A trust framework for digital food systems

Brewer, Steve[1], Pearson, Simon[*1], Maull, Roger[2], Godsiff, Phil[2], Frey, Jeremy G[3], Zisman, Andrea[4], Parr, Gerard[5], McMillan, Andrew[6], Cameron, Sarah[6], Blackmore, Hannah[6], Manning, Louise[7], and Bidaut, Luc[8]

[1]Lincoln Institute for Agri-Food Technology, University of Lincoln, Lincoln, LN2 2LG, UK
[2]University of Exeter, Business School, Exeter, EX4 4PY, UK
[3]University of Southampton, Chemistry, Southampton, SO17 1BJ
[4]Open University, Faculty of Science, Technology, Engineering & Mathematics, Milton Keynes, MK7 6BJ, UK
[5]University of East Anglia, School of Computing Sciences, Norwich, NR4 7TJ, UK
[6]Pinsent Masons, 30 Crown Pl, Earl St, London EC2A 4ES
[7]Royal Agricultural University, Cirencester, GL7 6JS
[8]University of Lincoln, School of Computer Science, Lincoln, LN6 7TS, UK

[*]Corresponding author: spearson@lincoln.ac.uk

The food system is increasingly reliant on a multitude of data-driven technologies that connect global supply chains and underpin productivity, trade and security. Improved governance of data exchange – through a data trust framework - will drive sustainable business growth and secure wider public benefits.

Introduction

The full potential for a digitally transformed food system has not yet been realised - or indeed imagined. Data flows across, and within, vast but largely decentralised and tiered supply chain networks. Data defines internal inputs, bi-directional flows of food, information and finance within the supply chain, and intended and extraneous outputs. Data exchanges can orchestrate critical network dependencies, define standards and underpin food safety. Poore and Nemecek[1] hypothesised that digital technologies could drive system transformation for the public good by empowering personalised selection of foods with, for example, lower intrinsic greenhouse gas emissions. Here, we contend that the full potential of a digitally transformed food system can only be realised if permissioned and trusted data can flow seemlessly through complex, multi-lateral supply chains, effectively from farms through to the consumer.

Data for the public good

Whilst the transmission of commercial and personal data are highly controlled and regulated, there are many examples where data is not readily transmitted through supply chains that could otherwise serve a public or common benefit. This data includes food safety, certification and standards, environmental costs of production, nutritional content and know-how that could drive whole supply chain efficiency. For food safety alone, regulation (e.g. UK Food Safety Act, 1990) requires all actors within a supply chain to trace products just “one-step-up” and “one-step-back” through the supply chain. There is no compulsion to connect traceability data beyond that requirement, or for supply chain actors to transmit data through the multiple tiers of the complex food system. Barriers to the exchange of data that can realise a common benefit are associated with a lack of trust between exchanging parties, technical and legal complexity of managing and governing data exchange and fragmented sector leadership.

Private sector companies within a supply chain are entitled to make their own arrangement to exchange data under terms and conditions agreed by all partners and subject to broader statutory constraints (including general data protection regulation (GDPR), and competition law). While a multitude of such arrangements exists, they were generally developed as local ad-hoc contractual arrangements and require continuous adaptation as trading relationships evolve, new data sources

become available, where novel approaches are developed for extracting value from data, and/or where inequalities from the exchange of data become apparent. These pragmatic, but short-term, approaches may succeed in addressing an immediate concern, but can also result, ultimately, in greater friction and inefficiencies being built into the system. As food systems undergo digital transformation, a new approach for data governance is required, one that is legally robust, secures a wider public purpose and facilitates the necessary trust to stimulate data exchanges across the whole food sector.

Data trusts and trust frameworks

The challenge to establishing trusted multi-lateral data exchange between parties, for example across a whole supply network is common across industrial business-to-business (B2B) interactions in any sector, not just food systems, and challenges also exist where data processors might interact with personal data (business-to-consumer, or B2C). Whilst B2B data sharing requires complex governance systems that define data ownership, commercial rights, use and access, exchanges that involve personal data (B2C) needs to protect obligations to individuals enshrined by regulations such as the UK and EU's GDPR. This poses considerable ethical challenges, especially as new technologies, such as artificial intelligence[2], have unprecedented power to analyse individual and group behaviours. To mitigate such ethical challenges, the term "data trusts" recently entered the vernacular as a governance model for the pooling and sharing of personal data by data processors deploying artificial intelligence technologies. Stricto sensu, "data trusts" are governance structures defined by "trust law". They are generally akin to libraries of information where data are securely shared for a greater good, and put under the care of a stewardship function (trustee) that has fiduciary responsibility to act in the interests of the beneficiary/ies - and only the beneficiary/ies. The data trust's stewardship function may be carried out by one or more individuals who make decisions regarding the data in terms of what can be done with or to them, in line with the terms on which data or rights have been put into the trust, and for the benefit of the trust's beneficiaries. Data trusts have been defined as a form of participatory governance[3].

The terminology, "data trust," is ambiguous. Defined by law, data trusts are only one of a set of collaborative data governance systems. It could for instance imply a system of governance as an embodiment of "trust law", or simply a defined governance system that secures trust in the data per se or even the trustworthiness of participants. We suggest a more appropriate descriptor of the governance set should be "trust frameworks"[4-6], which include the management of all forms of collaborative data, irrespective of whether it comprises personal data or indeed uses "trust law". As defined by Temoshok and Abruzzi (2018)[5], a "Trust framework [is] a generic term used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements".

Barriers to data exchange are associated with a lack of trust between exchanging parties[7], the technical and legal complexity of managing and governing data exchange, and a fragmented private sector leadership seeking to deliver a public good. Examples of multi-party systems using trust frameworks include credit card systems, electronic payment systems, the internet domain name registration system, and digital identity systems. Trust frameworks exist to provide assurances to participants that all other participants will conduct themselves according to pre-agreed roles and rules. These trust networks can be based on institutional trust, relational trust or a hybrid mix of the two elements. Accordingly, we see trust framework models as a key requirement for data sharing across distributed food supply networks, and propose[8,9] that any trust framework for the food system requires four logical components: 1) a governance and legal form that defines the pre-agreed rules and roles permissible in the system, 2) a security and permissioning layer where the network connectivity between the participants is implemented, 3) a knowledge mapping component which establishes inter-operability between the disparate system elements and across interfaces, and 4) an operational component where the business processes are executed (see Figure 1).

Governance and Legal Form

We envisage a two-tier governance structure with three key constituents: A) a *members' council* of stakeholder representatives from the private and public sector. Within the food system, private agents could be the companies in a supply chain that have common purpose to exchange data up to, and including, consumers or other representative groups (Unions, Trade Associations). The public sector bodies are likely to be regulators (e.g. UK's Food Standards Agency, Environment Agency) or government departments B) a *supervisory board* elected by that members' council to represent the

council and determine priorities, and hence supervise C) an *executive board* that is tasked to focus on the day-to-day strategies for developing and implementing the data trust framework protocols. The inclusion of a *regulator* within the governance framework could facilitate institutional and relational trust, and also reduce legislative burden on both the public and private sector. Initially, a legal form could be achieved through a collection of adaptable collaboration agreements (contractual framework), but it may ultimately be beneficial to establish a legal entity (corporate framework, such as a company limited by guarantee[9]) to represent such a governance structure. In all instances, there are key elements to engender trust among stakeholders: a clear statement of purpose, underpinned by robust governance, that respects the rights of all interests and ensuring the data is used ethically and according to agreed rules; transparent and consistent decision-making; and accountability and equality across stakeholders. The first of these will embed institutional aspects of trust whilst the other two elements will drive aspects of relational trust. While the benefits of data sharing can be manifold, stakeholders will want to know that any data, to which they provide access, will be used for appropriate and ethical purposes.

Security, permission, interoperability and operation

Digitally transformed food supply is inherently vulnerable to disruption or malicious intent, including cyberattacks[10]. As business processes becomes more transactional, carefully managed information sharing becomes central to operational success. Controlling access by individuals, role profiles, groups, specific data types or context is always challenging and primarily entails reliably authenticating individual parties for authorising specific actions. This challenge increases with controlling access across separate, independent organisations, and with disparate heterogeneous sets of data. Here we see a role for the FAIR Data Principles[11] which define findability, accessibility, interoperability and reusability. While these principles were originally developed for the data-rich research community, they have increasingly been successfully applied in the commercial domain.

Information sharing requires interoperability between distributed data sources, the systems that manage them, and users (either humans, systems or models). Connecting different information systems is challenging as information is often stored in different formats and housed in distinct proprietary systems[12]. The interoperability component thus provides an ability for users to interact with the whole framework, including through shared application programming interfaces (API's), open format data repositories, and also proper quality control and curation standards.

The operational layer defines how the community interacts at a business level, and includes directories of members (either humans, systems or groups thereof), their role profiles, and what data they can access and/or provide, i.e. their level of permission and authority within the trust framework. The operational component could also include a reasoning engine to provide insight into the overall operations of the supply chain or to highlight specific issues, for example to detect, monitor or risk assess foodborne illness outbreaks. The operational layer also includes the processes for monitoring of compliance and degree of adherence to standards across members.

The key characteristic of a data network for a food production supply chain is distributed data stores. Such data stores belong to independent organisations, such as a haulier, retailer and farm. Each organisation is responsible for its own data, held in its data store. Any flows of information, from these data stores, corresponding to a flow of goods between these organisations would be controlled in a decentralised manner. Retailers may request information from suppliers, but would not typically have free access to all of their data. Similarly, producers would receive selected data from their suppliers, and would pass on selected information to hauliers. For routine transactions, functional and regulatory processes would dictate such information flows. Only in exceptional cases, such as product recalls and other incidents, would further protocols around additional data sharing/access be enacted. These structures are partially operational within the existing food supply chain, but this is typically where data exchange is between bi-lateral entities for private rather than public purposes.

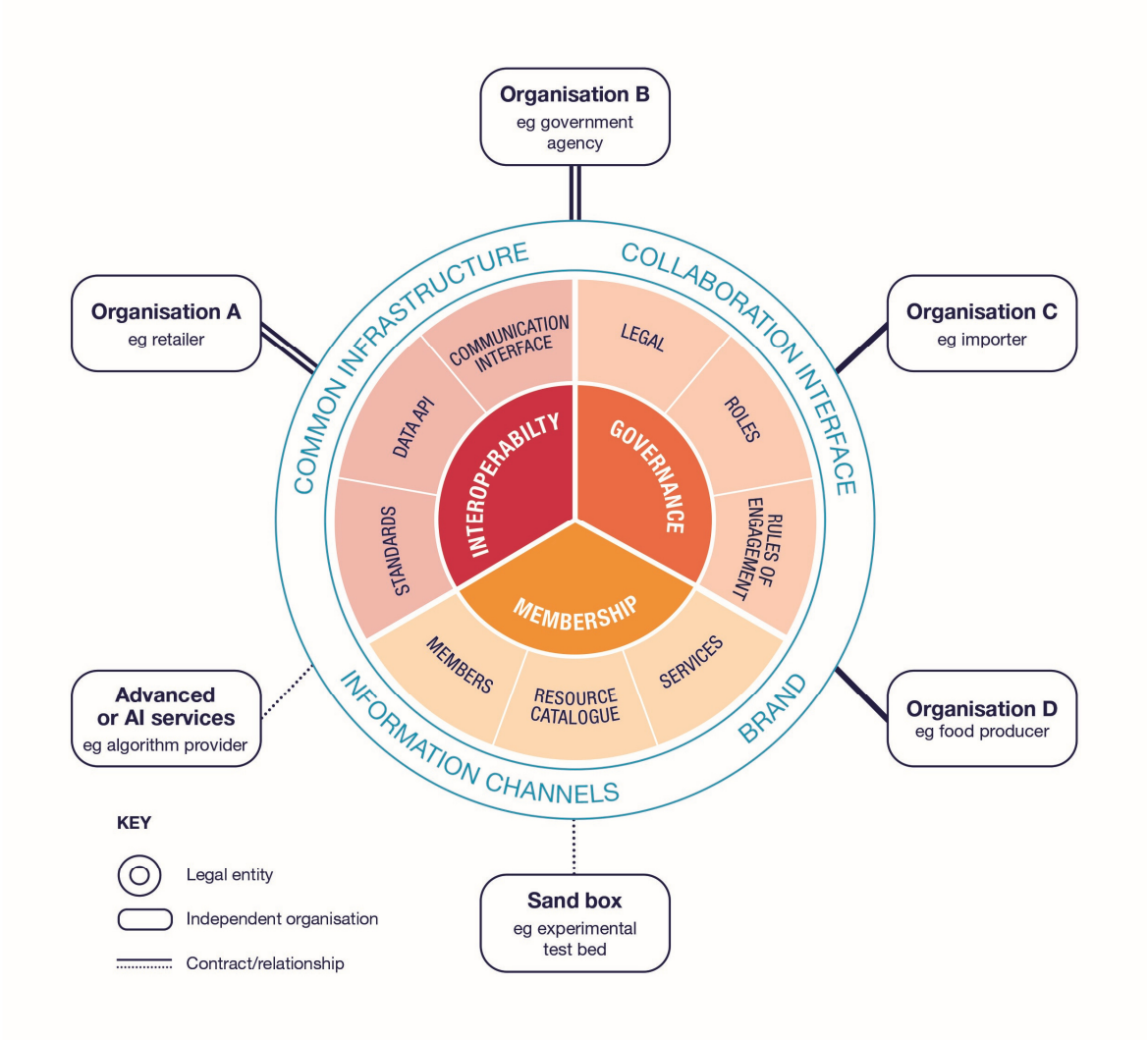

Figure (1) ***Model Food Data Trust Framework.*** A model trust framework for the food system structured with a defined legal form and proposed operational functions whilst interacting with multi-lateral parties within the food system.

Towards an intelligent and transformed food chain

What we thus foresee is an intelligent, decentralised food supply chain focussed on securing a common good by the secure exchange and sharing of information. This can range from secure sharing of regulatory compliance information, through to gaining unique insights from AI harnessing secure collection(s) of distributed data. Achieving this goal requires robust and resilient data-driven services, aligned with secure and independent AI services potentially accessing anonymised, but traceable, independent data, and a strong human-centred governance process representing all food system stakeholders, including the consumer. We contend that regulatory compliance can and should be better enabled through data trust frameworks and as a result contribute to a more resilient and robust food chain. This vision could be realised over a relatively short time period, considerable exchangeable data is already collected by supply chain actors for their own private or commercial purpose. The challenging step is the gain of consensus to exchange data between what could normally be highly competitive organisations operating in the food chain.

Conclusion and future

At this nascent stage, we recommend that a pilot food standards trust framework be established and evaluated, which could take the form of the Food Data Trust (FDT). This effort should be undertaken in conjunction with relevant regulators and with the participation of commercial entities as well as academic support. Industry engagement will be essential, as the mechanism should be co-designed and co-developed with partners relevant to each use case. The pilot must establish the common purpose and establish reproducible precedents that inform the design of legal standards and governance structures. Effective monitoring of the pilot can establish and quantify the transformational power of data trust frameworks, whether the governance structures are indeed sustainable and generate a significant public good.

While digital technology is already transforming some of the global food system, driving productivity and helping to realise improved environmental and societal outcomes across society, the full potential of a data-driven transformation that secures common benefits, such as improved food safety or movement towards a more environmentally sensitive and lower carbon food chain, has not yet been realised. The development of more coherent and effective mechanisms to govern data sharing with multi-lateral trust frameworks offers new potential to foster and enact further critical change.

References

1. Poore, J. & Nemecek, T. Reducing food's environmental impacts through producers and consumers. *Science* 360, 987–992 (2018).
2. Hall, W. & Pesenti, J. Growing the artificial intelligence industry in the uk. *Dep. for Digit. Cult. Media & Sport Dep. for Business, Energy & Ind. Strateg. Part Ind. Strateg. UK Commonw.* (2017).
3. Milne, R., Sorbie, A. & Dixon-Woods, M. What can data trusts for health research learn from participatory governance in biobanks? *J. Med. Ethics* (2021).
4. Makaay, E., Smedinghoff, T. & Thibeau, D. Trust frameworks for identity systems. https://openidentityexchange.org/networks/87/item.html?id=175 (2017).
5. Temoshok, D. & Abruzzi, C. *Developing Trust Frameworks to Support Identity Federations* (US Department of Commerce, National Institute of Standards and Technology, 2018).
6. Reed, C. & Ng, I. Data trusts as an ai governance mechanism. *Available at SSRN 3334527* (2019).
7. Behnke, K. & Janssen, M. Boundary conditions for traceability in food supply chains using blockchain technology. *Int. J. Inf. Manag.* 52, 101969 (2020).
8. Pearson, S., Brewer, S., Godsiff, P. & Maull, R. Food data trust: A framework for information sharing, DOI: 10.5281/zenodo.4575565 (2021).
9. PinsentMasons. Food data trust legal, structuring and governance report, DOI: 10.5281/zenodo.4575625 (2021).
10. Manning, L. Food defence: Refining the taxonomy of food defence threats. *Trends Food Sci. & Technol.* 85, 107–115 (2019).
11. Wilkinson, M. D. *et al.* The fair guiding principles for scientific data management and stewardship. *Sci. data* 3, 1–9 (2016).
12. Verhoosel, J., van Bekkum, M. & Verwaart, T. Semantic interoperability for data analysis in the food supply chain. *Int. J. on Food Syst. Dyn.* 9, 101–111 (2018).

Acknowledgements

This paper presents work funded by the Food Standards Agency (Project Ref FS301083) and the EPSRC Internet of Food Things DE Network (EP/R045127/1).

Author contributions statement

All authors contributed to the material and all authors reviewed the manuscript. SB prepared the draft supported by SP and PG, all other authors contributed to the research and reviewed the manuscript.

Competing Interests Statement

The authors declare no competing interests.