: http://www.networkcultures.org

This publication is available through various print on demand services and freely downloadable from http://networkcultures.org/publications

CONTENTS

THEME 3: GOOD DATA AS OPEN AND SHARED DATA

THEME 4: GOOD DATA ACTIVISM AND RESEARCH

THEME 5: GOOD DATA AND SMART CITIES AND HOMES

Theory on Demand #29
Good Data

Moving away from the strong body of critique of pervasive 'bad data' practices by both governments and private actors in the globalized digital economy, this book aims to paint an alternative, more optimistic but still pragmatic picture of the datafied future. The authors examine and propose 'good data' practices, values and principles from an interdisciplinary, international perspective. From ideas of data sovereignty and justice, to manifestos for change and calls for activism, this collection opens a multifaceted conversation on the kinds of futures we want to see, and presents concrete steps on how we can start realizing good data in practice.

Angela Daly is a transnational and critical socio-legal scholar of the regulation of new technologies. She is currently based in the Chinese University of Hong Kong Faculty of Law and holds adjunct positions at Queensland University of Technology Faculty of Law (Australia) and the Tilburg Institute of Law, Technology and Society (Netherlands).

S. Kate Devitt is a philosopher and cognitive scientist working as a social and ethical robotics researcher for the Australian Defence Science and Technology Group. She is an Adjunct Fellow in the Co-Innovation Group, School of Information Technology and Electrical Engineering, University of Queensland. Her research includes: the ethics of data, barriers to the adoption of technologies, the trustworthiness of autonomous systems and philosophically designed tools for evidence-based, collective decision making.

Monique Mann is the Vice Chancellor's Research Fellow in Technology and Regulation at the Faculty of Law, Queensland University of Technology. Dr Mann is advancing a program of socio- legal research on the intersecting topics of algorithmic justice, police technology, surveillance, and transnational online policing.

Printed on Demand
ISBN: 978-94-92302-28-1

Institute of network cultures