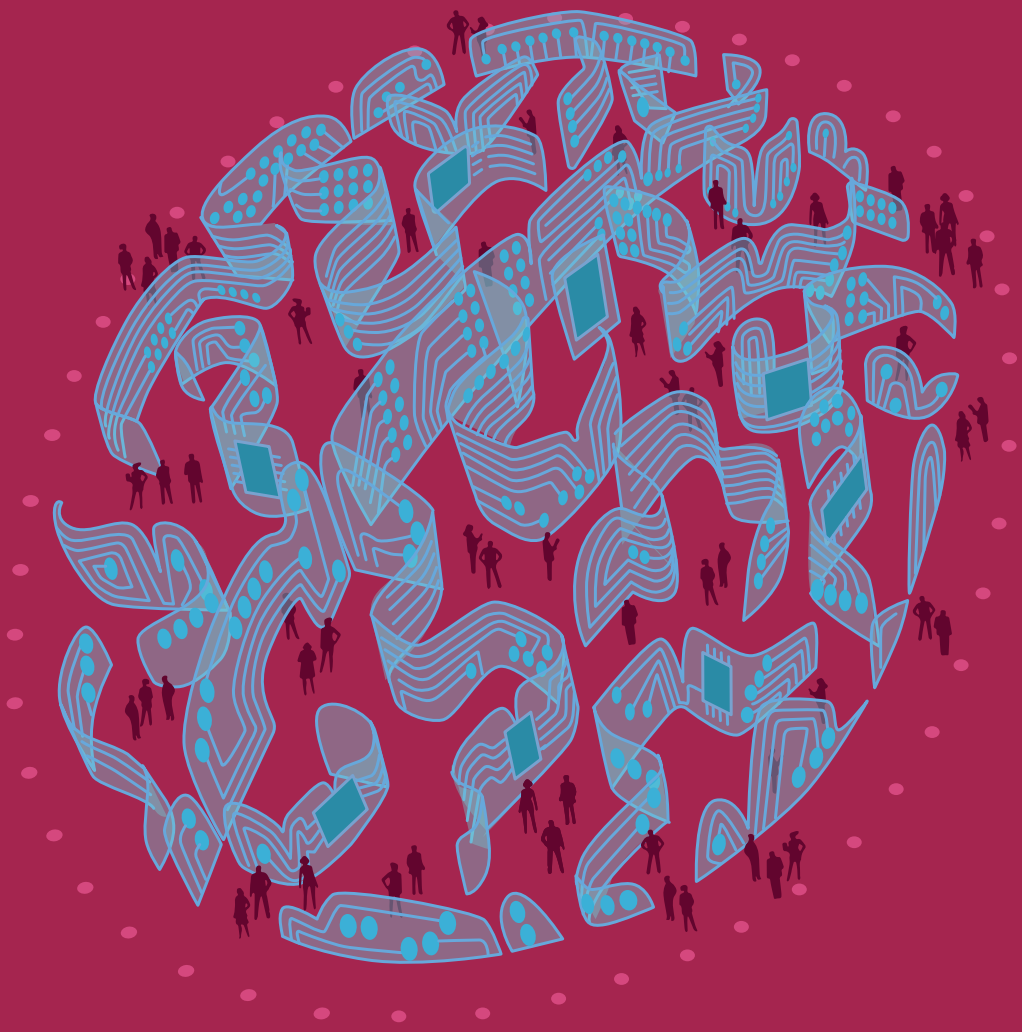
GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development



Association for Progressive Communications (APC),
Article 19, and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch

2019

Global Information Society Watch 2019
Artificial intelligence: Human rights, social justice and development

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

GISWatch 2019 advisory committee
Namita Aavriti (APC)
Rasha Abdul Rahim (Amnesty International)
Alex Comninos (Research ICT Africa)
Malavika Jayaram (Digital Asia Hub)
J. Carlos Lara (Derechos Digitales - América Latina)
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)
Andrew Lowenthal (EngageMedia)
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)
Valeria Milanes (Asociación por los Derechos Civiles)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch.
We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)
Anita Gurumurthy and Nandini Chami (IT for Change)
Rasha Abdul Rahim (Amnesty International)

APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19
for their support for Global Information Society Watch 2019.

Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

Towards data governance that empowers the public

Philip Dawson and Grace Abuhamad
Element AI
https://hello.elementai.com/data-trusts.html

Introduction

If the Cambridge Analytica scandal served as the public's "great privacy awakening,"[1] for public policy experts it affirmed several troubling messages about human vulnerability given the current state of the governance of big data and artificial intelligence (AI) systems. What started as a legitimate academic research project quickly became scandalous when a British political consulting firm used the data collected – from up to 87 million people's Facebook profiles – for a different purpose: to influence the 2016 United States (US) election through targeted political advertisements.

The data transfer occurred without consent from Facebook's users or, arguably, even Facebook itself, reinforcing the idea that big data and AI systems pose significant threats not only to the right to privacy, but to the enjoyment of human rights and the integrity of democratic institutions.[2] As the scandal unfolded, and the European Union's General Data Protection Regulation and the Council of Europe's modernised Convention 108+ entered into force, experts cautioned that in the absence of new approaches to data governance, even a new a "bill of data rights" could not check the power imbalances between data controllers and data subjects.[3] Facebook's refusal to attend hearings before the International Grand Committee on Big Data, Privacy and Democracy, even under subpoena, points to the urgency of finding new ways of dealing with the platform's power.

Current approaches to data governance suffer from a lack of transparency and accountability, in part because big data – in combination with AI – continues to make end runs around consent and privacy self-management.[4] AI-enabled methods of analysis can be used by companies to generate, infer and collect sensitive information about people that they have neither provided nor confirmed.[5] Companies have access to an array of data collection methods, some of which circumvent consent without detection: data is now, as the Cambridge Analytica case demonstrated, extracted through online profiling, purchased from third-party brokers, or derived from aggregated data sets. The complexity and opacity of information flows make it virtually impossible for individuals to discern, much less self-manage, the risks or rights they engage when consenting to the use of their personal data.[6]

Another problem is that current approaches to data governance tend to concentrate data in the hands of powerful digital platforms, preventing the public from sharing in its value.[7] In today's digital society, individuals serve as the inputs to AI systems and yet they wield little control over its outputs. While exceptional, scandals like Cambridge Analytica prove the following rule: not only do current approaches to governing data exclude (most) individuals from sharing in its value, but they expose them to human rights abuses, too.

1 Lapowsky, I. (2019, 17 March). How Cambridge Analytica Sparked the Great Privacy Awakening, *Wired*, https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening

2 Kaye, D. (2018). *Report of the Special Rapporteur to the General Assembly on AI and its impact on freedom of opinion and expression*. https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportGA73.aspx; Privacy International, & ARTICLE 19. (2018). *Privacy and Freedom of Expression in the Age of Artificial Intelligence*. https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence

3 Tisne, M. (2018, 14 December). It's time for a Bill of Data Rights. *MIT Technology Review*. https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights; Wylie, B. (2019, 30 January). Why we need data rights: 'Not everything about us should be for sale'. *Financial Post*. https://business.financialpost.com/technology/why-we-need-data-rights-not-everything-about-us-should-be-for-sale

4 Barocas, S., & Nissenbaum, H. (2014). Computing Ethics: Big Data's End Run Around Procedural Privacy Protections. *Communications of the ACM, 57*(11). https://nissenbaum.tech.cornell.edu/papers/Big%20Datas%20End%20Run%20Around%20Procedural%20Protections.pdf

5 Kaye, D. (2018). Op. cit.

6 Solove, D. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review, 126*(7); Rau, S. (2018, 16 October). Free, Informed and Unambiguous Consent in the Digital Age: Fiction or Possibility? *The Human Rights, Big Data and Technology Project*. https://hrbdt.ac.uk/free-informed-and-unambiguous-consent-in-the-digital-age-fiction-or-possibility

7 Element AI, & Nesta. (2019). *Data Trusts: A new tool for data governance*. https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf

Accordingly, an increasing proportion of policy workshops, discussions and research over the last year have focused on designing inclusive data governance models that facilitate public accountability and promote a more equitable distribution of data's economic value.[8] While a number of novel approaches have been considered, proposals based on fiduciary models of data governance have garnered significant attention. This report provides a brief overview of current research and policy discussions related to two such proposals – "information fiduciaries", which aim to improve the accountability of online platforms, and "data trusts", a flexible governance tool that is being considered for a range of different purposes – while offering an assessment of their unique value propositions and implementation challenges.

Information fiduciaries

The nature of fiduciary relationships and the precise duties they create is a contested subject.[9] Yet as Richard Whitt notes, "all definitions of fiduciaries share three main elements: (1) the entrustment of property or power; (2) the entrustors' trust of fiduciaries; and (3) the risk to entrustors emanating from the entrustment."[10] As such, the information fiduciary proposal recommends raising the intensity of obligations owed by data controllers (i.e. companies) to data subjects (i.e. individuals) through the imposition of fiduciary duties of care, confidentiality and loyalty, which would transform large data controllers like digital platforms into "information fiduciaries". The intent is to correct the power imbalance between companies and individuals by giving companies duties similar to those held by doctors, lawyers and accountants towards their patients or clients.

While scholars such as Lillian Edwards[11] and Jack M. Balkin[12] may be credited for first considering the imposition of fiduciary obligations, albeit through different methods, their approach has faced some criticism.[13] Whereas Edwards has suggested that fiduciary obligations are "implied"[14] whenever a data subject shares personal data with a data controller, on account of the risk the former exposes her- or himself to, Sylvie Delacroix and Neil Lawrence argue that taking up a duty of loyalty to manage data subjects' rights in their best interests would place data controllers in a conflict of interest with their competing duty to maximise shareholder value.[15]

To resolve this tension, Balkin has proposed that special immunities or financial incentives could help induce data controllers to take up a limited fiduciary obligation that could be defined by statute.[16] Several problems have been identified with this "grand bargain".[17] Special incentives for platforms to behave as fiduciaries may not be enough to nullify the conflict of interest between a platform's duty of loyalty to manage data subjects' rights and its duty of loyalty to shareholders.[18] As Delacroix and Lawrence have put it:

> [T]he "information fiduciary" proposed by Balkin would be placed in a position that is comparable to that of a doctor who gains a commission on particular drug prescriptions or a lawyer who uses a company to provide medical reports for his clients while owning shares in that company.[19]

Mike Godwin has argued that a "professional framework of fiduciary obligations for tech companies" supported by "professional codes of ethical conduct that bind the tech companies that have fiduciary duties to us" could be one way of ensuring platforms take their positions as information fiduciaries seriously.[20]

Balkin's recommendation to restrict digital platforms' fiduciary duties unfairly discounts the intangible vulnerabilities of living in an online world, where privacy and human rights violations routinely go unnoticed or unchallenged. Facebook may not be a doctor or YouTube an accountant,

8 Delacroix, S., & Lawrence, N. (2019). Bottom-up Data Trusts: disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law*. https://doi.org/10.1093/idpl/ipz014; Element AI, & Nesta. (2019). Op. cit.

9 McDonald, S. (2019, 5 March). Reclaiming Data Trusts. *Centre for International Governance Innovation*. https://www.cigionline.org/articles/reclaiming-data-trusts

10 Whitt, R. (2019, 26 July). Old School Goes Online: Exploring Fiduciary Obligations of Care and Loyalty in the Platforms Era. *SSRN*. https://ssrn.com/abstract=3427479

11 Edwards, L. (2004). The Problem with Privacy. *International Review of Law, Computers & Technology*, *18*(3), 263-294.

12 Balkin, J. M. (2016). Information Fiduciaries and the First Amendment. *UC Davis Law Review,49*(4).

13 McDonald, S. (2019, 5 March). Op. cit.; Delacroix, S., & Lawrence, N. (2019). Op. cit.; Khan, L., & Pozen, D. E. (2019). A Skeptical View of Information Fiduciaries. *Harvard Law Review, 133*, Forthcoming. https://ssrn.com/abstract=3341661

14 Edwards, L. (2004). Op. cit.

15 Delacroix, S., & Lawrence, N. (2019). Op. cit.

16 Balkin, J. M. (2016). Op. cit.; Zittrain, J. (2013). Engineering an Election. *Harvard Law Review Forum, 127*.

17 Balkin, J. M., & Zittrain, J. (2016, 3 October). A Grand Bargain to Make Tech Companies Trustworthy. *The Atlantic*. https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346

18 Khan, L., & Pozen, D. E. (2019). Op. cit.

19 Delacroix, S., & Lawrence, N. (2019). Op. cit.

20 Godwin, M. (2018, 16 November). It's Time to Reframe Our Relationship With Facebook. *Slate*. https://slate.com/technology/2018/11/information-fiduciaries-facebook-google-jack-balkin-data-privacy.html?wpsrc=sh_all_dt_tw_ru; Godwin, M. (2018, 26 November). If Facebook is really at war, the only way to win is to put ethics first. *Washington Post*. https://www.washingtonpost.com/outlook/2018/11/26/if-facebook-is-really-war-only-way-win-is-put-ethics-first

and yet each handles sensitive personal data that has been entrusted to them, and which can expose individuals, as entrustors, to abuse.[21] Balkin's position may be further undermined in his characterisation of data controllers' limited duty of loyalty as a prohibition from "act[ing] like con men"[22] or creating "an unreasonable risk of harm to their end user":[23] corporations already bear a duty to do no harm under tort law duty of care. This aspect of Balkin's proposal has led Lina Khan and David Pozen to question whether Balkin's proposal "is a fiduciary approach in any meaningful sense at all," and, ultimately, to recommend that competition and antitrust policy may be the more productive channel to explore.[24]

While the imposition of fiduciary obligations on data controllers may have been realistic in the past – when business models were less entrenched and operations less complex – today they are unlikely to broker meaningful change. For example, would a fiduciary duty model have prevented the misuse of personal data in the Cambridge Analytica scandal? Moreover, as Whitt observes, the forcible imposition of fiduciary obligations tends to produce suboptimal results, creating relationships of "grudging" care or loyalty.[25] To this end, Whitt posits that the market may one day privilege companies who voluntarily compete around the self-imposition of a positive duty of loyalty.[26] Yet such a prospect would likely depend on a clear signal that the market value of assuming a positive duty of loyalty outweighs the status quo, and on the emergence of alternative service providers. Absent important changes in the competitive landscape surrounding data controllers, neither of these developments is likely to occur, and the information fiduciary proposal will have limited impact on the power asymmetries embedded into current approaches to data governance or problems related to privacy self-management and data concentration. Structural problems such as these may require more than a light touch approach.

Data trusts

Data trusts result from the application of the common law trust to the governance of data or data rights. Trusts begin with an asset, or rights in an asset, that a "settlor" places into a trust.[27] A trust charter stipulates the purpose and terms of the trust, which exists to benefit a group of people, known as the "beneficiary". In more basic terms, a data trust creates a legal way to manage data rights for a purpose that is valuable to a beneficiary.[28]

In a data trust, data subjects would be empowered to pool the rights they hold over their personal data into the legal framework of a trust.[29] A trustee is appointed with a fiduciary obligation to manage the trust's assets in accordance with the trust charter and the interests of its beneficiaries. The trustee is accountable to the beneficiaries for the management of the trust, and has a responsibility to take legal action to protect their rights.

While there is currently no common definition for data trusts, they are often described in reference to the particular problem their proposer is aiming to solve.[30] As outlined below, governments have focused on the potential to use data trusts to promote data sharing and "responsible" innovation. The "civic data trust"[31] has been theorised as a way to protect the public interest in data governance decision-making processes. Perhaps the most expansive vision for data trusts at scale is the concept of the "bottom-up data trust",[32] which has been proposed as a way to return the power that stems from aggregated data to individuals.

To be sure, data trusts are not a governance model in and of themselves, and their effectiveness will depend on the complementary use of other tools that constitute good practice in corporate governance. Rather, data trusts provide a flexible framework that is capable of balancing a constellation of different interests or rights associated with a range of different stakeholders and use cases.

Data trusts as data-sharing vehicles

Governments' interest in data trusts has primarily focused on their potential to facilitate responsible data sharing and innovation in the AI sector. The following is a list of such proposals.

- In 2017, an independent review commissioned by the United Kingdom (UK) recommended "data

21 Balkin, J. M. (2016). Op. cit.; Balkin, J. M. (2018). Fixing Social Media's Grand Bargain. *Yale Law School*. https://ssrn.com/abstract=3266942

22 Balkin, J. M. (2018). Op. cit.

23 Ibid.

24 Khan, L., & Pozen, D. E. (2019). Op. cit.

25 Whitt, R. (2019, 26 July). Op. cit.

26 Ibid.

27 McDonald, S., & Porcaro, K. (2015, 4 August). The Civic Trust. *Medium*. https://medium.com/@McDapper/the-civic-trust-e674f9aeab43; Wylie, B., & McDonald, S. (2018, 9 October). What is a Data Trust. *Centre for International Governance Innovation*. https://www.cigionline.org/articles/what-data-trust; Delacroix, S., & Lawrence, N. (2019). Op. cit.; Element AI, & Nesta. (2019). Op. cit.

28 Element AI, & Nesta. (2019). Op. cit.

29 Delacroix, S., & Lawrence, N. (2019). Op. cit.

30 McDonald, S. (2019, 5 March). Op. cit.

31 McDonald, S., & Porcaro, K. (2015, 4 August). Op. cit.

32 Delacroix, S., & Lawrence, N. (2019). Op. cit.

trusts" as a way to "share data in a fair, safe and equitable way," adding that they would likely play an important role in growing the AI sector.[33]

- In 2018, the Open Data Institute (ODI) announced a partnership with the UK Office for Artificial Intelligence and Innovate UK to run three data trust pilots focusing on tackling illegal wildlife trade, reducing food waste and improving municipal public services.[34]
- In May 2019, the Canadian government announced a new Digital Charter[35] that referenced data trusts as a possible way to facilitate data sharing in a privacy- and security-enhancing manner for research and development purposes in areas such as health, clean technology or agribusiness. The Canadian government also included several recommendations related to data trusts in a discussion paper[36] that accompanied the Digital Charter, outlining proposals for the reform of Canada's federal privacy legislation.
- In May 2019, the Organisation for Economic Co-operation and Development adopted the OECD Principles on Artificial Intelligence (the "OECD Principles"), which recommend data trusts as a way to support the safe, fair, legal and ethical sharing of data.[37]
- In June 2019, the G20 Digital Economy Ministers incorporated the OECD's recommendation on data trusts into their "human-centred AI Principles".[38]
- Finally, that same month, the European Union High-Level Expert Group on AI (AI HLEG) published a series of policy and investment recommendations,[39] which acknowledged the need to foster the creation of "trusted data spaces" for data sharing, referencing the data trust proposals in Canada and the United Kingdom as examples.

Of particular interest in the Canadian proposal is the idea that data trusts could be used to alleviate the burden of consensual exhaustion and privacy self-management for transactions involving de-identified data. Specifically, the proposal states that "de-identified information could be processed without consent when managed by a data trust,"[40] before adding that other protections such as a "prohibition against intentional re-identification or targeting of individuals in data, or re-identification as the result of negligence or recklessness" would need to be put in place.[41] The proposal further stresses that clear linkages between statutory enforcement provisions and the oversight of a data trust would also be necessary. The proposal reflects the belief that a trustee's purpose-driven mandate, fiduciary duties and built-in accountability to beneficiaries could incentivise a level of proactive risk management that could remove the need to seek consent in subsequent data transactions with other trusts.

Civic data trusts

Civic data trusts move beyond the appointment of single trustees to build fiduciary governance structures that manage the use and sharing of rights to data on behalf of beneficiaries.[42] The purpose of a civic data trust is to embed civic values and participation processes into the governance and use of digital technologies.[43] By incorporating civic participation into the trustee organisation, civic trusts could ensure that decisions regarding the governance of data take into account evolving concepts of digital rights and the public good.[44]

Sean McDonald and Keith Porcaro identify at least three ways that a civic data trust is unique:

> [T]heir mission is to define and support the implementation of systems of public participation in decisions about data rights; the trustee organization itself must develop public participation models for its core governance decisions; and [they] can be designed to create reciprocal

33 Hall, D. W., & Pesenti, J. (2019). *Growing the Artificial Intelligence Industry in the UK*. Government of the United Kingdom. https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk.

34 Open Data Institute. (2018). *Data trusts: lessons from three pilots*. https://theodi.org/article/odi-data-trusts-report. Interestingly, though the ODI concluded that trust law was not necessary to advance these pilot projects, it has chosen to continue using the term "data trust", risking popular confusion as to whether or not a data trust should always imply the application of trust law, or whether the word "trust" is merely being used as a "marketing tool". See Delacroix, S., & Lawrence, N. (2019). Op. cit.

35 Innovation, Science and Economic Development Canada. (2019). *Canada's Digital Charter: Trust in a digital world*. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

36 Innovation, Science and Economic Development Canada. (2019). *Strengthening Privacy for the Digital Age*. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

37 https://www.oecd.org/going-digital/ai/principles

38 https://www.mofa.go.jp/files/000486596.pdf

39 High-Level Expert Group on Artificial Intelligence. (2019). *Policy and Investment Recommendations for Trustworthy Artificial Intelligence*. https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence

40 Innovation, Science and Economic Development Canada. (2019). *Strengthening Privacy for the Digital Age*. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

41 Ibid.

42 McDonald, S., & Porcaro, K. (2015, 4 August). Op. cit.; McDonald, S. (2019, 5 March). Op. cit.; McDonald, S. (2018, 17 October). Toronto, Civic Data, and Trust. *Medium*. https://medium.com/@McDapper/toronto-civic-data-and-trust-ee7ab928fb68; Element AI, & Nesta. (2019). Op. cit.

43 Ibid.

44 McDonald, S., & Porcaro, K. (2015, 4 August). Op. cit.

relationships between the public (the trust), technology companies (the licensee), and technology stakeholders.[45]

In 2018, Sidewalk Labs, a subsidiary of Alphabet, proposed to establish an "independent urban data trust"[46] to help manage the data collected as part of its planned smart city development project in the city of Toronto. While Sidewalk Labs drew a lot of attention to data trusts as a concept, their proposal was criticised for its lack of detail, failure to incorporate feedback from community organisations and residents, and for not including fiduciary obligations for the proposed trustee organisation.[47]

Bottom-up data trusts

Delacroix and Lawrence propose a bottom-up[48] approach to data trusts as a way to return the power that stems from aggregated data to individuals. Data subjects would be empowered to pool their data into a trust that would champion a social or economic benefit of their choosing.[49] Professional data trustees would exercise the data rights of beneficiaries on their behalf.[50] The data trustees would act as an independent intermediary that negotiates the terms of data collection and use between data subjects and data collectors.

As more people join a data trust, the trustee's negotiating power over the data controller would grow. In similar fashion, the pooling of data rights could act as a powerful collective action mechanism against abuse by a data controller, as trustees could exercise the right of portability on behalf of all the trust's beneficiaries and withdraw the sum of the trust's data rights en masse.

Delacroix and Lawrence envision an ecosystem of data trusts in which data subjects could choose a trust that reflects their aspirations, and be able to switch trusts when needed. Delacroix and Lawrence explore the application of bottom-up data trusts in several domains, including health care, social media, genetics, financial services and loyalty programmes.[51]

Implementation challenges

Like information fiduciaries, data trusts face their own implementation challenges. First, clarity is needed regarding the legal foundation – whether in property or contract law – that would enable data subjects to pool any rights they may have to the personal data they participate in generating into a data trust of their choosing. Without changes to the current conception of data ownership, this may represent a barrier to the availability of data trusts as a viable model in the context of online platforms.

Second, data trusts would likely require a new class of professional data trustees[52] capable of balancing competing and complex interests related to data access and use. Given the increasing scale of data transactions and potential risks, however, some question whether a single trustee or even a trustee organisation would be able to discharge the trustee's duties, or if technological solutions, such as an ecosystem of "personal AI"[53] trustees, may be necessary.

Core features of trusts, including the nature and scope of fiduciary obligations (but also their governance structures and technical architectures), will need to achieve a level of standardisation for data trusts to be deployed at scale. The Hague Convention on the Law Applicable to Trusts and on their Recognition,[54] which uses a harmonised definition of a trust, and sets conflict rules for resolving problems in the choice of the applicable law, could be a natural starting point for this conversation.

Conversely, civil law jurisdictions – where the reception of trust law is more recent and its features more fluid – may be particularly well suited to the task of adapting fiduciary models of governance to the evolving field of data rights management. The Quebec Civil Code, for instance, conceives of the trust as a universality of rights affected to a particular purpose,[55] which a trustee has positive legal powers to administer on behalf of a trustee or trustee organisation. The fact that neither the settlor, trustee or beneficiary retains rights of ownership in

45 Ibid.

46 Harvey Dawson, A. (2018, 15 October). An Update on Data Governance for Sidewalk Toronto. *Sidewalk Labs*. https://www.sidewalklabs.com/blog/an-update-on-data-governance-for-sidewalk-toronto

47 McFarland, M. (2019, 9 July). Alphabet's plans to track people in its 'smart city' ring alarm bells. *CNN Business*. https://www.cnn.com/2019/07/09/tech/toronto-sidewalk-labs-google-data-trust/index.html; Cecco, L. (2019, 11 September). 'Irrelevant': report pours scorn over Google's ideas for Toronto smart city. *The Guardian*. https://www.theguardian.com/cities/2019/sep/11/irrelevant-panel-pours-scorn-over-googles-ideas-for-toronto-smart-city; Ryan, A. (2019, 24 June). Here's how the Quayside data trust should operate. *The Star*. https://www.thestar.com/opinion/contributors/2019/06/24/heres-how-the-quayside-data-trust-should-operate.html

48 Delacroix, S., & Lawrence, N. (2019). Op. cit.

49 Delacroix, S., & Lawrence, N. (2019). Op. cit.; Element AI, & Nesta. (2019). Op. cit.

50 Delacroix, S., & Lawrence, N. (2019). Op. cit.

51 Ibid.

52 Ibid.

53 Whitt, R. (2019, 26 July). Op. cit.; Wylie, B., & McDonald, S. (2018, 9 October). Op. cit.; McDonald, S. (2019, 5 March). Op. cit.

54 https://assets.hcch.net/docs/8618ed48-e52f-4d5c-93c1-56d58a610cf5.pdf

55 Emerich, Y. (2013). The Civil Law Trust: A Modality of Ownership or an Interlude in Ownership? In L. Smith (Ed.), *The Worlds of the Trust*. Cambridge University Press; Smith, L. (Ed.). (2012). *Re-imagining the Trust: Trusts in Civil Law*. Cambridge University Press.

the asset, moreover, may remove legal barriers to the sharing or pooling of data rights.

Other important issues that require further research and testing include the accountability and liability procedures that will need to be developed in the context of data misuse, the integrity of licensing[56] in data supply chains to ensure organisations seeking to use data from a data trust do so in accordance with its terms, and the role of public institutions in defining and conducting oversight of high-level requirements for data trusts in particular sectors, for instance, to ensure data trusts themselves are not manipulated to form new oligopolies of power. Public awareness regarding the opportunity but also the risks associated with the management of their data rights, is another.

Way forward?

It is important to recall that this is not the first time society has successfully devised checks and balances capable of addressing problematic concentrations of power. Good governance in democratic political regimes – the separation of powers, for instance – has helped safeguard individual rights and advance the public good while providing the certainty needed for innovation and economic growth.

The information fiduciary model represents an important first step in recognising that digital platforms should hold obligations towards internet users that are proportionate to the risk of harm they may potentially cause. Nevertheless, practical limitations related to the ability of fiduciaries to manage competing duties to both data subjects and their shareholders may impact their ability to build public trust.

If the data trust agenda appears more ambitious, this is as much an indication of data trusts' promising features as it is a reflection of the public's aspirations for data governance in the digital age: representation, shared rights, accountability and remedy.[57] Not only are these just demands, but meeting them may help create an environment for the digital economy that is sustainable in the long term.[58] So while data trusts may face a number of concrete implementation challenges related to their legal, governance and architectural foundations, they remain an indisputably promising innovation that merits greater investment – narrowly, as tools that could facilitate fair and ethical data sharing to alleviate burdens related to consent and privacy self-management; and broadly, as ways to empower the public to participate in decisions regarding the use of their personal data, and to collectively seek redress in cases of harm.

56 Benjamin, M., Gagnon, P., Rostamzadeh, N., Pal, C., Bengio, Y., & Shee, A. (2019, 21 March). Towards Standardization of Data Licenses: The Montreal Data License. *arXiv*. https://arxiv.org/abs/1903.12262

57 Surman, M. (2019, 13 May). Consider this: AI and Internet Health. https://marksurman.commons.ca/2019/05/13/consider-this-ai-and-internet-health

58 Ibid.

GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building "smart cities"? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called "killer robots".

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH
2019 Report
www.GISWatch.org

APC
ARTICLE 19
Sida