



Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing

Simone van der Burg¹ · Leanne Wiseman² · Jovana Krkeljas²

Published online: 10 July 2020
© The Author(s) 2020

Abstract

Digital farming technologies promise to help farmers make well-informed decisions that improve the quality and quantity of their production, with less labour and less impact on the environment. This future, however, can only become a reality if farmers are willing to share their data with agribusinesses that develop digital technologies. To foster trust in data sharing, in Europe the EU Code of Conduct for agricultural data sharing by contractual agreement was launched in 2018 which encourages transparency about data use. This article looks at the EU Code through the lens of literature on trust and contract agreements. We agree with the makers of the EU Code that a contract can make an important contribution to trust relationships as it is needed to mitigate the detrimental effects of power relationships between experts and non-experts. Building on Onora O’Neill’s perspective to trust, however, we argued that a contract can only be successful in fostering trust when (a) information is comprehended by the more vulnerable party in this relationship who has to sign the contract, (b) the more powerful partner takes responsibility to provide that information, and (c) information is tailored to the information needs of the party signing the contract, even when data are re-used over a longer period. In addition, we think that differences between trust relationships and relationships of accountability, give reason to add to informed consent other more substantive ethical components in a more encompassing code of conduct.

Keywords Digital farming · Ethics · GDPR · EU code of conduct · Informed consent · Trust

Introduction

The emerging literature about ethical, legal and social aspects of digital (or ‘smart’) farming usually starts by describing the promises it brings for the future. It highlights how robots, drones and digital technologies help farmers to make well-informed decisions that improve the quality and quantity of their production, with less labour and less impact on the environment. These technologies are in widespread use in irrigation, monitoring the health or location of cattle

or driving a herd in a direction, sowing of crops or milking of cows or sensors and weather satellites that offer information that is helpful to tailor irrigation, fertilizer or pesticides to plant’s needs or to define the right moment for seeding. The digital revolution in farming bears with it the promise to contribute to resolving the looming challenges posed by world food insecurity. As more food, which is safe and nutritious, is produced in a more environmentally friendly way, it is expected to help feed the growing world population in an era where climate change is foreseen and resources become scarce.

This promising frontier in farm technology can, however, only become a reality when farmers are willing to share their data with other stakeholders, such as the agribusinesses that are developing the digital farming technologies. Yet surveys carried out in Australia and interviews in Europe and North America point out that farmers are not always eager to do that (Jakku et al. 2019; Wiseman et al. 2019; Regan 2019; Fleming et al. 2018; Carolan 2017; Zhang et al. 2017). Farmers often distrust the agribusinesses as they could re-use their data to build other businesses and services, while

✉ Simone van der Burg
Simone.vanderburg@WUR.nl

Leanne Wiseman
l.wiseman@griffith.edu.au

Jovana Krkeljas
jovana@griffithuni.edu.au

¹ Wageningen Economic Research, Wageningen University and Research, Droevendaalsesteeg 4, 6708 PB Wageningen, The Netherlands

² Griffith Law School, Griffith University, Brisbane, Australia

the farmer is excluded and thus is not able to share in the benefits. Alternatively, these agribusinesses may do other things with their farm data, such as using it to influence or inform decisions on the stock market, profiling the farmers and selling those profiles to third parties, such as input suppliers, who are interested in farmers' preferences, or they can sell data to other stakeholders such as researchers, governments, NGO's, banks, insurance companies etc.

Ethicists and legal specialists in Australia, as well as New Zealand, North America and Europe have only recently begun thinking about the issues that cause distrust (Wiseman et al. 2018; Janzen 2018). Sometimes issues are understood as a privacy-protection problem, as farms are private businesses and therefore farmers should be in control over data that contain information about their farms (Sykuta 2016). Sometimes, they are explained in terms of data ownership as farmers ask who is the owner of the data and therefore who has the right to monetize and profit from the data's value (De Beer 2016; Kshetri 2014; Poppe et al. 2016; Rasmussen 2016; Schuster 2017), and sometimes the farmers' unease about data sharing is conceptualized as a response towards shifting power relationships that the digital technologies (and the companies that make them) affect in the social network surrounding farms, raising questions about fair and equitable distribution of benefits and responsibilities within that network (Van der Burg et al. 2019; Bronson 2018; Bronson and Knwzevic 2016; Kshetri 2014; Jakku et al. 2017; Carbonell 2016; Eastwood et al. 2017; Rodriguez et al. 2017; Wolfert et al. 2017).

In the absence of clear and carefully elaborated perspectives of the appropriate ways to deal with ethical legal and social implications of digital agricultural technologies on farming enterprises and relationships, stakeholders (farmers, their stakeholder organisations and agribusinesses who make or deliver digital farming technologies) began to shape their own guidelines to improve ag data management practices and provide a basis for trust. In different parts of the world, agricultural privacy and security principles and data codes of conduct have been developed. In 2014, in the US, the American Farm Bureau's Privacy and Security Principles for Farm Data (2019) were the first to draw attention to some of the concerns farmers had about the way their data was being managed and shared. Following this initiative was the development of the 2014 New Zealand's Farm Data Code of Practice and more recently in 2019, we saw the development and launch of the EU Code of Conduct on agricultural data sharing by contractual agreement (hereafter referred to as the EU Code), and in 2020 the Australian Farm Data Code was launched (National Farmers Federation 2020).

The main purpose of these ag data sharing principles and codes of practice is to establish trust between farmers and agribusinesses, by means of a contract agreement. Although entirely voluntary, the principles and codes encourage

agribusinesses to give information about what they do with farmer's data to the farmer, in order to reassure farmers and help them make an informed choice about sharing their data (or not) with the agribusinesses that develop and deliver tech-services. We believe, however, that there is need to examine these principles and codes more closely. While it is worth noting the efforts that were undertaken to initiate and shape a responsible data sharing practice, the focus on a contract appears limited. Contract agreements between human actors can only play a limited role in fostering trust relationships that remain largely virtual.

This is what we want to argue in this article. We will focus on the EU agricultural data code of conduct by first providing an overview of its development and key features, followed by critical reflections and observations about the function and role of contracts in fostering trust. In so doing we draw upon the literature on (e-) trust, more specifically on the distinction that has been made between contractarian-individualist approaches to trust and phenomenological-social approaches to trust.¹ We will argue that both approaches have a role to play, but that they need to be combined. To do that we will draw on the work of the bioethicist Onora O'Neill about the relation between informed consent and trust, to highlight particularly important functions contracts can have in mitigating unequal power-relationships, such as between experts (such as those who possess digital knowledge and skills, such as the agribusinesses) and people who are not digital experts (such as farmers). Starting from O'Neill, we will argue that contracts cannot function as a foundation for a trust relation, such as the contractarian-individualist perspective supposes, but only as *maintainers* of trust in social contexts in which trust relations are already there and are supported by norms, obligations, rights and principles that organize social interactions. Given the role of contracts as trust maintainers, it becomes possible to draw attention to some of the shortcomings of the present EU Code in providing guidance for stakeholders who aim to enhance trust in data sharing by means of a contract.

The European Union Code of Conduct on Agricultural Data Sharing by Contractual Agreement ("EU Code of Conduct")

On the 23 April 2018, a coalition of associations from the EU agri-food chain launched a joint EU Code of Conduct on agricultural data sharing: the EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement.² The

¹ This distinction is made in: Coeckelbergh (2012).

² For the news-item about the launch see: European Crop Protection Association (ECPA), (23 April 2018). <https://www.ecpa.eu/news/>

Code of Conduct explains contractual relations and provides guidance on the use of agricultural data, particularly on the rights of access and use of the data. It is important to note that the Code was a collaborative effort between farmer's cooperatives in the EU allied to Copa-Cogeca and CEJA (that focusses on young farmers up to 40 years of age), as well as representatives of animal breeding companies and large organizations representing various industries producing animal feed, fertilizers, seeds or farm machinery (like CEMA, Fertilizers Europe, CEETTAR, ECPA, EFFAB, FEFAC and ESA).³ In launching the Code, it was highlighted by the parties that “the Code promotes the benefits of sharing data and enables agri-business models, including agri-cooperatives and other agri-businesses, to swiftly move into an era of digitally enhanced farming.”⁴

Before looking in detail at (limitations of) the role that the EU Code can play in building trust in data sharing, it is useful to understand the background and context in which the EU Code was developed. To do this, we will begin by examining the landscape of data and privacy regulation within the EU more generally.

Data Privacy and Data Protections within the EU

The EU has a long history of regulating databases, personal data and non-personal data.⁵

Footnote 2 (continued)

[code-conduct-agricultural-data-sharing-signing](#); Copa-Cogeca et al. (2018, p. 20).

³ CEMA (www.cema-agri.org) is the association representing the European Agricultural Machinery Industry; CEETTAR (www.ceettar.eu) is the European organization of agricultural rural and forestry contractors; ESA (www.euroseeds.eu) is the European Seed Association, representing the interests of those active in research, production and marketing of seeds of agricultural, horticultural and ornamental plant species; Fertilizers Europe (www.fertilizerseurope.com/) represents the majority of fertilizer producers in Europe; FEFAC (www.fefac.eu/), the European Compound Feed Manufacturers Federation; ECPA (www.ecpa.eu/) represents the crop protection industry in Europe; EFFAB (www.effab.info/) is the European Forum of Farm Animal Breeders and is the association of animal breeding and reproduction organizations in Europe.

⁴ CEJA, Two new partners sign up to the EU code of conduct on agricultural data sharing, <https://www.ceja.eu/two-new-partners-sign-eu-code-conduct-agricultural-data-sharing/>.

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on General Data Protection Regulation [2016]. <https://gdpr-info.eu/>; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on A Framework for the Free Flow of Non-Personal Data in the European Union [2018] OJ L 303/59. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>.

Since the late 1990s, the EU has recognised the impacts that the rapid surge in digital technologies, with its accompanying compilation/accumulation of individual data within databases has caused (Schneider 1998).

In response to concerns over data privacy and cyber securities, the EU enacted the *1996 Database Directive* to standardise the protection of databases across all EU member states.⁶ This *Directive* increased the protection of subsequent databases created from the synthesis of various personal and non-personal data.⁷ It enables the attribution of appropriate ownership rights to the databases and promotes, ‘investing in database creation’ (Schneider 1998). More specifically, it also consists of a sui generis scheme preventing the un-authorised use of information within databases.⁸ This scheme vests the owner with the rights to prohibit extraction/use of data from their database (Schneider 1998). This scheme is an addition to the copyright that may subsists in the tables or compilations of data themselves.

As data became more susceptible to privacy violations, in 2018 the EU implemented the *General Data Protection Regulation (GDPR)* to complement the *Directive* in data protection.⁹ The *GDPR* safeguards how data aggregators process the personal data of EU residents.¹⁰ Prior to the *GDPR*, data privacy protection was governed by each EU member states’ differing national regulations (Díaz 2016). Similar to the *Directive*, data protection regulations were not applied uniformly across the EU. Consequently, these disparities fettered the development of the EU’s digital economy.¹¹ The *GDPR* sought to eliminate this fragmentation and foster a coherent and universal approach in data protection.¹² It also imposes harsher restrictions on how personal data is collected and subsequently utilised.

While the EU Database Directive covered both personal and non-personal data, the *GDPR* was solely aimed at regulating personal data. Accordingly, the EU followed the *GDPR* with the introduction of the *Regulation on Free*

⁶ Directive 96/9/EC Of The European Parliament And Of The Council of 11 March 1996 on the Legal Protection of Databases [1996] OJ L 77/20, art 3; Davison (2016). <https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1692&context=caselrev>.

⁷ Ibid.

⁸ Directive 96/9/EC Of The European Parliament And Of The Council of 11 March 1996 on the Legal Protection of Databases [1996] OJ L 77/20, art 3; Davison (2016).

⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on General Data Protection Regulation [2016] <https://gdpr-info.eu/>.

¹⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on General Data Protection Regulation [2016] <https://gdpr-info.eu/>; He et al. (2019).

¹¹ Ibid.

¹² Ibid., pp. 207–208.

Flow of Non-Personal Data ('Free Flow Regulation').¹³ This regulation was designed to supplement the *GDPR* and stimulate the free flow of *all* categories of data within the EU market.¹⁴ 'Free flow' refers to the unlimited circulation of non-personal data within the EU.¹⁵

Of relevance to our discussion of the EU Code of Practice is the fact that this Regulation makes explicit reference to agricultural data and in so doing, categorises it as non-personal data.¹⁶ Therefore, the Regulation is endorsing the circulation of ag-data on the basis it has the potential to significantly contribute to the ag-data economy and boost revolutionary data services.¹⁷ Article 4 of the Regulation makes specific reference to the processing of smart farming data and prohibits its exclusive storage in one geographical area. The act of storing ag-data is known as 'localisation.' Localisation is prohibited, as it may inhibit innovation and restrict the flow of useful information within worldwide data economies.¹⁸

While the complexities of ag data have been recognized, it is worth pointing out that there is not only one type of data, but data may often contain a combination of personal and non-personal information (Wiseman et al. 2018). The EU has recognised the potential for the overlap of the provisions of the *GDPR* and the Free Flow Regulation by providing that should ag-data fail to meet the definition of 'personal data',

under the *GDPR*, it may fall within the free flow regulation (European Commission 2018).

In efforts to advance the free flow of data, article 6 specifically advocates for self-regulatory codes of conduct for data in all EU sectors.¹⁹ The implementation of such codes is thought to enhance and guide data mobility practices. Generally, data codes aim to guide the practices on the consent, disclosure and transparency of data sharing (Sander-son et al. 2018). The European Commission itself reinforced the Regulation's call for codes and aims to accelerate their development by highlighting that with codes, EU citizens and service providers will engage in unambiguous and clear practices when transferring data between service providers (European Commission 2017). More specifically, the Commission seeks to ensure data providers and their professional users (businesses) are well informed on the terms and conditions of data use.²⁰ This is essential in developing transparent practices prior to data processing contracts taking effect.

As ag-data was categorised as non-personal data for the purposes of the Free Flow regulation, the development of codes became highly appealing to the European agri-business sector. Accordingly, the major EU stakeholders within the agri-sector instigated the prompt drafting of the EU Code for ag-data sharing.²¹ Director Daniel Azevedo of the leading association for EU farmers, Copa-Cogeca, indicated the agri-industry was the first to acknowledge the Commission's request in creating self-regulatory codes.²² Azevedo further emphasised, an ag-data code advances ag-data circulation and promotes its benefits, thus fortifying the objective of the *Free Flow Regulation*.²³ This would ensure farmers seamlessly adapt to the digital era and more readily adopt technological solutions to farming.

The timely response from the agri-sector led to the official launch of the EU Code on 23 April 2018, which was signed by eleven major organizations representing EU agri-businesses.²⁴ To help understand the role that the EU Code can play in building trust and transparency in data sharing, first, it is useful to examine the key aims and features of the EU Code.

¹³ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on A Framework for the Free Flow of Non-Personal Data in the European Union [2018] OJ L 303/59, (9). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>.

¹⁴ European Commission, Legal study on Ownership and Access to Data, Report No 2016/0085 (2016), 28. <https://publications.europa.eu/en/publication-detail//publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1>.

¹⁵ European Commission, Legal study on Ownership and Access to Data, Report No 2016/0085 (2016), 28. <https://publications.europa.eu/en/publication-detail//publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1>.

¹⁶ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on A Framework for the Free Flow of Non-Personal Data in the European Union [2018] OJ L 303/59, (9). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>; European Commission, Free Flow of Non-Personal Data, European Commission. <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>.

¹⁷ European Commission, Legal study on Ownership and Access to Data, Report No 2016/0085 (2016), 28. <https://publications.europa.eu/en/publication-detail//publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1>.

¹⁸ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on A Framework for the Free Flow of Non-Personal Data in the European Union [2018] OJ L 303/59, art 2. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>; Council of the European Union (2018)

¹⁹ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on A Framework for the Free Flow of Non-Personal Data in the European Union [2018] OJ L 303/59, art 6. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>.

²⁰ Ibid.

²¹ COPA COGEC A et al. (Press Release, CDP(18)5022:1, 26 June 2018).

²² Ibid.

²³ Ibid.

²⁴ European Crop Protection Association (ECPA), (23 April 2018); Copa-Cogeca (2018).

Table 1 The five principles of the EU code

Principles	Key features
Data ownership	Rights are assigned to the entity that engages in the creation/collection of ag-data either independently, via advanced machinery or by way of commissioning data providers to do so (ie Data originator) This entitles the 'data originator' to exclusive control over ag-data, its subsequent use, access and/or distribution 'Data originators' can be farmers, but also other parties in the value-chain whose data are being collected (such as, for example, input suppliers, nurseries, the slaughterhouse)
Data access/control/portability	The access, use, storage and potential sharing of ag data with third parties is <i>only</i> permitted if the 'data originator' explicitly consents to this in the contract
Data protection and transparency	Unauthorised ag-data sharing cannot occur with third parties that are not originally referred to in the contract Prior consent must first be received to rectify the contract should circumstances change, and include the intended third parties Personal, or sensitive information requires replacement with pseudonyms (artificial identifiers) to ensure it is 'less identifiable'
Privacy and security	Personal data should not be subject to potential losses, theft, or unauthorised access the need to notify 'data originators' on any security breaches that may occur <i>GDPR</i> becomes applicable in circumstances where a data originators' personal/sensitive data is exploited to the advantage of third parties and utilised to 'make decisions about the data originator as a natural person
Liability and intellectual property rights	The contractual agreements must entail any terms of liability However, liability does not ensue from the faultiness of data machinery or devices during farming operations. There must be protection of any relevant IP rights that may result from the ag-data value chain

Key aims and features of the EU Code

In welcoming the new EU Code and highlighting the important role that data can play in the technological breakthroughs in precision farming, the EU Agricultural Commissioner, Phil Hogan, warned that data sharing could be very controversial "if not handled properly". He observed "We need to protect farmers in regard to the data they generate and make sure everybody participates; not only the big companies" (Stam and Michalopoulos 2018). The EU Code starts by addressing this very issue by stating, "The farmer remains at the heart of the collection, processing and management of agricultural data (Copa-Cogeca et al. 2018)." One of most positive features of the EU Code is that it has raised awareness of a wide range of issues raised by ag data sharing by attempting to open the conversation between agribusinesses who produce IOT technologies for farms and farmers about the terms of their data sharing relationship. The signatories to the Code acknowledge that 'farmer and agribusinesses are more than willing to share data with each other and engage in a more open data mind-set. However, they will only do so if the potential benefits and risks are made clear and when they can trust that these are settled in a proper and fair way through contractual agreements.'²⁵

At the heart of the EU Code is the notion that with greater transparency around the terms dealing with the access and

use of data, farmers will develop trust in the way that their data is being managed. To do that, the EU Code has formulated five key principles (see Table 1) that serve as a guiding framework on the access and use of ag-data and which aim to ensure trust between agribusinesses regarding: data ownership, data access/control/portability, protection and transparency, privacy and security, and principles on liability/intellectual property.²⁶ All five principles taken together require the parties in the data sharing network to respect that the 'data originators'²⁷ should have control over their data, in the sense that they should know how the data are used and who has access to them. They also require that the contracts be transparent: i.e. explaining the key rights, obligations and data sharing purposes and any benefits, in simple and understandable language.²⁸ Collection, storage and use can only happen with informed express permission

²⁶ European Crop Protection Association (ECPA) (23 April 2018).

²⁷ Data originator is defined in a very detailed way: 'the person or entity that can claim the exclusive right to license access to the data and control its downstream use or re-use.' i.e. 'the party that the data is attributed to. The data originator of all of the data generated during the operation is the party who has created/collected this data either by technical means (e.g. agricultural machinery, electronic data processing programs), or who has commissioned data providers for this purpose'. Copa-Cogeca et al. (2018, p. 6).

²⁸ Copa-Cogeca et al., EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement (2018) 8–9. https://www.copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf.

²⁵ Ibid 4.

of the data originator in a contract and further permissions must be sought where data is to be shared with third parties.²⁹ Agribusinesses are encouraged to explain what they do with data and to give data originators control and this is evinced through its leading statement, 'transparency and responsibility are key to gaining trust.'³⁰ While this goal is laudable in itself, there are reasons to doubt if and to what extent it will be able to realize its eventual purpose, which is to foster trust in the data sharing network and foster ag-tech innovations. Of course, these principles signify the EU Code is targeting the outcomes arising out of ag-data practices, such as trust, rather than formulating enforceable rules (Sanderson et al. 2018). But apart from that, a contractarian perspective can only tell part of the story about trust, which needs to be supplemented by another approach which takes into account the contextual and social interactions in which trust-relationships historically generate.

Given that the EU Code expects contracts to play a fundamental role in establishing trust relationships, it is useful at this point to delve further into the notion of trust and its relationship to contracts.

Trust and the role and function of contracts

Trust is a much discussed concept in ethics of digital technologies (Taddeo 2010a, b). Mark Coeckelbergh distinguishes between two types of approaches to trust relationships between human actors: contractarian-individualist approaches to trust and social-phenomenological approaches.³¹ In contractarian approaches to trust, people start out as individuals and they engage in relationships with other people based on rational reflection. Trust relationships come about only when individuals engage in them willingly, based on rational arguments, and they can also retreat from these relationships when they have reason not to trust the relationship anymore. 'Contract' is a metaphor to describe the rational basis of trust relationships. Sometimes the terms of the trust relationship are formalized on a piece of paper (such as a contract that needs to be signed), but trust can also be based on a personal reflection about one's reasons to trust another person or not. In digital ethics, Taddeo's concept of e-trust between non-human actors (such as robots or systems) is based on a version of this contractarian-individualist approach to trust, as she discusses trust as the result of rational deliberation: there are 'reasons' to choose

to 'trust' a different (digital) actor, weighing the goals to be achieved, the risks involved in trusting another party, beliefs formed about the actor and an assessment of its trustworthiness. Machines, according to Taddeo, are able to make these choices in a more rational way than human beings, as they are not hindered by emotion.

In contrast to this contractarian-individualist approach, the social-phenomenological approach starts from the supposition that human actors are always already part of social environments, before trust comes forwards as a topic for consideration. Trust is then not 'created' after careful rational argumentation, for it is always already part of the relationships and therefore has an embodied, affective and social dimension which is not always argued for, but which is lived from childhood onwards. This social approach to trust also forms Coeckelberghs approach to trust between human and non-human actors such as artefacts, tools, machines or digital systems; discussions about whether to trust them or not, always come up in contexts in which people are already interacting with an environment of (digital) artefacts and systems. Furthermore, trust in networks of non-human actors, may also differ from context to context, depending on the history people have with dependence on non-human (networks of) agents.

Both approaches to trust are hard to combine, according to Coeckelbergh, as they start from different presuppositions regarding the nature of relationships. It is imaginable, of course, to take the social perspective as a starting point and to consider trust to be the default situation from which one deviates only when there is a problem, which demands a rational trust assessment and a kind of 'contract'. However this presupposes that we always have a choice with regard to our social relationships and that this choice is rational and voluntary and that we can also always retreat from relationships. This however exaggerates the rational nature of our relationships, according to Coeckelbergh, and he writes that: 'Sometimes we trust in spite of good reasons not to trust, or sometimes we mistrust in spite of good reasons to trust' (Coeckelbergh 2012, p. 56).

Acknowledging the non-rational nature of a lot of trust relationships, we see however a different possibility to combine both approaches to trust. Bioethicist Onora O'Neill's theoretical elaboration of the relationship of trust and informed consent offers a way to combine both perspectives to (e-)trust in an intelligent way. Informed consent, just like a 'contract' in contractarian-individualist approaches to trust, may take informal forms in practice but also more formal ones that are like signed 'contracts'. This informed consent or 'contract', in O'Neills perspective, does not have a *primary* role in establishing or founding trust relationships; it is only used in situations in which people who already trust each other consider doing something that could potentially harm the trust between them. Any informed consent

²⁹ Copa-Cogeca et al., EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement (2018) 9. https://www.copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf.

³⁰ Ibid 4.

³¹ P. 54/55 in: Coeckelbergh (2012).

or contract presupposes a social world in which there is already trust; consent is only asked for actions that somehow stand out and could potentially undermine that trust. It therefore has a *secondary* role in maintaining the trust that was already there in the social world. Together with co-author Neil Manson, O'Neill clarifies this secondary role of informed consent in the justification of actions in *Rethinking Informed Consent in Bioethics* (Manson and O'Neill 2007). Here they reject the *fundamental role* that many people ascribe to informed consent in the justification of action, which has strong parallels with the fundamental role of contracts in contractarian–individualist approaches to trust. Proponents of this fundamental role presuppose that *any* intervention can eventually be justified if it is chosen by the consentor and if it can be shown, that the autonomy of the consentor was respected when he or she chose. In contrast, Manson and O'Neill ascribe to informed consent a *secondary* role in justifying action. In this view, the primary justification for action is provided by the social trust relationships, which are already in place in society, similar to Coeckelbergh's social-phenomenological approach to trust (Manson and O'Neill 2007, p. 72). The primary justification depends on (sometimes tacit) principles, codes, obligations, rights and ideals which function to maintain the fine-tuned web of social expectations which make it possible to move around freely without having to be suspicious or afraid of what other people will do. Within such trust relationships, informed consent has a specific function: consent is asked only for actions that somehow stand out and that could harm trust, as they disrespect certain principles, codes or obligations that would usually apply in society. Informed consent then functions as a (temporary) “waiver” of obligations, ideals, principles and rights that would usually apply; people who give consent choose to temporarily set these social prohibitions and values aside, on which social trust usually depends. An example of such ‘waiving’ of an accepted social prohibition is a situation in which a person asks consent before taking something out of someone else's bag: this action ceases to be qualified as theft because consent was asked first. The trust that was already there in society is *maintained* by asking consent for an action that would break (tacit) social norms. Consent therefore functions as a trust *maintainer*, rather than as the fundament of trust.

The perspective to trust and informed consent and trust that O'Neill and Manson provide, also helps to think about the contribution that a (more or less formal) contract can give to trust relationships. According to O'Neill informed consent is particularly important in social contexts where there is a power difference between people, such as between professionals (who possess a certain knowledge and expertise) and laymen. In those relationships, informed consent serves as a mechanism for dealing with the vulnerability of the layperson in this power relationship, as it has a role

in making, “coercion, manipulation and deception much harder to effect and much easier to detect,” and in this way it helps “establishing, keeping and restoring trust relations (O'Neill 2002, p. 153). While there are many accounts of informed consent, in the basis informed consent implies a communicative relationship between two parties who have unequal knowledge and expertise. One party in this relationship (who has knowledge and who is therefore the information provider) is ascribed the responsibility to give accurate information to the other party about an action, service, procedure, intervention or measure, including the possible benefits, harms and risks it implies. Based on this information, the other party (the consentor) makes a choice about what action to take or whether to accept the service, procedure, intervention or measure or not. The choice of the consentor is subsequently communicated to the information provider (Beauchamp and Childress 2001).

A lot can go wrong in this communicative relationship, which is important to consider also in other relationships where a form of contract is imagined to play a role such as in digital farming. In *Autonomy and Trust in Bioethics*³² O'Neill explains that those who ascribe to consent a fundamental role, usually do not foster trust but create relationships of accountability. In relationships of accountability, professionals use informed consent as justification for their action: professionals who possess knowledge and expertise give complete information to clients to allow them to give their consent, but they do not particularly care for the relationship with the clients and therefore do not check whether they have *comprehended* this information. Informed consent procedures will then primarily function as protection for the professional, who is already the more powerful party in the relationship. In O'Neill's words, in a biomedical context consent that plays a fundamental role will function “as protection against accusation, litigation and compensation claims that patients could file against an institution or professional” (O'Neill 2003, p. 4). It leads to situations, in which the layman who is already the more vulnerable in the relationship has to digest voluminous and complex information prior to giving consent. Doing this, O'Neill argues, does not empower the layman.³³ It primarily protects the professional, who therewith gives the responsibility for taking the risks of the service provided to the layman. In a healthcare context, this means that if a treatment fails and the patient files a complaint, the doctors can use the signed informed consent form to cover their backs, arguing that the patient was given information beforehand and therefore knew what he was getting into and thus has no right to complain.

³² Ibid.

³³ Ibid.

O’Neill’s approach to trust offers an intelligent way to combine the contractarian–individualist perspective to trust and the social-phenomenological perspective. It functions here as a lens to look at the EU Code. The EU Code aims to foster trust by means of a contract agreement between parties that differ in power, because they have different (digital) knowledge and expertise. Agribusinesses that use farmer’s data to develop digital farming technologies and services possess the technologies and have a higher level of knowledge and digital expertise needed to collect, combine and analyse data for various purposes, than farmers do. While farmers sometimes have digital expertise too, they spend most of their time farming and therefore have less time to develop their digital capacities. Also, some farmers lack digital expertise entirely and do not even possess the relevant technologies. To mitigate the harmful effects of this power difference, it is understandable that the EU Code (as well as the other principles and codes developed for ag-data governance) considers it important to foster transparent communication of information before signing an agreement (the consent), as this is a way to deal with power differences. It is questionable, however, if the EU Code is doing this well and therefore, whether it is successfully protecting the more vulnerable party in this relationship, i.e. the farmer.

This is what we will discuss in this article. If we want contracts to foster trust like O’Neill’s approach to informed consent does, (a) information provided should be comprehensible for the more vulnerable party in the relationship (such as the farmer) prior to giving consent, (b) the more powerful parties should take responsibility to provide information, and (c) information should be tailored to information needs, even when data are re-used over a longer period. In the following we will discuss whether and to what extent the EU code of conduct is living up to these requirements.

Comprehension of information

There is a lot of debate about the conditions for obtaining an informed consent, which is informative to reflection about the role of communication in fostering trust. But according to O’Neill, comprehension of the information provided about an action that one consents to, is of vital importance.

Informed consent is often taken to need four necessary elements, which help draw attention to the roles of both parties in informed consent (Dawson 2009). Consenters:

- Must have the required competence to understand the information
- Must be subject to no undue influence or coercion
- Must be in possession of the relevant information, and

- Must *comprehend* the relevant information.³⁴

These four elements, nicely summarized by Angus Dawson, draw attention to the capacities the consenter must possess in order to give an informed consent, which implies responsibilities for the information provider to foster those capacities. During the informed consent procedure, the information provider is responsible for communicating information in a comprehensible way, attune it to capacities of the consenter to understand, check whether the information is understood and refrain from (subtly or more forcefully) pushing the consenter towards a specific choice.

Dawson, just like O’Neill, stresses the importance of the fourth element, *comprehension*, as it is sometimes not included in accounts of informed consent. He argues that it should be included, as it is in line with the most influential and widely cited accounts of the requirements of genuine informed consent (Faden and Beauchamp 1986; Beauchamp and Childress 2001). This fits with the most common justification for informed consent, which is that it respects a person’s autonomy and without understanding of the implications of a decision an autonomous choice would not be possible. In addition, it saves informed consent from being ‘trivial and uninteresting,’ as without comprehending the information, what would be the point of having an informed consent procedure? (Dawson 2009, p. 100).

With these four aspects of informed consent in mind (especially the fourth aspect of *comprehension*) we now turn to the EU Code. It is easy to see that the EU Code is a longer, more detailed document than its counterparts: the US Privacy and Security Principles and New Zealand Farm Code. The EU Code requires the use of unambiguous contracts to clarify the roles of each of the parties involved during farming operations and it encourages parties to ensure agreements are comprehensible and set out the specific conditions on the ag-data’s intended collection and potential on sharing. Furthermore, the EU Code is more explicit about its aims and sets out key provisions and guidance on a range of issues arising from agricultural data (particularly the rights to access, use, privacy and liability). It provides detailed definitions of key terms, as well as case studies and it ends with a checklist for parties who wish to come to an agreement about the sharing of agricultural data.

The detail that is provided in the EU Code has its advantages, for a serious attempt has been made to clarify. We observe, however, that the attempt to be precise may also have counterproductive effects. It has disadvantages, given the level of comprehension that it helps to realize on the part of the consenter/farmer. Here we highlight some key aspects

³⁴ Ibid.

of the Code that appear to confuse, rather than simply issues around data collection and sharing for farmers.

One of the key stumbling blocks for the adoption and use of the Code is the confusion that appears to be introduced by the terms ‘data originator’ and ‘data contributor’. These appear in the detailed definitional section. The data originator is defined as:

the person or entity that can claim the exclusive right to license access to the data and control its downstream use or re-use’ i.e. ‘the party that the data is attributed to. The data originator of all of the data generated during the operation is the party who has created/collected this data either by technical means (eg agricultural machinery, electronic data processing programs), or who has commissioned data providers for this purpose.³⁵

The data provider is defined as:

a natural or legal person that under an agreement delivers data to the data user and/or Data contributor. (Copa-Cogeca et al. 2018, p. 6).

These are interesting categorisations of parties in the ag data relationship, but they are also confusing. When thinking about the number of data collections and transactions that can take place on a farm, it is important that parties clearly comprehend their roles with respect to operation of the EU Code. However, the case studies themselves highlight the complexity of the data relationship, as farmers may be data originators in one relationship with their advisor but then the advisor becomes data originator when dealing with agribusinesses who provide digital services.³⁶ This lack of clarity is problematic, for the EU Code ascribes different responsibilities to parties with different roles and every party needs to know its role prior to understanding how to use the code. A further problem is that these terms sit outside the legal categories of data ownership that are recognized in law. This adds to the potential confusion, as it is unclear how the Code relates to the law that is already in place. This is one example of how the Code seems to introduce a level of complexity rather than simplify and make the nature of the data relationship more transparent.

Responsibility to inform

The EU Code is developed with the best of intentions and probably agribusinesses and farmers do everything right in practice. However, in the text of the code, it is unclear who

has the responsibility to provide comprehensible information. The terms that are to be made transparent in the agribusiness’ data contracts are as follows:

- “The most important terms and conditions
- The purpose of collecting, sharing and processing the data
- Rights and obligations that the parties have related to data, rules and processes for data sharing, data security, and the legal framework in which the data is kept and in which back-ups are stored
- The software or the relevant application and information storage and use of the agricultural data
- Verification mechanisms for the data originator
- Transparent mechanisms for adding new and/or future uses.”³⁷

While the code does not expressly clarify *who* has to make these elements explicit in the contract, it can be implied that it is the agribusinesses that develop the contractual documents. Yet the checklist provided by the EU Code seems to be aimed mostly at farmers.³⁸

The checklist sets out a series of questions such as:

- “Is there an agreement in place?
- What obligations are there? What warranties and indemnities are there for each party?
- What data is collected?
- Who owns/controls access to the data?
- What services are delivered?
- Can I retrieve my dataset from the system in a usable format?
- Will my data be used for purposes other than providing me, the data originator (i.e., the farmer) with a service?
- Will I be updated on security breaches?” (Copa-Cogeca et al. 2018, p. 19).

Given the way in which questions are formulated, most questions on the checklist are designed to prompt farmers to make enquiries of their agribusiness. While it is quite important to show how these questions are related to elements that should be in the contract, and more fundamentally, the importance in developing a fairer and more equitable data sharing relationship, the onus seems to be placed on the farmers to make the enquiries. This seems unfair regarding the fact that they are the more vulnerable party in the relationship that ought to be protected by a Code that demands to offer transparent information prior to forming an agreement. How are farmers to take this

³⁵ Ibid., p. 6.

³⁶ Ibid.

³⁷ Ibid., p. 5.

³⁸ Ibid., p. 10.

role? While the questions on the checklist in the EU Code maybe help the farmer to be inquisitive, it does not offer guidance on how to determine whether the contractual deal that a service provider or agribusiness is offering is an acceptable one or not. For example, the question of ‘who owns/controls access to the data?’ will likely not have an easy answer, which again highlights the vulnerable position this would leave farmers in, as they have little or no knowledge of the terms of use of the service provider.

The checklist seems to place an unfair burden on the shoulders of farmers to research the terms of use of their agribusiness partners. Research has shown that many farmers are not even aware of the terms when entering into data contracts. This is largely due to the fact that with digital farming, transactions are happening without any face-to-face dealings (Wiseman et al. 2018). When services are being delivered digitally, via a download or app, it will become very difficult to ask for clarifications: for, at what point would a farmer be able to make these enquiries? To whom? Digital consent procedures we already see proliferating risk to become quite hollow, much like agreeing to privacy agreements when you download an app on your mobile phone. This certainly will not help to reach the level of comprehension needed to make an informed consent procedure truly *informed*.

Making information comprehensible could therefore include asking agribusinesses to provide a one page summary of the key terms of the complex licensing agreements that relate to data sharing and making them responsible for explaining these to farmers prior to any agreements are entered into. These key terms should address all of the matters that farmers should inquire into, according to the checklist that is already part of the EU Code. This helps to give clearer understanding on the responsibilities of the tech service providers in the relationship. This is similar to the shift in onus on industry areas such as financial agreements and mobile phone contracts. For now, the unclarity of terms and unclarity in the distribution of responsibilities regarding who needs to provide comprehensible information, could easily bring about relationships of accountability, rather than trust, which is bad news for the farmer. According to O’Neill, informed consent in relation to accountability tends to enhance the power of the more powerful, such as health care providers and researchers in a biomedical context, or the digital expert agribusinesses in digital farming. Whenever unwanted effects of data sharing occur, the agribusiness can refer back to the consent that farmers gave and say that they received all appropriate information and afterwards gave consent. Therefore, if someone is to blame for possible detrimental effects of the decision, it is the consenters themselves. This happens more easily, when procedures of informed consent are digitized: agribusinesses send information to

the farmer and if the farmer consents by ticking a box, he or she becomes responsible for everything that follows.

Tailoring information to needs when data are re-used

The EU Code attempts to articulate what information should be included in a contract. The list of information on page 5 (this list is already quoted above) includes information about the purposes for which information is used, technical information about the software utilised, and ‘transparent mechanisms for adding new and/or future uses’. It is worth noting, however, that the possibility to re-use data may open a whole range of questions regarding the information that has to be given prior to making a contract.

It is in line with the spirit of informed consent to go back to data originators to ask for consent about re-uses of data. However, it is also questionable whether it is practically feasible and desirable to do that for every new use of the data.

We believe that it is important here to learn from the limitations of informed consent in the biomedical field, where the governance of the use and re-use of increasingly large repositories of biomedical data (such as data that represent the entire genome) in biobanks has led to a lot of discussions. While medical data are self-evidently different from farm data, we think that discussions in this context allow to draw attention to relevant limitations of informed consent as a data governance model. It is important to take these into account, for informed consent is now proposed all over again to govern uses and re-uses of farm data, whereas many authors have drawn attention to its limited value.

Discussions about re-use of biomedical data began to emerge around 15 years ago, when sequencing technologies that allowed to look at the entire genome began to emerge. In line with informed consent requirements, commentators initially stressed the importance of asking for consent for every individual project re-using data. This allowed research subjects to say ‘no’ to every re-use, if the risks were not acceptable to them (Helgesson and Johnsson 2005; Gertz 2008; Eriksson and Helgesson 2005; Chalmers 2011). However, in practice, it also quickly turned out to be an elaborate, time-consuming and expensive administrative task to re-contact the many individuals contributing to a biobank, which was sometimes fruitless, as contributors sometimes moved or died since they originally gave their consent to the storage of their data in the biobank. Furthermore, it was questioned whether consent was truly informed as genetic information could be used for a wide variety of purposes that were difficult to foresee at the moment when consent was asked. Giving voluminous and complex information was considered burdensome to research subjects, as it takes time to read and it is difficult to comprehend (Ashton-Prolla et al.

2015; Bunnik et al. 2013; Cambon-Thomsen et al. 2007). Without being informed, however, the consent procedure risked becoming meaningless.

Responding to these problems, some authors proposed to ‘simplify’ the informed consent procedure (Knoppers 2004). They proposed to abandon asking specific consent for each and every research project that was being carried out on samples or data, but instead adopt broad or generic consent, meaning that biobanks should ask a person for his or her consent for the storage and re-use of samples or data for a variety of future research projects, without specifying the projects for which they are being used (Hempel et al. 2012; Wendler 2006). Broad consent was, according to some objections, however not really *informed*. Therefore other authors proposed ‘tiered consent’ which would allow contributors to make more than one choice: after choosing to store samples/data in the biobank, they were presented a menu of other choices, which could specify for what specific types of research (for example: cancer research), or by what types of users, their data could be used (such as publicly funded researchers or private companies) (Hansson 2009; Wolf and Lo 2004; Hofmann 2009). It has been noted, however, that all of these options come with problems, as the idea of informed consent suggested that the consenter comprehends what he or she consents to, and the information provided about that is rather limited. Some authors therefore proposed to have a group of representatives of research subjects take a role in developing data sharing policy of biobanks (Boeckhout et al. 2014). This would make it possible that research subjects share their data with the biobank, and then after that, the panel of representatives will take charge of the governance of those data. This would liberate researchers from having to ask for consent for each specific use of the data, while still granting donors a role in managing the purposes for which their data are being used.

Lessons learned in the context of data governance in the biomedical field have hitherto insufficiently informed the governance of farm data. While it seems good to ask for informed consent and empower farmers to make a choice, it is also important to be clear about the limitations of that consent. While the burden lies on the agribusinesses to take responsibility to inform farmers about what they do with the farmer’s data, careful choices have to be made about how much information can reasonably be provided and comprehended by farmers concerning the re-use of the data. It will likely overburden farmers, if they are re-contacted over and over again and have to read through piles of information and find out whether or not a specific new use of their data is acceptable to them. Digitizing the process of information provision (which is sometimes suggested as a solution to this problem³⁹) will not really solve these problems, as it is

impossible to see whether the information provided responds to information needs of the variously situated farmers.

Possible ways to limit that information would be to offer farmers a menu of choices, such as: giving them a choice between different possible users of their data (e.g. companies, governments, researchers), or between different types of purposes for which their data could be used (such as, for research by publicly funded researchers, to inform policy-making, to inform banks and insurance companies, to develop innovative applications by businesses etc.). Alternatively, if farmers find it difficult to make such choices, farmers could choose to have their data stored in a larger repository, which is governed by a group of farmer’s representatives specialized in data governance issues, who could lay down general principles (e.g. fiduciary or public interest ones) governing decision-making concerning data re-use. In this way, individual farmers would delegate their decision to these representatives, who make the policy for the data repository and develop guidelines governing how they can be used and to whom data users can turn to ask for access to specific data sets. The discussion about such alternatives, however, has not yet started.

Conclusion

Reflecting on the concept of trust and its relationship to contractual relationships, we have drawn attention to some limitations of the EU Code. We agree with the makers of the EU Code that a contract, or informed consent, can make an important contribution to trust relationships as it is needed to mitigate the detrimental effects of power relationships between experts and non-experts. Building on Onora O’Neill’s perspective to informed consent as a trust maintainer, however, we argued that a contract can only be successful in fostering trust when (a) information is comprehended by the more vulnerable party in this relationship who has to sign the contract, (b) the more powerful partner takes responsibility to provide that information, and (c) information is tailored to the information needs of the party signing the contract, even when data are re-used over a longer period.

While these three elements of the EU Code are probably satisfied in the daily practice of forming agreements between farmers and agribusinesses, the support that the Code itself offers for it could be improved. Some of the detail in the EU Code is confusing as, (a) it introduces unclear terminology, (b) responsibilities in the contract procedure are not clearly distinguished and distributed and therefore a contract risks to protect the agribusinesses in relationships of

³⁹ See for example initiatives such as DjustConnect and Joindata.

accountability instead of fostering trust and (c) the discussions about the limited role of informed consent procedures in the governance of use and re-use of large biomedical datasets in biobanks are insufficiently taken into account in the formation of the EU Code, thus risking to make the same mistakes all over again in the context of farming when the recommendations of the EU code are followed.

The EU Code has gone to some lengths to make trust a topic of reflection and conversation between agribusinesses and farmers, which is an important step in the right direction. This provides an important contribution to ag-tech innovation, as trust is a vital problem that could hinder acceptance within agricultural industries. However, given the philosophical perspectives on trust and its relation to contracts and socio-phenomenological contexts, we believe it is also important to reflect on the question whether a contract is ever able to function as a *trust builder* in relationships that are just emerging. Using the perspective of Manson and O'Neill on informed consent, which can be carried out formally as a contract or informally as a spoken agreement, we gave arguments to doubt this. According to Manson and O'Neill, informed consent functions as a *trust maintainer*: it is able to maintain trust in relationships that are already established and in which people lead their lives without thinking about all the ways in which others can harm them. Their expectation not to be harmed by others is supported by prohibitions, norms and rights that everyone tends to respect. Informed consent is just used in situations where people who are already part of these relationships need to do things that disobey prohibitions or disrespect rights that would otherwise apply, and on which their trust is based.

In digital farming, however, trust relationships are not necessarily already existent. As Wolfert et al. have shown, in a lot of contexts digital technologies will effect quite a fundamental change in the social network around farms (Wolfert et al. 2017). Farmers have traditionally had trusted relationships with many actors such as advisors, cooperatives, farmer's associations and input suppliers. In these relationships they knew what to expect. With the introduction of actors from the software industry, farmers are asked to engage in new and frequently more abstract relationships than they are used to. While start-ups and relatively small tech companies often do engage with farmers in real life through face to face agreements about collaboration, it is expected that these relationships will become increasingly digitized and thus abstract, as these companies and their client numbers grow. Contractual deals with large tech companies are not likely sealed by a traditional hand-shake and will seldom happen face to face. We expect that expansion of the number of people who will share data in the network, as well as the increasing geographical distance between them, will lead to the development of tools that digitize the informed consent

process. However, the theory of informed consent gives important reason to doubt that these efforts will by themselves lead to trust. They may also come to function as protection for the agribusinesses who make the digital technologies, as they can always refer to the consent of the farmer as a justification for what they do with the data.

Reflections about contracts, informed consent and trust give reasons to approach digital innovation in a contextual way. Trust in digital technology is more likely to come about if it is introduced in contexts with already established relationships and collaborations, or when innovators invest significant time and effort in fostering trusted social relationships before introducing their technologies. These relationships will demand continued care and nurturing. If these relationships are non-existent to begin with, it is questionable whether a contract alone can create trust. In more abstract relationships, it could be advisable to broaden the code of conduct and give partners in this uneven power relationship a richer range of topics to think and talk about, in order to develop broader conditions for their mutual engagement. Codes of conduct that have been developed for other groups of professionals (such as engineers, researchers or physicians (Davis 1991)) usually include informed consent in a wider menu of requirements, which relate to a wider variety of principles. In the biomedical field, for example, the demand to respect the autonomy of research subjects and patients (which is done with informed consent), figures next to principles that demand to do good (beneficence), to not inflict harm (non-maleficence) and to be just (Beauchamp and Childress 2001).

A Code of Conduct which aims to foster trust in the sharing of farm data should also be richer. It could consider, for example, including responsibilities for agribusinesses to use the data to develop services that help farmers thrive, or adopt protective measures against making them vulnerable for new risks and harms that farmers may still be unaware of, or could commit to fostering broader (and more just) accessibility of the technologies for farmers with little digital expertise or resources to spend on buying the technologies. Rather than seeking solely transparency and consent, the EU Code would then foster trust by engaging all partners in a shared effort to realize fairer and more equitable outcomes for the diverse partners in the data-sharing network.

Acknowledgements We thank Hugh Breakey for his comments on an earlier draft of this paper, which allowed to us to make improvements. We thank Griffith University 2019 Short Term Visiting Research Fellowship for funding the collaboration between the authors that led to this article. Also, the contribution of the first author that led to this article was part of the project Internet of Food and Farming (www.IOF2020.eu), which is funded by the Horizon 2020 Framework Program of the European Union. Grant Agreement No. 731884. This project will work on the issues that come forwards in the discussion of this article. We would also like to thank Prof Jay Sanderson for his thoughts and contributions.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- American Farm Bureau Federation. (2019). Privacy and security issues for farm data, centennial. Retrieved October 20, 2019, from <https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data>.
- Ashton-Prolla, P., Goldim, J. R., Vairo, F. P., da Silveira, M. U., & Sequeiros, J. (2015). Genomic analysis in the clinic: Benefits and challenges for health care professionals and patients in Brazil. *Journal of Community Genetics*, 6, 275–283.
- Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics*. New York: Oxford University Press.
- Boeckhout, M., Reuzel, R., & Zielhuis, G. (2014). *The donor as partner. How to involve patients and the public in the governance of biobanks and registries*. Graz: Biobanking and Biomolecular Research Infrastructure.
- Bronson, K. (2018). Smart farming: including rights holders for responsible agricultural innovation. *The Technology Innovation Management Review*, 8, 7–14.
- Bronson, K., & Knezevic, I. (2016). Big data in food and agriculture. *Big Data & Society*, 3, 1–5.
- Bunnik, E. M., de Jong, A., Nijsingh, N., & de Wert, G. M. (2013). The new genetics and informed consent: Differentiating choice to preserve autonomy. *Bioethics*, 27, 348–355.
- Cambon-Thomsen, A., Rial-Sebbag, E., & Knoppers, B. M. (2007). Trends in ethical and legal frameworks for the use of human biobanks. *European Respiratory Journal*, 30, 373–382.
- Carbonell, I. M. (2016). The ethics of big data in agriculture. *Internet Policy Review*, 5, 1.
- Carolan, M. (2017). Publicising food: big data, precision agriculture, and co-experimental techniques of addition. *Sociologia Ruralis*, 57(2), 135–154.
- Chalmers, D. (2011). Genetic research and biobanks. *Methods in Molecular Biology*, 675, 1–37.
- Coeckelbergh, M. (2012). Can we trust robots? *Ethics and information technology*, 14(1), 53–60.
- COPA COGECA (European Farmers European Agri-Cooperatives) et al. (2018). Copa and Cogeca highlight importance of EU Code of Conduct on agricultural data sharing at high-level conference (Press Release, CDP(18)5022:1, 26 June 2018). Retrieved October 20, 2019, from www.copacogeca.eu/Download.ashx?ID=1838642&fmt=pdf.
- European Commission. (2016). *Legal study on ownership and access to data*. Report no 2016/0085. Retrieved October 20, 2019, from <https://publications.europa.eu/en/publication-detail/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1>.
- European Commission. (2017). A framework for the free flow of non-personal data in the EU (Press Release, IP/17/3190). Retrieved October 20, 2019, from https://europa.eu/rapid/press-release_MEMO-17-3191_en.htm;%2520https://europa.eu/rapid/press-release_IP-18-3364_en.htm%3E.
- COPA-COGECA et al. (2018). EU code of conduct on agricultural data sharing by contractual agreement. Retrieved October 20, 2019, from https://www.copacogeca.eu/img/user/files/EU%2520CODE/EU_Code_2018_web_version.pdf.
- Council of the European Union. (2018). EU to ban localisation restrictions as ambassadors approve deal on free flow of data (press release, 29 June 2018). Retrieved October 20, 2019, from <https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/eu-to-ban-data-localisation-restrictions-as-ambassadors-approve-deal-on-free-flow-of-data/>.
- Davis, M. (1991). Thinking like an engineer: The place of a code of ethics in the practice of a profession. *Philosophy & Public Affairs*, 15, 150–167.
- Davison, M. (2016). Database protection: Lessons from Europe, congress, and WIPO. *Case Western Reserve Law Review*, 57(4), 831–833.
- Dawson, A. (2009). The normative status of the requirement to gain an informed consent in clinical trials: comprehension, obligations and empirical evidence. In O. Corrigan, J. McMillan, K. Liddell, M. Richards, & C. Weijer (Eds.), *The limits of consent. A socio-ethical approach to human subject research in medicine* (pp. 99–113). Oxford: Oxford University Press.
- De Beer, J. (2016). *Ownership of open data: Governance options for agriculture and nutrition*. Wallingford: GODAN.
- Díaz, E. (2016). The new European Union general regulation on data protection and the legal consequences for institutions. *Church, Communication and Culture*, 1(1), 208.
- Eastwood, C., Klerkx, L., Ayre, M., & Dela Rue, B. (2017). Managing socio-ethical challenges in the development of smart farming: From a fragmented to a comprehensive approach for research and innovation. *Journal of Agricultural and Environmental Ethics*, 32, 741–768.
- Eriksson, S., & Helgesson, G. (2005). Potential harms, anonymization, and the right to withdraw consent to biobank research. *European Journal of Human Genetics*, 13, 1071–1076.
- European Council of Young Farmers (CEJA). (2019). *Two new partners sign up to the EU code of conduct on agricultural data sharing*. Rome: European Council of Young Farmers (CEJA).
- European Crop Protection Association (ECPA). (2018). Code of conduct on agricultural data sharing signing. European Crop Protection Association. Retrieved October 20, 2019, from <https://www.ecpa.eu/news/code-conduct-agricultural-data-sharing-signing>.
- Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford: Oxford University Press.
- European Feed Manufacturers' Federation, Press Release. (2018). Retrieved October 20, 2019, from <https://www.fefac.eu/latest-news/press-releases/25458/>.
- Fleming, A., Jakku, E., Lim-Camacho, L., Taylor, B., & Thorburn, P. (2018). Is big data for big farming or for everyone? Perceptions in the Australian grains industry. *Agronomy for Sustainable Development*, 38, 24.
- Gertz, R. (2008). Withdrawing from participating in a biobank—A comparative study. *Eur J Health Law*, 15, 381–389.
- Hansson, M. G. (2009). Ethics and biobanks. *British Journal of Cancer*, 100(1), 8.
- He, L., Lu, Y., & Wu, H. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1–6), 1.
- Helgesson, G., & Johnsson, L. (2005). The right to withdraw consent to research on biobank samples. *Medicine, Health Care and Philosophy*, 8, 315–321.
- Hempel, C., Lomax, G., & Peckman, S. (2012). Broad consent in biobanking. *Nature Biotechnology*, 30(9), 826.
- Hofmann, B. (2009). Broadening consent—And diluting ethics? *Journal of Medical Ethics*, 35, 125–129.

- Jakku, E., Taylor, B., Fleming, A., Mason, C., Fielke, S., Sounness, C., et al. (2017). A review on the practice of big data analysis in agriculture. *Computers and Electronics in Agriculture*, *143*, 23–37.
- Jakku, E., Taylor, B., Fleming, A., Mason, C., Fielke, S., Sounness, C., et al. (2019). If they don't tell us what they do with it, why would we trust them? Trust, transparency and benefit-sharing in Smart Farming. *NJAS Wageningen Journal of Life Sciences*. <https://doi.org/10.1016/j.njas.2018.11.002>.
- Janzen, T. (2018). Data ownership questions—And why they're important. *Future Farming*, 3 October. Retrieved October 20, 2019, from <https://www.futurefarming.com/Tools-data/Articles/2018/10/Data-ownership-questions--and-why-theyre-important-340743E/>.
- Knoppers, B. M. (2004). Biobanks: Simplifying consent. *Nature Reviews Genetics*, *5*, 485.
- Kshetri, N. (2014). The emerging role of big data in key development issues: Opportunities, challenges, and concerns. *Big Data & Society*, *1*, 1–20.
- Manson, N. C., & O'Neill, O. (2007). *Rethinking informed consent in bioethics*. Cambridge: Cambridge University Press.
- National Farmers Federation. (2020). Australian farm data code. <https://nff.org.au/programs/australian-farm-data-code/>.
- New Zealand's Farm Data Code of Practice. Retrieved October 20, 2019, from <https://www.farmdatacode.org.nz/>.
- O'Neill, O. (2002). *Autonomy and trust in bioethics*. Cambridge: Cambridge University Press.
- O'Neill, O. (2003). Some limits of informed consent. *Journal of Medical Ethics*, *29*, 4–7.
- Poppe, K., Bogaardt, M. J., & Wal, T. (2016). *The economics and governance of digitalisation and precision agriculture*. Briefing paper 4. Precision agriculture and the future of farming in Europe. Technical horizon scan. Brussels: STOA.
- Rasmussen, N. (2016). From precision agriculture to market manipulation: a new frontier in the legal community. *Minnesota Journal of Law, Science & Technology*, *17*, 489–516.
- Regan, Á. (2019). 'Smart farming' in Ireland: A risk perception study with key governance actors. *NJAS-Wageningen Journal of Life Sciences*, *90*, 100292.
- Rodriguez, D., de Voil, P., Rufino, M. C., Odoendo, M., & van Wijk, M. T. (2017). To mulch or to munch? Big modelling of big data. *Agricultural Systems*, *153*, 32–42.
- Sanderson, J., Leanne Wiseman, L., & Poncini, S. (2018). What's behind the ag-data logo? An examination of voluntary agricultural data codes of practice. *International Journal of Rural Law and Policy*, *8*, 6043.
- Schneider, M. (1998). The European Union database directive. *Berkeley Technology Law Journal*, *13*(1), 553–556.
- Schuster, J. (2017). Big data ethics and the digital age of agriculture. *Resource*, *24*, 20–21.
- Stam, C., & Michalopoulos S. (2018). EU agri-food operators sign milestone data sharing deal. *Euractiv*, 24 April. Retrieved October 20, 2019, from <https://www.euractiv.com/section/agriculture/news/eu-agri-food-operators-sign-milestone-data-sharing-deal/>.
- Sykuta, M. (2016). Big data in agriculture: Privacy, property rights and competition in ag Data Services. *International Food and Agribusiness Management Review*, *19*, 57–74.
- Taddeo, M. (2010a). Modelling trust in artificial agents, a first step toward the analysis of e-trust. *Minds and Machines*, *20*(2), 243–257.
- Taddeo, M. (2010b). Trust in technology: A distinctive and a problematic relation. *Knowledge, Technology and Policy*, *23*(3–4), 283–286.
- Van der Burg, S., Bogaardt, M.-J., & Wolfert, S. (2019). Ethics of smart farming: current questions and directions for responsible innovation towards the future. *NJAS Wageningen Journal of Life Sciences*. <https://doi.org/10.1016/j.njas.2019.01.001>.
- Wendler, D. (2006). One-time general consent for research on biological samples. *British Medical Journal*, *332*(7540), 544–547.
- Wiseman, L., Sanderson, J., & Lachlan Robb, L. (2018). Rethinking ag data ownership. *Farm Policy Journal*, *15*(1), 71–77.
- Wiseman, L., Sanderson, J., Zhang, A., & Jakku, E. (2019). Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming. *NJAS-Wageningen Journal of Life Sciences*, *90*, 91.
- Wolf, L. E., & Lo, B. (2004). Untapped potential: IRB guidance for the ethical research use of stored biological materials. *IRB*, *26*, 1–8.
- Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M. J. (2017). Big data in smart farming—A review. *Agricultural Systems*, *153*, 69–80.
- Zhang, A., Baker, I., Jakku, E., & Llewellyn, R. (2017). *Accelerating precision agriculture to decision agriculture: The needs and drivers for the present and future of digital agriculture in Australia. A cross-industry producer survey for the Rural R&D for profit 'precision to decision' (P2D) project*. EP175936. Canberra: CSIRO.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.