Realising the full potential of precision agriculture: encouraging farmer 'buy-in' by building trust in data sharing

Assoc. Prof Leanne Wiseman
Griffith Law School, Griffith University
Nathan, Brisbane
Australia

Assoc. Prof Jay Sanderson
USC Law School
USC, Queensland, Australia

A paper from the Proceedings of the
14th International Conference on Precision Agriculture
June 24 – June 27, 2018
Montreal, Quebec, Canada

Abstract. "Realising the full potential of precision agriculture: encouraging farmer 'buy-in' by building trust in data sharing"

Keywords. *Precision ag, data sharing, law, trust*

Uncertainty around the ownership, privacy and security of farm data are most commonly the reasons cited for farmer's reluctance to "buy-in" to big data in agriculture. Evidence provided to the recent US Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protections, Product Safety, Insurance, and Data Security, United States Senate Technology in Agriculture: Data Driven Farming (Nov 2017) highlighted that "data ownership, and related privacy and security issues, are problems that are frequently discussed in relation to Big Data and analytics ...[that are] concerns that need to be addressed."

This paper will draw upon results of the Accelerating Precision Agriculture to Decision Agriculture (P2D) research project, funded by the Australian Commonwealth Government (Department of Agriculture and Water Resources as part of its Rural R&D for Profit program) and all 15 of Australia's key agricultural funders, the Rural Development Corporations (lead by the Cotton RDC), which included a large farmer survey completed with 1000 farmers from a broad range of Australian agricultural industries that highlights their attitudes and concerns about data sharing. While over 74% of Australian farmers knew nothing or very little about the terms and conditions of their data contracts what is more telling is the fact that over 62% lack trust in their service providers in the way that they deal with farm data.

In this paper, we examine how good governance in data sharing develops and builds trust between farmers, agribusinesses and service providers. Providing clarity around issues of data ownership, privacy and security will empower farmers to fully understand the terms and conditions upon which they are willing to share their data. We draw upon the broadening of the notion of "consent" that is being re-examined in light of the General Data Protection (GDPR) Regulation in the European Union (2016/679) which will take effect on the 25 May 2018. While this regulation is intended to strengthen and unify data protection for all individuals within the EU, it also addresses the export of personal data outside the EU. While farm data is not yet seen as personal data, lessons can be drawn from developments in privacy to empower farmers to take steps to ensure more transparency in their dealings with technology providers.

1. Introduction

Uncertainty around the ownership, privacy and security of farm data are most commonly the reasons cited for farmer's reluctance to "buy-in" to big data in agriculture. Evidence provided to the recent US Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protections, Product Safety, Insurance, and Data Security, United States Senate Technology in Agriculture: Data Driven Farming (Nov 2017) highlighted that "data ownership, and related privacy and security issues, are problems that are frequently discussed in relation to Big Data and analytics ...[that are] concerns that need to be addressed." These issues are the very same that Australian farmers encounter when engaging with precision agricultural technologies. In this paper, we provide targeted consideration of the current legal and regulatory issues that were flagged

as important to Australian farmers, particularly as identified by *the Accelerating Precision Agriculture to Decision Agriculture* (P2D) research project that was completed in March 2018. (Leonard et al, 2018)

One of the key components of the research conducted in relation to farmer's attitudes to precision agriculture and their concerns around the sharing of their on farm data was the large farmer survey completed with 1000 farmers from a broad range of Australian agricultural industries (17 in all) that highlighted their attitudes and concerns about data sharing. (Zhang, A., et al, 2018) What this survey reinforced is that while over 74% of Australian farmers knew nothing or very little about the terms and conditions of their data contracts, what is more telling is the fact that over 62% lack trust in their service providers in the way that they deal with farm data. This coupled with issues such as 'Who owns data?' and 'Is my data safe and private?' form the basis of the analysis of the reluctance of farmers to fully embrace precision agricultural technologies thus arguable denying its full potential.

Concern over the potential for (mis)use of digital technology and data is not just a topic for Australian farmers, and is not unfounded. For example, in 2017 in Oklahoma, a group of American chicken farmers sued the country's biggest poultry processors, including Tyson Foods Inc. (*Haff Poultry v Tyson et al.*, 2017) for allegedly conspiring to depress their pay, the latest accusation of improper collusion in the sector. It was alleged that Tyson, Pilgrim's Pride Co, Sanderson Farms Inc. and other companies illegally agreed to share detailed data on grower pay with one another to keep payments below competitive levels.

2. Current state of data rules dealing with ownership, access, privacy and trust

Before examining farmers' concerns about the use and reuse of their farm data, it is useful to provide an overview of the way the law approaches data ownership, control and access as it is the absence of understanding of clear legal rules within the agricultural industry as a whole that is contributing to the lack of trust that is behind the reluctance of farmers' to fully embrace precision ag technologies.

2.1 Data ownership, control and access

The current legal framework around data ownership, control and access in Australia, like many other jurisdictions, is complex and fragmented.

2.1.1 Who owns data?

There is no general property right in raw data. While data is an asset (e.g. a farm that has five years of data is clearly worth more than a farm that has no historical data), data is unlike other forms of physical property that is owned. Ownership rights in data will only arise if copyright law can protect the data. Not all data or collections of data will attract copyright protection. It has long been recognised that raw data, information or mere facts are not protectable subject matter under copyright law. However, aggregated data in the form of a data base may attract copyright protection.

However, under copyright law, the ownership of copyright can be varied by contract. So if there is a contractual arrangement between the farmer and the third party that

addresses ownership of the data collected, then the ownership provisions in the contract (if any) will override the position in copyright law. It is worth noting at this point that most other countries, such as the United Kingdom, Canada and the United States, take a similar approach to data ownership. That is, the law of copyright is the primary means by which ownership of datasets (but not raw data) may be claimed.

However, by way of contrast, in the European Union database creators have been given a specific property right, known as a database right since 1996. This right is a right to prevent extraction and/or reutilisation of the whole or of a substantial part of the contents of a database. To gain this protection, the database creator must establish that there has been a substantial investment in the obtaining, verification or presentation of the contents. The term of protection is 15 years, but it is renewable whenever the database holder makes any substantial change to the contents of the database. To determine whether a use is an infringement of the database right, both the qualitative and/or quantitative measure will be considered. (See *Directive on the Legal Protection of Databases 1996*.)

2.1.2 Data contracts: Data control and access

In recognition of the fact that copyright law allows contracts to override its ownership provisions, it is necessary to focus on the data contracts (licences) that are entered into between the data contributors (i.e. farmers) and data aggregators. This is important, as contracts are the primary means by which agricultural data in Australia (and elsewhere) is being controlled, managed and shared. In many ways, speaking about the right to control data is more helpful than speaking about a right of ownership of data.

Many data licences involve the use a 'click wrap' agreement (where the click of an 'I agree' icon signifies consent to the terms of a software licence), and this is often the way farmers enter into and agree to data licences for agricultural technology. The data licences that are embedded in digital agricultural technologies are generally complex standard-form licence agreements that are generally non-negotiable and presented on a 'take it or leave it' basis when the technology is adopted. The terms of use of the technology are therefore agreed to either at the time of downloading an app or turning on a machine.

This is when knowledge of all of the terms of the licence becomes an important issue, as it is when the contract between the technology supplier and the farmer is formed.

While best practice in contracting is that parties are aware of and agree to the terms of the licence prior to entry into the contract, in practice where there is the use of the 'click' wrap agreements, there is very little opportunity for farmers to view, let alone negotiate, the terms of the data licences. Farmers are presented with and often have no option but to accept a number of standard terms of use that relate to the ownership, control and use of the data collected. Often a data licence will also provide links to other policy documents such as the agricultural technology provider's privacy policy. In some cases, it is the privacy policy rather than the terms of use of the data licence which outlines who may have access to the data generated under the agreement

3. Concerns with current data licences

The results of the P2D research project suggest that farmers' concerns about the current data licences that govern their data can be grouped into three major themes:

1. a lack of transparency about the terms of use in data licences, particularly in relation to who may have access to the data that is being shared,
2. inequality of bargaining power, and
3. a lack of benefit-sharing between farmers (i.e. data contributors) and third party advisers/agri-business (i.e. the data aggregators).

3.1 Lack of transparency

One of the major concerns raised by farmers was the lack of transparency over the terms of the data licences that govern the use of their agricultural data. Farmers expressed concern about the lack of information they were given at the point of sale about data ownership, control and sharing prior to entering contracts with agri-businesses.

The survey that was conducted as part of the P2D project has revealed that 47% of farmers surveyed said they have no understanding and an additional 27% said they have little understanding of the terms and conditions of data licence agreements before signing up to a new software or service, particularly where the service is provided online. The fact that so many farmers are unaware of the terms that govern the ownership and use of, and access to, their data indicates that there appears to be very little discussion about issues relating to data ownership or access prior to entering a contract for agricultural technology or services. As farmers do not understand the implications of what they are signing, they are often unaware of how much control the service provider is asserting over their data or the extent to which their data is being shared and traded.

One clear concern of farmers is the fact that their farm data is regularly traded or disclosed to third parties, leaving farmers unaware of who knows the details of their commercial enterprises.

This was highlighted by the recent review by the Australian Productivity Commission, which concluded that:

> One of the most potentially pernicious practices with data is the onward trade or disclosure of data to third parties … The damage is not so much in cost terms but in the feeling of exploitation. This has great capacity to undermine social licence over time, if misused. (Productivity Commission, 2017, p. 212)

Farmers also expressed concern about the potential risk of loss of data following the wind-up or takeover of an agri-business. Uncertainty over the duration of the data licence agreement was another area about which farmers expressed concern. For example, some data licences provide that the agri-business 'will continue to have access to and use of past, current and future Customer content [data] during and after the term of this contract and the subscription'.

3.2 Inequality of bargaining power

Another concern raised by farmers is that many agri-businesses supplying services in the Australian agricultural industries are large multinational corporations. This is often

referred to as the digital data divide – a divide between those who contribute the data and those who control, aggregate and share the data. The power imbalance between data contributors and data aggregators is evidenced by the inability of farmers to negotiate the standard terms of the large agri-business' data licences that govern the agricultural technology, and is well accepted (Carbonell, 2016).

The fact that many large agri-businesses involved in digital agriculture are foreign owned is another important factor when examining the level of trust and confidence that farmers have in their terms of use. Often these licence agreements will be governed by the law of the country where that company is registered. This creates uncertainty over the level of protection afforded to Australian farmers. For example, farmers may not have the benefit of protections of Australian law, such as the Australian Consumer Law (ACL) or the *Small Business and Unfair Terms Act* that was passed to regulate unfair terms in business-to-business contracts in 2016.

The ACL was amended in 2016 to redress the imbalance in the bargaining position between large businesses that rely upon standard term contracts when dealing with small business enterprises, such as those in farming by expanding the unfair contracts term legislation to 'small businesses' that employ fewer than 20 persons. While there are some notable exceptions, many farmers operate businesses that would fall under this definition of a 'small business'.

Under the changes to the ACL, a contract term may be declared *void and unenforceable* if three criteria are met:

1. the contract is a *standard-form contract* for the supply of goods and services (including financial services) or the sale or grant of an interest in land,

2. where the upfront price payable under the contract does not exceed $300,000 for contracts shorter than one year (or $1,000,000 for contracts longer than 12 months), and

3. the term is 'unfair'.

When considering these criteria in light of ag-data licences, it appears that, as many agricultural technology providers use *standard-form contracts* for the supply of their digital services, this criterion would easily be satisfied in many cases.

The second requirement of the unfair terms legislation is in relation to the 'upfront price' of less than $300,000 for contracts shorter than one year (or $1,000,000 for contracts longer than 12 months). As many digital licence agreements are either annual licences (or agreements that are in place for the life of the machinery/technology), this criterion would also appear to be satisfied by many of the agricultural data licences.

The third requirement for the unfair terms provisions to operate is that the term is 'unfair'. Terms are 'unfair' where they could cause:

- a significant imbalance in the parties' rights and obligations; and
- it is not reasonable necessary to protect the legitimate interest of the party relying upon the term; and
- the term would cause detriment (financial or otherwise).

When determining whether the term is unfair, the extent to which the term is 'transparent' and how it relates to the contract is considered.

Put simply, 'transparency' means whether the term can be understood in reasonably plain language, is presented clearly, and is readily available to any party affected by the term.

As many of the terms in ag data contracts (which relate to the ownership, privacy, security and sharing of farm data with third parties) are not discussed or made clear prior to entry into the contracts, it is arguable that they could not be 'transparent' for the purposes of the unfair terms legislation. In some instances, the small print is locked under layers of policies that can only be found on the websites of some agri-businesses.

Where the terms of the licences allow for broad access rights to be granted to third parties without the knowledge of the farmer, the test of 'unfairness' could arguably be satisfied. This is particularly the case when these terms are not made transparent to the farmer prior to entry into the contract.

This reform indicates that the practice of using standard-form contracts comes with a responsibility on the part of the larger businesses to ensure that their contractual terms are transparent and fair in the sense that they do not go beyond what is legitimate to protect their legitimate interest and that they do not create a significant imbalance in the parties' rights and obligations. This in turn, empowers farmers by giving them a right to hold businesses to account where their terms of use are not 'fair'.

3.3 Lack of benefit sharing between data aggregators and data contributors

Many Australian farmers who were surveyed were concerned that advisers or agri-businesses derive the greatest benefit from their data. While recognising the value added by the third-party aggregators, farmers recognise that they are the original contributors of their agronomic data, and are thus responsible for the integrity and quality of the data that is later aggregated and analysed. Farmers are concerned that businesses are making money from their data without sharing any of the benefits with the original data contributors.

While there were some examples of cooperative benchmarking exercises that returned benefits to member farmers, many farmers expressed concern that the real value of sharing data was not yet being returned or shared with them. While improved knowledge, products and services is often said to be the real benefit of digital agriculture being returned to farmers, many said they were uncomfortable about the current business models of them contributing their data for nothing but then paying full cost for the services delivered from the aggregated data.

4. Data privacy, safety and security

Another of the key concerns expressed by Australian farmers is whether their data is private, safe and secure.

4.1 Distinguishing personal and non-personal data

Not all data is treated equally. While many Australian farmers are clearly concerned about the security of their personal, financial and health data, they are less concerned about the use of agronomic data (e.g. yield and nutrient data) or machine data (e.g. sensor and machine data). Importantly, Australian privacy law distinguishes between different types of data or information – that is, personal and non-personal information. Put simply:

- Personal Information is data or information that can be used to identify a person, such as name, address, location data, telephone number, medical records and bank account details.
- Non-personal information is data or information that cannot be used to identify a person. Often, data such as agronomic data, machine data and weather data is non-personal information.

The distinction between personal and non-personal information is an important one to make because under Australia's *Privacy Act 1988*, a set of Australian Privacy Principles (APPs) exists that applies only to 'personal information'. By contrast, 'non-personal information' is generally governed by the law of contract.

The Productivity Commission states that:

> [A] common misperception is that privacy laws – or, indeed, the privacy policies of individual organisations – give individuals ownership over data created by or about them. Privacy legislation, the primary generic tool offering individuals some control, regulates how personal information is collected, used and disclosed. (Productivity Commission, 2017, p. 53)

So, when farmers are wondering whether their data is safe and secure (and what companies may do with their data), one of the first things to do is to determine whether the data in question is 'personal information'. So, is agricultural data personal information?

Agricultural data is not generally 'personal information'. However, it is possible that in some circumstances, certain agricultural data could identify an individual and thus be personal information. Perhaps one example of data being personal information is GIS or location data. Once the geographic coordinates are known, and this is used to bring data together, the collection of that data may then point to an individual. This could possibly mean that the GIS location could be viewed as potentially personal information. Another way in which agricultural data may be personal information is where data from different sources are connected (e.g. GIS, machine and production data), which may also point to individuals.

Many agri-businesses companies are APP entities and are required to comply with the APPs for personal information. To this end, they have privacy policies and statements that set out how they handle, use and manage personal information that can be found on their respective websites.

4.2 Personal information, the APPs and big data

While not legally binding, the draft *Guide to Big Data and the Australian Privacy Principles* (the Guide) outlines key privacy requirements and encourages the implementation of the Privacy Management Framework to facilitate big data activities while protecting personal information. The Guide sets out considerations and privacy tips, which are useful for ensuring compliance with APP guidelines and the *Privacy Act 1988* when handling personal information for big data activities.

The Guide encourages entities to use big data and to conduct big data activities in a way that personifies the privacy principles, and includes matters such as ensuring that

personal information is collected through 'lawful and fair means'; that data is only disclosed for the primary purpose for which it was created, how entities should ensure the quality and security of the information they possess and 'tak[ing] reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure'.

It is important to note, however, that the APPs specifically concern 'personal information'. Thus, Australian farmers' data must fall within the definition provided by the Act to be within the application of the APPs. For non-personal information (i.e. most agricultural data), the contract that exists between a farmer, their business and the agricultural data entity is vitally important.

2.2.4 Data and contracts

Much data generated on farm such agronomic data, machine data and weather data is not generally 'personal information'. If data cannot be used to identify an individual (i.e. non-personal information), then the *Privacy Act 1988* and APP do not apply. Instead, that data or information is either not regulated at all or is governed by contract. Therefore, given that a large portion of data is non-personal information, contracts are the mean by which this data is controlled.

One strategy for facilitating more transparent and fairer data contracts is to encourage agricultural technology providers to engage in discussion around appropriate principles, policies and practices. An example of this comes from the industry-negotiated set of guidelines announced on 13 November 2014, which were negotiated by the American Farm Bureau Federation (AFBF), the National Farmers' Union and the national trade groups for soybean, corn, wheat and rice growers, and by several leading agricultural data companies including John Deere, Monsanto's Climate Corporation, DuPont Pioneer and Dow AgroSciences. The Privacy and Security Principles for Farm Data recommend and facilitate clear, simple and transparent data contracts, as well as notification if there are any changes to the contracts. More specifically, the key principles of the AFBF's Privacy and Security Principles for Farm Data consider a range of topics including education; ownership; collection, access and control; notice; transparency and consistency; and liabilities.

While the benefits of policy statements such as the AFBF's Privacy and Security Principles on Farm Data are questioned by some, what is important about such initiatives is the role that they lay in raising awareness among farmers and the agricultural communities about the concerns arising from data ownership and the privacy and security of farm data.

5. Strenthening and Empowering the position of data contributors

5.1 European approach to empowering data contributors

Over the past 5 years, there has been increasing scrutiny by Governments over the way in which personal data is being exchanged and disseminated though digital transactions. One of the key shared concerns has been that many of those data exchanges potentially breach the privacy laws that were enacted to protect individuals.

On 14 April 2016, the European Parliament adopted the General Data Protection Regulation 2016 (GDPR). The Regulation entered into force on 24 May 2016 and its provisions will be directly applicable in all Member States on 25 May 2018. The EU General Data Protection Regulation (GDPR) replaces the older Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.

A general theme of the Regulation is that organisations must be accountable for all of their data processing activities. This Regulation will apply to the processing of personal data by controllers or processors in relation to the activities of their establishment in the EU, regardless of where the processing actually takes place.

Of particular interest, is the expansive notion of 'consent' that has been incorporated into this new Data Regulation. When consent has been obtained to process personal data, the controller must be able to demonstrate that the consent is freely given, specific and informed. Consent will be purpose-limited, i.e. it will permit processing only for explicitly specified purposes. The consent obtained must be intelligible, easily accessible, and in clear and plain language. This is intended to eliminate any confusion as to whether consent has or has not been given, and whether it can be implied by a particular action (or inaction). Data subjects must also have the right to revoke their consent at any time and it must be as easy to withdraw consent as it is to give it.

The 2016 EU GDPR shows a very important change in the attitude and approach to data management, placing more responsibility of those who collect, aggregate and process personal data. This is shown by the need for controllers have not only obtained prior consent from their data subjects for the particular purpose but also that their data subjects have the ability to revoke that consent at any time. This signals an important change in the approach to what is good data management and the impact this is having across information and digital industries, including those in agriculture, cannot be underestimated.

5.2 Empowering Australian Consumers and Small businesses in relation to their Data

Along a similar vein to the GDPR in the EU, in Australia, on 8 May 2017, the Australia Productivity Commission released its final report into data availability and use in Australia. If implemented in its current form, the Report's recommendations will have a fundamental impact on the way agricultural data is managed. More specifically the Commission noted that:

> fundamental and systematic changes are needed to the way Australian governments, their industries and business handle data (Productivity Commission, 2017, p. 12).

The Commission also deliberately recommended:

> the creation of a new, broad-reaching Data Framework that should, by design, be capable of enduring beyond current technologies, policies, personnel and institutional structures (Productivity Commission, 2017, p. 13).

At the centre of the recommended Australian reforms is a new *Data Sharing and Release Act* and a National Data Custodian to guide and monitor new access and use arrangements, including proactively managing risks and broader ethical considerations around data use.

In its final report, the Commission proposed two facets to Australia's data framework for the future:

1. a new right that enables both opportunities for active data use by consumers (and small business) and fundamental reform in Australia's competition policy, and
2. a structure for data sharing and release that would allow access arrangements to be dialled up or down according to the different risks associated with different types of data, uses and use environments.

If implemented, both facets of the Productivity Commission's recommendations will have a major impact on the collection, collation and management of agricultural data in Australia.

5.2.1 Comprehensive right for consumers (and small businesses)

Under the Productivity Commission's recommendations, consumers (and small businesses) would be given the right to:

- share in perpetuity joint access to and use of their consumer data with the data holder,
- receive a copy of their consumer data,
- request edits or corrections to it for reasons of accuracy,
- be informed of the trade or other disclosure of consumer data to third parties, and
- direct data holders to transfer data in machine-readable form, either to the individual or to a nominated third party.

These five new rights to information defined as 'consumer data' make up the comprehensive right. It is comprehensive because it is intended to apply across the economy, to all data-holding entities – whether in the private or public sector.

At its broadest level, the Productivity Commission has indicated that consumer data (and small business data) should include:

- personal information (as defined in the *Privacy Act 1988*) that is in digital form,
- files posted online by the consumer,
- data created from consumers' online transactions, internet-connected activity or digital devices,
- data purchased or obtained from a third party that is about the identified consumer, and
- other data associated with transactions or activity that is held in digital form and relevant to the transfer of data to a nominated third party.

When applying this to agricultural data, the definition of consumer data would capture data that is collected remotely from agricultural technology providers. While the Australian Government is rolling out this reform sector by sector, it is intended that the laws will extend to all sectors so the potential of such a monumental change to Australia's

approach to the way data is managed will most definitely have an impact on the way agricultural data is managed.

5.3 Developing Farmer Trust

Trust is an essential component in the relationship between farmers and agricultural service providers. Farmers want to know that their data is adequately protected and used fairly. Over 36 % of respondents in the Australian Farmer survey had no trust whatsoever in service/technology providers not sharing their data with third parties. A lack of trust regarding the way in which data is collected, stored and shared has the potential to limit the benefits of digital technologies and data. Building trusted relationships around agricultural data is critical to maintaining successful business relationships in digital agriculture.

In its 2017 Report on Data Availability and Use, the Productivity Commission noted that:

> Lack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia's data. In fact, improving trust community-wide is a key objective. (Productivity Commission, 2017, p. 2)

Trust in data contracting will develop when attention is paid to developing transparency around the terms that govern the collection, aggregation and sharing of a farmer's data.

Trust is more evident when parties are free to negotiate the terms of their commercial relationships themselves. Farmers enter into many data contracts where they can negotiate the terms that govern the relationship. One example is the relationship between a farmer and their adviser or agronomist. In these arrangements, best practice suggests that open dialogue between the service provider and the farmer about any concerns the parties have about the way in which data being collected from the service will be managed would result in an arrangement that would be more agreeable to both parties.

To enhance trust, issues of ownership and access to data need to be discussed at the start of the commercial relationship, as the parties to the agreement are more likely to be comfortable with the arrangements that will govern the data. To do this, farmers need to be empowered with knowledge of their rights of privacy in certain situations but also of the general trend towards more open transparent transactions that take into account the rights of the data contributor.

It is useful at this point to note the approach taken to 'transparency' under the Australian Consumer Law (ACL) standard-form contracts. The notion of 'transparency' takes into account whether the terms are clearly present, and whether they are expressed in reasonable plain language and available to any party that is affected by the term. Examples of terms that may not be considered 'transparent' include those that are hidden in fine print or schedules, those phrased in legalese or in complex or technical language, or those that are ambiguous or contradictory.

To develop a *genuine* two-way street to support farmers continued willingness to supply a crucial input to agricultural data (i.e. their data), agri-businesses should ensure that their terms governing data are more transparent, as without this trust will be hard to achieve.

Some data certification schemes can enhance trust because farmers are assured that an independent and objective party has evaluated the service provider's practices and deemed them worthy of certification. So, provided the business is confident about the accreditor's credibility, and it seeks the qualities as certified under the scheme, trust can be placed in a provider that has attained certification under the scheme. It also aims to help farmers verify the 'responsible' nature of the services and technologies they purchase (Bartiaux, 2008). In a similar vein, certification marks for ag-providers may increase transparency and trust between farmers and service providers because it certifies that the provider's data practices adhere to prescribed standards. The trust would lie largely in the fact that the provider was assessed and accredited under an independent scheme, by an objective party.

Data certification is not without its challenges, and it is not a one-size-fits-all solution. (Sanderson, 2018) One of the most crucial aspects of ag-data certification is "buy in". Like all voluntary programs, ag-data standards and certification depend on participation from agri-business and farmers. The effects of ag-data certification depend on agricultural companies deciding to adopt the standards and seek certification. Typically, the introduction of standards and certification has been in response to industry or government initiatives (e.g. funding); not necessary as a response to farmer or agri-business demand. Currently, it appears that there is little incentive for agribusiness to seek certification and accreditation. That said, as farmers become increasingly aware of data use issues they will be looking for 'good' products and services that are more transparent and fairer in the way they deal with ag-data. Therefore, voluntary ag-data standards and certification can be part of the ag-data regulatory mix, and can help to govern ag-data access and use.

Conclusion

There is no doubt that good governance in agricultural data sharing develops and builds trust in the farmers in the way in which their farm data will be managed in the future. Providing clarity around issues of data ownership, privacy and security through good governance frameworks will empower farmers to fully understand the terms and conditions upon which they are willing to share their data. While many of the steps taken to increase the level of transparency around the collection, aggregation and sharing of farm data to date have focused on the role and approach taken by agribusinesses and the third party service providers, it is suggested that to build farmer trust in precision ag technologies and the way in which the data that is collected is managed, that it is time to fully engage farmers in the dialogue about what good governance and good policy of ag data management looks like.

The broadening of the notion of "consent" that is being re-examined in light of the General Data Protection Regulation (GDPR) in the European Union (2016/679) which will take effect on the 25 May 2018, provides a perfect opportunity to bring farmers into the dialogue and discussion about what constitutes full and open consent to data sharing in the agricultural context. The fact that the GDPR reinforces the need for the language of data licensing to change – to a simpler, less complex language that can be easily understood – provides further grounds for farmers to expect nothing less when transacting with their service providers.

Other ways to empower farmers is to make sure there is room at the table when discussions about what good governance and good ag policy looks like to ensure the

concerns and issues arising from current ag data management practices are taken into account from a farmer perspective. To have full and open discussions of the specific terms of use and consent provisions around the sharing of farm data would help to strengthen the position of farmers achieve more transparency in their dealings with technology providers.

References

Legislation

Australian Privacy Act 1988 (Cth) and Australian Privacy Principles

EU Directive on the Legal Protection of Databases 1996.

EU General Data Protection Regulation 2016

Journals

Albersmeier, F., Schulze, H. and Spiller, A. (2010) "System dynamics in food quality certifications: development of an audit integrity system". *International Journal of Food System Dynamics*, 1(1): 69-81.

Bartiaux, F. (2008) "Does environmental information overcome practice compartmentalisation and change consumers' behaviours?" *Journal of Cleaner Production*, 16(11): 1170-1180.

Carbonell, I. (2016) "The ethics of big data in big agriculture". *Internet Policy Review*, 5(1).

Sanderson, J., Wiseman L., Porcini 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,* forthcoming.

Online Documents

American Farm Bureau Federation (2014) *American Farm Bureau Federation's Privacy and Security Principles for Farm Data*. http://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data. Accessed 24 February 2018.

Australian Productivity Commission, Data Availability and Use, May 2017, available at https://www.pc.gov.au/inquiries/completed/data-access#report, accessed January 2018.

Leonard, E. (Ed), Rainbow, R. (Ed), Trindall, J. (Ed), Baker, I., Barry, S., Darragh, L., Darnell, R., George, A., Heath, R., Jakku, E., Laurie, A., Lamb, D., Llewellyn, R., Perrett, E., Sanderson, J., Skinner, A., Stollery, T., Wiseman, L., Wood, G. and Zhang, A. (2017). Accelerating precision agriculture to decision agriculture: Enabling digital agriculture in Australia. Cotton Research and Development Corporation, Australia. Available at https://www.crdc.com.au/sites/default/files/CRD18001-001%20CRDC%20P2D%20Report%20low%20res.pdf, accessed 28 March 2018.

Wiseman, L. and Sanderson, J. (2017). The legal dimensions of digital agriculture in Australia: An examination of the current and future state of data rules dealing with ownership, access, privacy and trust. Griffith University, USC Australia and Cotton Research and Development Corporation, Australia, available at https://www.crdc.com.au/precision-to-decision, accessed 28 March 2018.

United States Senate, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Technology in Agriculture: Data-Driven Farming, 14 November 2017, available at https://www.commerce.senate.gov/public/index.cfm/2017/11/technology-in-agriculture-data-driven-farming, accessed 24 February, 2018.

Zhang, A., Baker, I., Jakku, E.,, and Llewellyn, R., *Accelerating precision agriculture to decision agriculture: The needs and drivers for the present and future of digital agriculture in Australia. A cross industries farmer survey for the Rural R&D for Profit 'Precision to Decision*, (P2D) project. (2017) CSIRO and Cotton Research and Development Corporation, Australia, available at https://www.crdc.com.au/precision-to-decision, accessed 28 March 2018.