

TECHNICAL REPORT

ACCELERATING PRECISION AGRICULTURE TO DECISION AGRICULTURE

Enabling digital agriculture in Australia



This Project is supported by funding from the Rural R&D for Profit Program



Australian Government
Department of Agriculture and Water Resources



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. L Wiseman and J Sanderson



About the authors

Leanne Wiseman is an Associate Professor in Law at the Griffith Law School, Griffith University and Associate Director of the Australian Centre for Intellectual Property in Agriculture (www.acipa.edu.au). Leanne researches and publishes in the areas of intellectual property, corporate and contract law. Leanne's current research focuses on the intersection between law and agriculture, with particular focus on the legal issues arising from the adoption and uptake of digital agricultural technologies.

Contact: l.wiseman@griffith.edu.au

Jay Sanderson is an Associate Professor in Law at USC Australia and a member of ACIPA. He is also an Adjunct Research Fellow with the Law Futures Centre (Griffith Law School, Griffith University). Jay researches and publishes in the areas of law, food and agriculture. Jay's recent publications include: *Plants, People and Practices: The Nature and History of the UPOV Convention* (Cambridge University Press, 2017); 'Not Free to Roam: Misleading Food Credence Claims, the ACCC and the Need for Corporate Social Responsibility' (2017) 43(1) *Monash University Law Review* 113 (with S. Hobill); and 'Health Conscious and Confused: Why 'Healthy' Trade Marks Matter' (2016) 39(2) *University of New South Wales Law Journal* 658.

Contact: jsander4@usc.edu.au

Acknowledgments

The authors would like to acknowledge the contributions of the producers, service and technology developers and providers, researchers and industry partners. They would also like to thank Carol Ballard, and our Research Assistants, Sharn Hobill, Sam Poncini, Lachlan Robb, Berta Nagy, Chamila Talagala, Mike Crowley and Elizabeth Clark.

Copyright

© Griffith University, USC Australia and Cotton Research and Development Corporation (CRDC) 2017.

ISBN: 978-0-6482462-0-6 (Hard Copy) 978-0-6482462-1-3 (Electronic)

To the extent permitted by law, all rights are reserved and no part of this publication covered by copyright may be reproduced or copied in any form or by any means except with the written permission of Griffith University, USC Australia and CRDC.

Griffith University and USC Australia advises that the information contained in this publication comprises general statements based on scientific research. The reader is advised and needs to be aware that such information may be incomplete or unable to be used in any specific situation. No reliance or actions must therefore be made on that information without seeking

prior expert professional, scientific and technical advice. To the extent permitted by law, Griffith University and USC Australia (including its employees and consultants) excludes all liability to any person for any consequences, including but not limited to all losses, damages, costs, expenses and any other compensation, arising directly or indirectly from using this publication (in part or in whole) and any information or material contained in it.

The project that delivered this report is led by the Cotton Research and Development Corporation and is jointly funded by the Department of Agriculture and Water Resources Rural Research and Development (R&D) for Profit Program and all 15 Rural Development Corporations.

Contents

Executive summary	i
Key findings	i
Recommendations	v
1. Introduction	1
1.1 Background	2
1.2 Structure and content of this Report	5
2. Current state of data rules dealing with ownership, access, privacy and trust	7
2.1 Data ownership, control and access	7
2.1.1 Who owns data?	7
2.1.2 Data contracts: Data control and access	11
2.1.3 Proposed future reforms allowing for access to data.....	18
2.1.4 International developments on agricultural data ownership and access.....	23
2.1.5 Key findings on data ownership, control and access	25
2.2 Data privacy, safety and security	26
2.2.1 Distinguishing personal and non-personal data	27
2.2.2 Data that is ‘personal information’	29
2.2.3 Personal information, the APPs and big data	30
2.2.4 Data and contracts.....	30
2.2.5 Other issues around privacy, security and data.....	31
2.2.6 Key findings on data privacy, safety and security	36
2.3 Data: Trust, transparency and certification	37
2.3.1 Contracts: Trust and transparency	38
2.3.2 Current attempts to develop trust and transparency in data practices	39
2.3.3 Ag-Data co-operatives and other collaborative initiatives	49
2.3.4 Findings on trust, transparency and certification	55
References and Further Reading	57

Executive summary

Currently, the legal and regulatory frameworks around agricultural data are piecemeal, fragmented and ad hoc. The aim of this part of the P2D project is twofold: first, to outline the current state of data rules dealing with data ownership, access, use, liability and licensing in Australian agriculture; and second, to recommend an effective, efficient and ethical data governance framework for Australian agriculture.

This Report has four parts:

1. Introduction,
2. Data ownership, control and access,
3. Data privacy, safety and security, and
4. Data: trust, transparency and certification.

In this Executive Summary, we provide our key findings on the current state of agricultural data governance and present recommendations to ensure that the legal and regulatory framework for Australian agriculture is digital and data ready.

Key findings

Key findings on data ownership, control and access

1. Many producers will own copyright in the datasets that they create, while many third parties will own copyright in the aggregated datasets. While Australian copyright law provides ownership rights to both producers and third parties in different situations, in practice, with digital agriculture, it is the contracts that are entered into between producers and third parties, such as advisers and agri-businesses, that will govern the ownership of their data, rather than copyright law.
2. Producers and their advisers and agri-businesses should note that mere payment for data services does not result in a transfer of data ownership, unless there is a contract that deals with data ownership.
3. A number of ag-technology providers encrypt their digital farming software. This restricts the ability of producers to access software that would inform them of the diagnostic and

repair information of their farm machinery. This, in turn, prohibits producers from attempting to repair or modify their machinery.

4. Producers are unaware of the terms of data licences that they are entering. The general lack of discussion of the terms of the data licences at both a broad industry level and at individual points of sale of agricultural technologies contribute to the lack of trust about the management of agricultural data.
5. Agri-businesses that rely upon standard-form data licences should recognise that they have a responsibility to ensure that their contractual terms are legible, transparent and fair, and they are readily available to contracting parties.
6. It is imperative that the terms of use that govern the aggregation, ownership, storage and dissemination of producers' agricultural data be made more transparent to producers prior to their entry into commercial relationships with third-party advisers and technology service providers. This is particularly the case where standard-form licences are used.
7. To support producers' continued willingness to supply their agronomic data to agri-businesses, producers need to see and be assured of the benefits that they are receiving in the form of improved goods and services or knowledge.
8. The Productivity Commission's *Final Report on Data Availability and Use* will, if implemented, have a fundamental impact on the way that agricultural data is managed in Australia. Open dialogue is needed between data contributors, data aggregators and industry stakeholders about the future management practices of data in the agricultural sector.
9. Open access to publicly funded research and its underlying data, including agricultural research, is now a well-entrenched mandate of governments around the world, and of public and private agricultural funders.
10. Australian agricultural industry must keep abreast of international developments in this field.

Key findings on data privacy, safety and security

1. Australian producers are concerned about third parties gaining unauthorised access to their data. Their priority is to ensure that their data is kept private, safe and secure.
2. Not all data is treated equally, and under the *Privacy Act* a distinction is made between personal and non-personal information.
3. The current privacy policies used by businesses in digital agriculture tend to deal with personal information only. A consequence of this is that agricultural data, as it is generally not personal information, does not have the protections under *Privacy Act*. It is therefore vulnerable to unauthorised use unless protection is afforded by contract between the parties.
4. The absence of clear and consistent data governance within Australia's rural industries has the potential to expose Australian producers to threats to their privacy, security and safety of their agricultural data. This limits the potential benefits that can be derived from digital agriculture.

Key findings on trust, transparency and certification

1. Many Australian producers lack trust in service and technology providers when collecting and sharing their data.
2. In Australia, there are no governing principles that clarify and build trust in producers around the access and use of agricultural data. An absence of appropriate and dynamic ag-data standards and licensing arrangements contributes to the lack of trust producers have towards data contracts.
3. There is an urgent need for a genuine two-way relationship between agri-businesses and Australian producers. This will facilitate a willingness to supply and share agricultural data. To achieve this, third parties and agri-businesses should ensure that their terms governing data are more transparent and available, and that this is clearly communicated to producers.
4. Globally, ag-data certification and labelling is being used to indicate to producers that service and technology providers meet certain data standards. For example: in the United States (with the Ag Data Transparency Evaluator) and New Zealand (with the NZ Farm

Data Code). While the process by which third parties' data licences are certified can instill confidence and trust in producers the evidence on this is unclear.

5. A trade or certification mark can be used to develop and communicate certain standards around data practices. A data certification scheme can involve a registered trade or certification mark; registering a standard trade mark provides more flexibility and is less onerous than registering a certification mark.
6. While there are different reasons for introducing an Australian ag-data certification scheme, it is first necessary to have a clearly articulated set of goals and objectives. Without this, it will be difficult, if not impossible, to develop appropriate standards and processes of certification. Similarly, without specific goals and objectives it will be impossible to evaluate the effectiveness of such schemes and to conduct any meaningful review of the schemes once they are introduced. Further, if an ag-data scheme is introduced—and is to provide an instrument to promote good data management—then RDCs and industry must work hard to convince producers and agribusinesses that the standards and associated certification represent value.
7. Other collaborative models, including data cooperatives, have been used to manage ag-data access and use. More research needs to be done to assess the impact and effectiveness of ag-data co-operatives. It is important that Australian industries or individuals do not blindly follow what is happening elsewhere (e.g. in the United States). Indeed, it is difficult to distinguish the ag-data co-operative marketing and hype from their substance and effectiveness. While it is hard to argue with the aims and ideals of data co-operatives (e.g. the pooling of producer ag-data for their benefit) the devil is in the detail, particularly around: ag-data co-operative rules and formation; the difficulty of attracting and retaining members and/or investment; and how, and with whom, the data will be shared.

Recommendations

Recommendation 1

Australian rural policy makers and rural industries should work towards developing a clear and consistent **national voice** in relation to the need for developing clear, ethical and efficient agricultural data practices.

Recommendation 2

It is recommended that key rural stakeholders, including Rural Development Corporations and expert members, should commit to an **Information and Data Management Collaborative Working Group**. There are a number of ways in which this could be achieved, including:

Option 1: Through the establishment of a cross-industry **Information and Data Management Collaborative Working Group**

Option 2: In the absence of a cross-industry approach, by the establishment of industry-specific **Information and Data Management Working Groups**.

Recommendation 3

It is recommended that an **Australian Agricultural Data Governance Strategy** be developed. There are a number of ways in which this could be achieved, including:

Option 1: Through a cross-industry **Information and Data Management Collaborative Working Group**

Option 2: In the absence of a cross-industry approach to the development of an Ethical Australian Agricultural Data Governance Strategy, by rural sectors developing individual industry-specific **Industry Specific Agricultural Data Governance Strategies**.

Recommendation 4

It is recommended that, once the Information and Data Management Working Group has developed policies about the control and use of data, each of Australia's Rural and Development Corporations should **develop data policies and industry guidelines** that implement and complement the overarching Ethical Framework for Agricultural Data Governance.

Recommendation 5

It is recommended that, in order to implement an Agricultural Data Governance Framework, **dynamic data standards and licensing arrangements** should be established. Key areas of concern include: obtaining prior and informed consent when collecting and using data; being transparent about the reasons for collecting data; making sure data is secure; allowing producers to access their own data; not sharing data with third parties without prior consent; and notifying of breaches.

Recommendation 6

It is recommended that the merits of the creation and implementation of a voluntary Data Code of Practice—that would set out the standards for ethical and transparent data practices that advisers and agribusinesses must meet when providing services to producers—be investigated by rural industries and rural policy makers. In signing up to the Data Code of Practice, advisers and agricultural technology providers would agree to act in an ethical and transparent manner in all their data dealings with Australian producers.

Recommendation 7

It is recommended that **education and capacity building** is needed for producers, agribusinesses, rural industries and their stakeholders to increase knowledge and understanding of best practice in data management and data licensing.

To assist broader industry education and capacity building, cross-industry discussion and consultation needs to occur on the merits of **developing training programs and schemes** that assist in the development of skills, capabilities and digital literacy.

Recommendation 8

It is recommended that rural industries develop and implement a **communication and extension strategy for Agricultural Data Management**. There are a number of ways in which this could be achieved, including:

- Option 1: Through the establishment of a cross-industry **communication and extension strategy**, or

Option 2: In the absence of a cross-industry approach, by the establishment of an industry specific **communication and extension strategy**.

Recommendation 9

It is recommended that the merits of the creation and implementation of **data certification or accreditation schemes**, as well **data cooperatives** and **other collaborative models**, for Australian agricultural data be investigated.

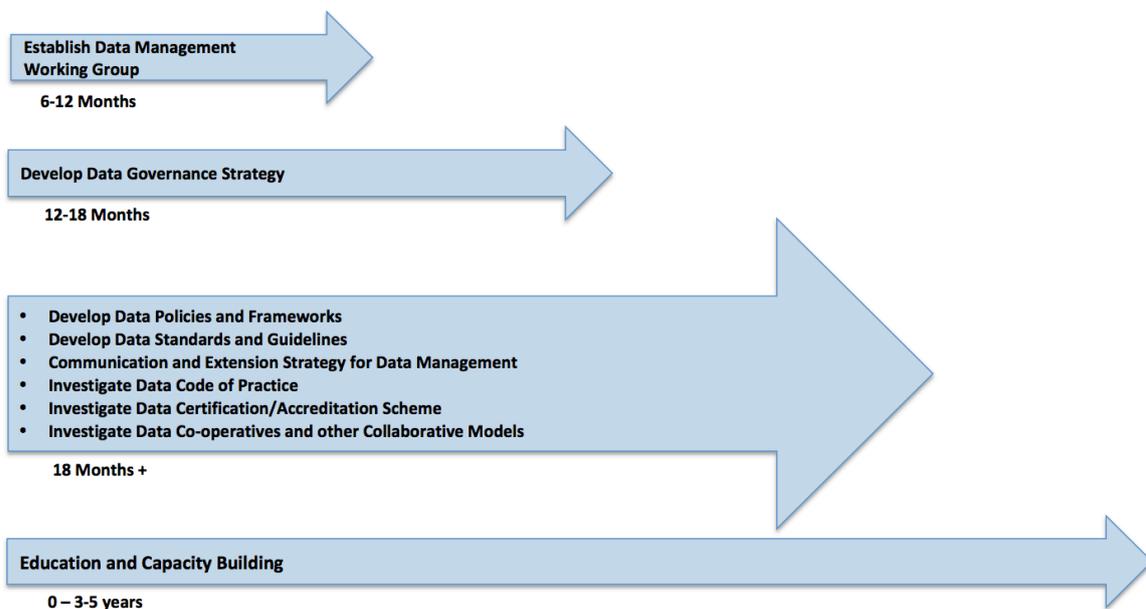


Figure 1: Timeframe for recommendation

1. Introduction

Currently, the legal and regulatory frameworks around agricultural data (data) are piecemeal and ad hoc. Because the aim of this part of the ‘Accelerating Precision Agriculture to Decision Agriculture’ (P2D) project is to outline the current state of data rules dealing with data ownership, access, use, liability and licensing in Australian agriculture, and then to recommend an effective and efficient data-governance framework for Australian agriculture, this report does not provide an exhaustive or descriptive overview of all laws and regulations related to the management and use of Australian agricultural data. Instead, it provides targeted consideration of the current legal and regulatory issues that were flagged as important to Australian producers, particularly as identified by P2D research, agri-business forums, producer workshops and producer surveys. During the P2D Project, Australian producers frequently asked questions about data, including: ‘Who owns data?’, ‘Is my data safe and private?’ and ‘Should I trust service providers with my data?’

The key concerns identified by the P2D Project relate to ownership, trust and privacy of data.

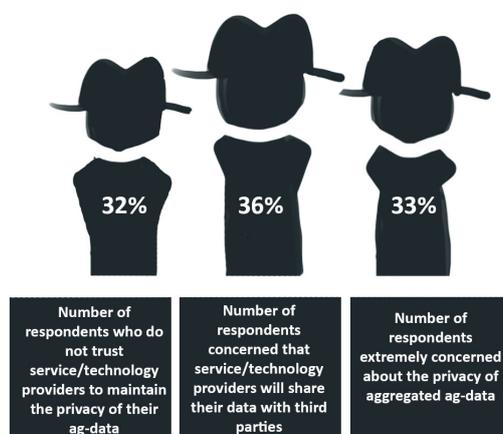


Figure 2: Key findings of P2D Project on ownership, trust and privacy

Concern over the (mis)use of digital technology and data is not just a topic for Australian producers, and is not unfounded. For example, in Oklahoma in 2017, 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.

To allay concerns over ag-data access and use, numerous industry organisations and groups are introducing various initiatives and schemes to improve data practices, and to help producers better understand them. For example, under the New Zealand Farm Data Code of Practice (*'NZ Farm Data Code'*), organisations agree to disclose their practices and policies around data rights, data processing and sharing, and data storage and security. In return, these organisations can display the Code of Practice trade mark on their websites and documents. In the United States in 2014, the American Farm Bureau Federation (AFBF) negotiated with a number of large agri-businesses to a set of Privacy and Security Principles for Farm Data that addressed the concerns of US farmers about ownership and control of, and access to, their farm data. To support US farmers, a guide called *Ponder These 9 Before You Sign* was also developed in conjunction with the Privacy and Security Principles. Soon afterwards, the AFBF developed the Ag Data Transparency Evaluator to help US farmers understand how their data would be used when they adopted precision agriculture technologies. The tool was created by the AFBF and backed by a consortium of farm industry groups, commodity organisations and agricultural technology providers to bring transparency, simplicity and trust to the contracts governing precision agricultural technologies (Ag Data Transparent, 'FAQ'). For more information on the Ag Data Transparency Evaluator and the associated 'approval' process and logo see section 2.3.2 of this Report.

In November 2017, there were further discussions about the issues raised by data driven farming by the US Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security in their hearing, *Technology in Agriculture: Data-Driven Farming*. U.S. Sen. Moran's opening statement highlighted 'the collection and use of [ag] data raises issues regarding control of the data [and] transparency of agreements between farmers and data firms.' These issues are the very same that Australian producers encounter when engaging with digital agricultural technologies. (Available at <https://www.commerce.senate.gov/public/index.cfm/consumerprotectionproductsafetyandinsurance>.)

1.1 Background

Before we outline the structure and content of this Report, it is necessary to highlight and acknowledge the previous research and reports published on the various issues in digital agriculture as well as to make some general comments about the regulation and governance of digital technologies and data. These are important to set the scene for the discussion that follows and

provide an outline of the background that informed our analyses of Australia producers' concerns and attitudes to the ownership, collection, control and use of data in the context of the broader rural sector. They also provide valuable resources for those wanting to read more about digital agriculture and data.

Research and reports on issues in digital agriculture

Over the last decade, some insightful research has been conducted into digital technologies, data and agriculture, including:

- Australian Farm Institute, *The Implications of Digital Agriculture and Big Data for Australian Agriculture* (May 2016)
- Birchip Cropping Group, *Connectivity Capability Trust: Creating Farmer Driver Traceability for Victorian Grain Exports using Precision Agriculture* (May 2017)
- CSIRO, *Trust and Collaboration: Exploring the Social-Technical Enabling Conditions for Big Data in the Grains Industry* (June 2016),
- Todd Sanderson, Andrew Reeson and Andrew Box, *Cultivating Trust: Towards an Australian Agricultural Data Market* (CSIRO, 2017), and
- a wide range of Nuffield Scholars' reports: including Jonathon Dyer's, *The Data Farm: An investigation of the implications of collecting data on farm* (October 2016).

General comments on the regulation and governance of digital technologies

- Governance and business models around digital technologies and data are key to supporting and encouraging the use of digital technology and data in the future. Importantly, governance is not synonymous with government regulation (e.g. legislation), and can also include industry and voluntary initiatives as well as co-operatives and other collaborative initiatives. Further, governance is not synonymous with data management, custodianship or stewardship (see Figure 3).

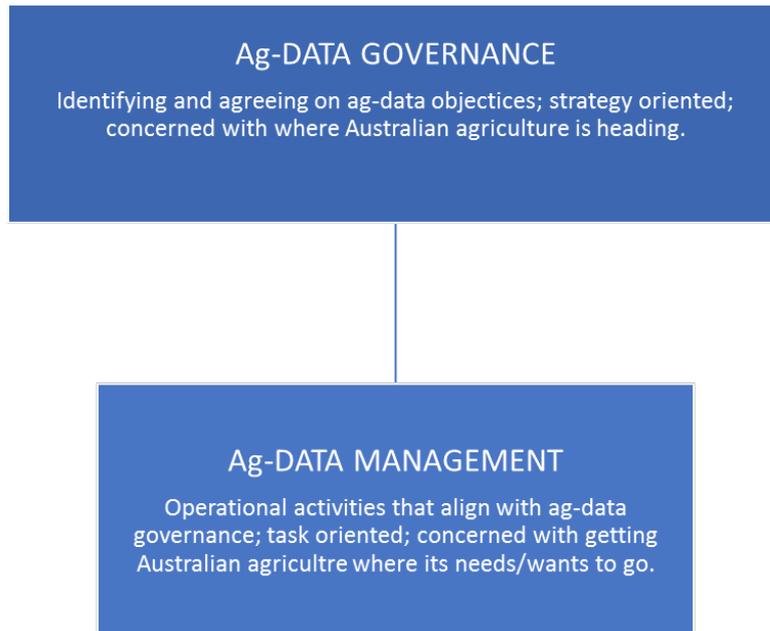


Figure 3. Ag-Data governance and management

- Globally, there is general acceptance by national governments, as well as public and private research funders, that publicly funded research should be made openly accessible. The rationale for this is that publicly funded research, including publicly funded agricultural research, should be made freely available to those who may wish to use it, so that society in general can benefit. In December 2015, Prime Minister Malcolm Turnbull made a commitment to the Australian people, as part of the Australian Government Public Data Policy Statement, that ‘the Australian Government commits to optimise the use and reuse of public data; to release non-sensitive data as open by default; and to collaborate with the private and research sectors to extend the value of public data for the benefit of the Australian public’.

The problem is that ‘open’ has various meanings, and data may be open for some, but not all, uses. Further, many technology and service providers are proprietary in nature. This raises conflict and tension between the desire for open access scientific – including agricultural – research and the incentives provided by restrictions on access to and use of data.

- Currently, there is little or no legislation in Australia that deals specifically with data. The key consequence of this legislative vacuum is that the main way in which duties and obligations around data are set out is in private data contracts (or licensing) agreements.

Although contracts are currently the most important aspect of data regulation, the Australian government and industry are increasingly trying to grapple with issues of data access and security. In late 2016, for example, the Productivity Commission was asked to:

- look at the benefits and costs of making public and private datasets more available,
 - examine options for collection, sharing and release of data,
 - identify ways consumers can use and benefit from access to data, particularly data about themselves, and
 - consider how to preserve individual privacy and control over data use.
- On 8 May 2017, the Productivity Commission released its final *Data Availability and Use* report, which recommends a fundamental shift in the approach taken to the management of data in Australia. If implemented, this will have a significant impact on the way data (including agricultural data) is managed. The federal government has established an intergovernmental committee to investigate and advance the Productivity Commission’s recommendations on data access.
 - It is not enough to merely copy or implement initiatives that have been used elsewhere. Australian agriculture needs to carefully think through what it wants to achieve with its data governance and management. Indeed, “buy in” is vital to the success of data principles and policies, and is one of the main challenges for voluntary schemes such as data certification and accreditation.

Finally, while data governance is crucial, it is only part of the answer in ensuring that digital technology and agricultural data have the potential to transform agriculture and agribusiness. The solutions to Australian digital and data needs must also include technical standards and analytics. Put simply, even the most effective data governance will be ineffective if technical capabilities and interoperability are absent or unworkable; and vice versa. Therefore, this Report needs to be read in conjunction with the other P2D Technical Reports which are available at <http://farminstitute.org.au/p2dproject>.

1.2 Structure and content of this Report

In summarising the current state of agricultural data governance and making recommendations about the future state of Australia’s agricultural data governance, the remainder of this Report is divided into three parts, with key findings presented at the end of each part. While there is some overlap between the legal issues that arise with these concerns, the remainder of the Report is structured around the concerns identified by the producer participants of the P2D project. Key areas of concern are:

- data ownership, control and access (2.1), which raises issues of the potential barriers posed by

Intellectual Property (IP) regimes such as copyright, the current contractual practices that regulate data ownership, control and use of ag-data and, importantly, the 2017 Productivity Commission review into data availability and access;

- data privacy, safety and security (2.2), which raises issues of privacy, confidentiality and contract, and
- data trust, transparency and certification (2.3), which raises issues of rural industry guidelines (e.g. US Farm Bureau, NZ Dairy), and reconciling openness and transparency with private contracts and commercial interests.

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

2.1 Data ownership, control and access

The current legal framework around data ownership, control and access is complex and fragmented. While many laws potentially impact the ownership and control of, and access to, data, our focus in this project has been to examine the legal issues that have been raised through workshops, surveys and discussions with primary producers, agri-business, and primary industries stakeholders.

At the outset, it is useful to highlight some of the key concerns that Australian producers raised about data ownership, control and access. Throughout the project, the following questions were asked:

- How is my data being used and who has access to my data?
- Who owns my data?
- Can I get my data back and use it in another system?
- What happens to my data if the company that has it merges with (or is sold) to another?
- Why does it feel like everyone seems to be making money from my data except me?

In addressing the legal issues raised regarding the ways in which agricultural data is currently owned and shared, this section of the report is divided into four parts:

- Who owns data? (2.1.1)
- Data contracts: Controlling and accessing data (2.1.2)
- Proposed future reforms allowing for access to data (2.1.3), and
- Current international developments on agricultural data ownership and access (2.1.4).

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 we own. As will be discussed in 2.1.2 of this Report, this means that talking about the right to control data is more helpful than talking about a right of ownership of data.

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.

In this section, we will examine briefly how copyright may protect and provide rights of ownership over data. We also note that copyright is the relevant area of law that provides ownership and protection over the digital software that is embedded in digital agricultural machinery, which gathers, stores and transmits data. We will examine the implications of the ownership of digital software later in this section.

While some datasets have copyright protection, many collections of data do not. It is for this reason that in the next part of this section (2.1.2), we will examine the role of contract law in determining ownership and control of, and access to, agricultural data.

Copyright

Copyright law in Australia does not provide protection for raw data or mere facts. So raw data itself is not capable of ownership under copyright law. Copyright law may, however, provide protection for tables or compilations of data where the selection and arrangement of the data has resulted from the input of some human labour, skill or effort.

At this point, it is useful to illustrate how copyright might protect data through some practical examples. In some rural industries, there is widespread use of analogue note-taking for data collection. Where this is the case, if the collection and arrangement of the data is collated by a producer into a table, compilation or report, then the data collector may have copyright in the data tables. Many primary producers have traditionally kept notes or records of data of their farming operations. Where this is the case, those producers may have ownership of the copyright in that collection and arrangement of data. As an owner of the copyright in the dataset, a producer has rights to control that data and may choose how they wish to exploit that data, and this may include sharing that data with others by the granting of a licence (i.e. permission to use). In many cases, where producers have collated data themselves and turned it into reports and so on, the producers will have ownership over those datasets.

Collection of rainfall data

A good illustration of the way the ownership principles of copyright law operate is to apply it the exercise of collecting rainfall. The measure of rain that falls each day is raw data and the measure itself in its purest form is not capable of protection under copyright law. However, once there has been an intellectual input or contribution to the rainfall collection, such as the selection or arrangement of daily rainfall data into information, then the aggregated rainfall data may be categorised as what is known as a 'table or compilation' in copyright law, which is able to be protected. A table or compilations of data would still need to be *original* to attract copyright protection. What this means is whether there has been *sufficient skill labor and effort* put into the creation of the data table or data compilation.

In this situation, the aggregator of the rainfall data compilation or table would be the copyright owner.

It is important to note that, under copyright law, ownership of copyright can be varied by contract so if the rainfall data were collected and collated by a third party who had permission to collect that data, and there was an agreement that addressed the issue of who owned the dataset, then that could alter the 'ownership' of the resulting data table.

Table 1: Example of ownership of rainfall data

Who owns copyright in a dataset when a third party collects and collates the data?

Several producers raised the issue of who owns the data and the resulting aggregated dataset when the data is collected by a third party, such as an adviser or a consultant or a technology service provider.

Put simply, where a third party is collecting and collating data with the permission of the producer, then copyright determines that whoever puts labour, skill and effort into the collection, selection and arrangement of the data into a dataset would be the owner of that dataset. In many cases, this would be the third party who aggregates the data into a dataset. It is not the producer who provides the raw data.

However, under copyright law, the ownership of copyright can be varied by contract. So if there is a contractual arrangement between the producer 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. For this reason, the focus will now shift to the data contracts that deal with ownership and access of data.

It is important to note here that that payment for a data service does not result in a transfer of copyright ownership of the resulting product (i.e. dataset) to the person who made the payment, unless a contract between the parties provides for this.

International approaches to data ownership

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*.)

Copyright protection for the software embedded in digital farming technology

Many agri-businesses are the copyright owners of the computer software that is embedded in the digital agricultural technology (e.g. farm machinery). Under copyright law, copyright owners are given an additional right to protect their software using 'locks'. These 'locks' can take the form of encryption, passwords or contracts (e.g. the terms of the licences themselves). It is common to see in data licence agreements terms that restricts the ability of the producer to 'access the software that is embedded in the digital ag technology'. The effect of such a clause is that if there is an issue with the software – such as a modification required – the producer is required to abide by the terms of the licence, which commonly provide that only an authorised service technician can access the software. It would be a breach of the data licence for the farmer to attempt to break the 'lock' on the digital program so that they could adjust the machine or the technology.

Given the size of rural properties and the vastness of rural Australia, producers expressed concern that the use of technology locks may mean a producer has to wait days to have an authorised service technician come to their property. The inability of producers to access the same agricultural

equipment diagnostic and repair information that is made available to the manufacturers' dealers and authorised repair facilities was raised as a concern by numerous producers.

The United States 'right of repair'

In the United States, the prohibition on accessing the software in farm machinery that is found in data licences has raised such concern within farming communities that the American Farm Bureau has recently joined into lobbying efforts for a 'Right of Repair' to be introduced into law in a number of states (https://motherboard.vice.com/en_us/article/farmers-right-to-repair).

'Right of repair' legislation has already been introduced into a number of US states, with Bills being introduced in Nebraska, Minnesota, New York, Massachusetts, and Kansas. A farm equipment repair bill has been introduced in Wyoming that closely mirrors the legislation in the other states, but would at least nominally be targeted only at tractors and other farm equipment. The legislation is modelled on the *Motor Vehicle Owners' Right to Repair Act*, a law passed in Massachusetts in 2012.

Lobbying efforts have also resulted in the US copyright defence of fair use being expanded to recognise that a right of repair of software programs embedded in digital machines may, in some circumstances, fall under the defence of fair use in 2015.

In January 2017, the American Farm Bureau resolved that the *US Digital Millennium Copyright Act* (DCMA) be amended to require agricultural equipment manufacturers to allow equipment owners and independent repair facilities to have access to the same agricultural equipment diagnostic and repair information made available to the manufacturers' dealers and authorised repair facilities.

John Deere is one of many agricultural technology providers that has strongly opposed the right of repair movement in the United States, reaffirming that producers only own the machines but not the technology embedded in the machines. John Deere and others stated that the reason for the encryption of their technology was to prevent the tampering with the technology, as it may lead to machinery being less effective or safe (see John Deere, *Long Comment Regarding a Proposed Exemption under 17 U.S.C 1201*, https://www.copyright.gov/1201/2015/comments-032715/class%2022/John_Deere_Class22_1201_2014.pdf).

2.1.2 Data contracts: Data control and access

In recognition of the fact that copyright law allows contracts to override its ownership provisions, this section will examine the data contracts that are entered into between the data contributors (i.e. producers and data aggregators). This is important, as contracts are the primary means by which

agricultural data in Australia 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.

As part of their agricultural business, producers enter numerous contracts with different parties for products and services. Some of the contractual relationships that producers enter that result in the collection and collation of agricultural data include for:

- chemical/fertilizer suppliers,
- broader service providers (e.g. telecommunications, sensors, soil testing, drones, etc.),
- agri-technology/agri-business providers, and
- third parties and professional advisers (e.g. agronomists, advisers).

Given that producers use commercial professional relationships and/or a range of technologies – such as sensors, drones and machinery – to collect and/or collate data, it is beyond the scope of this project to give a detailed examination of each data contract that Australian producers enter into. Further, many of these contracts are stated to be commercial-in-confidence, and thus cannot be reproduced. Each primary industry has an industry-focused range of commercial relationships. The more vertically integrated the industry, the tighter the contractual relationships tend to be. Given that many digital technologies rely upon standard-form software contracts, what follows is an examination of the standard terms that are most commonly found in data contracts.

Data licences

The data contracts currently in use in Australian agriculture take the form of a data licence. A licence is the granting of permission for the use of content protected by copyright – for example, a data licence allows the use of the data but does not grant ownership rights in relation to the data. As with many social media licences, the range of uses of data that is allowed can be so broad that they virtually operate as a transfer of ownership.

Many data licences involve the use of 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 producers 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 producer 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 producers to view, let alone negotiate, the terms of the data licences. Producers 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. These terms tend to cover a broad range of matters such as:

- who owns the data,
- who has rights in relation to the aggregated data,
- who the data may be shared with,
- where the data may be stored (including in which country),
- the security and privacy of the data,
- the duration of the contract,
- indemnities and liabilities in relation to the data,
- what may occur with the data when the contract comes to an end (legacy data),
- what happens with data when the business is sold or wound up,
- can data be migrated or transferred from one vendor to another, and
- where disputes about the data may be heard – for example, in which country a dispute under the agreement may be heard.

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 (see section 2.3 on Data: Trust, transparency and certification).

Producers' concerns with current data licences

The results of the P2D project suggest that producers' 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 producers (i.e. data contributors) and third party advisers/agri-business (i.e. the data aggregators).

Lack of transparency

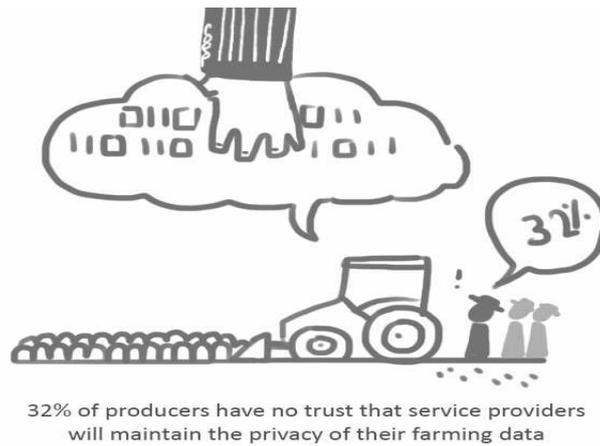
One of the major concerns raised by primary producers has been the lack of transparency over the terms of the data licences that govern the use of their agricultural data. Producers expressed concern about the lack of information they were given about data ownership, control and sharing prior to entering contracts with agri-businesses.

The Producer Survey that was conducted as part of the P2D project has revealed that 47% of primary producers surveyed say 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 producers 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 producers 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. This has significant consequence for the agricultural industry as a whole, as it forms the basis for the lack of trust that producers have towards some of the new digital services and products on offer.



One concern of producers is the fact that their data is regularly traded or disclosed to third parties, leaving producers unaware of who knows the details of their commercial enterprises. This was highlighted by the 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)

Producers 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 producers 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'. Transparency and trust are discussed further in section 2.3.

US approach to data licensing

To empower American farmers to be able to discuss data issues with their technology providers, the American Farm Bureau Federation, as part of its work on Data Security and Privacy Principles (see section 2.3.2) developed a list of questions that would help farmers learn more about how their technology providers would deal with their data. The questions raise matters such as who owns, controls and can access the data, and whether the farmer can stop sharing the data.

This serves to raise awareness among both farmers and technology providers about the issues that concern farmers regarding the use of their data.

Inequality of bargaining power

Another concern raised by producers 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 producers 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 producers 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 producers. For example, producers 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* (discussed below) that was passed to regulate unfair terms in business-to-business contracts in 2016.

Addressing the digital data divide: Potential Impact of Small Business (Unfair Terms) Act 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 we see in agriculture, and the small businesses themselves. The ACL was amended to introduce and expand the unfair contracts term legislation to 'small businesses' that employ fewer than 20 persons. While there are some notable exceptions, many primary producers 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.

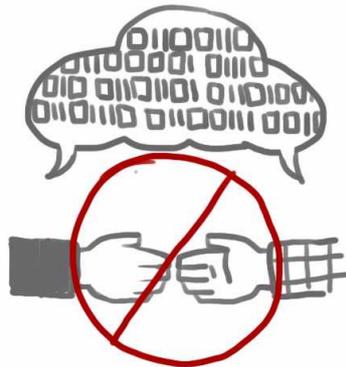
Put simply, 'transparency' means whether the term can be understood in reasonably plain language, is presented clearly, and is readily available to any party affected by the term.

As many of the terms in these 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 reforms. 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 producer, the test of 'unfairness' could arguably be satisfied. This is particularly the case when these terms are not made transparent to the producer prior to entry into the contract.

This reform to the Australian unfair terms regime does indicate 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.

Lack of benefit sharing between data aggregators and data contributors

Many producers are concerned that advisers or agri-businesses derive the greatest benefit from their data. While recognising the value added by the third-party aggregators, producers 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. Producers are concerned that businesses are making money from their data without sharing any of the benefits with the original data contributors.



Some 38 % of Australian producers are extremely concerned that businesses are making money from their data without sharing it with the producer.

While there were some examples of cooperative benchmarking exercises that returned benefits to member farmers, many producers expressed concern that the real value of sharing data was not yet being realised.

While improved knowledge, products and services is often said to be the real benefit of digital agriculture being returned to producers, many producers 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.

2.1.3 Proposed future reforms allowing for access to data

Australian Proposed Reform

On 8 May 2017, the Productivity Commission released its final report into data availability and use in Australia. If implemented in their current form, the 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 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.

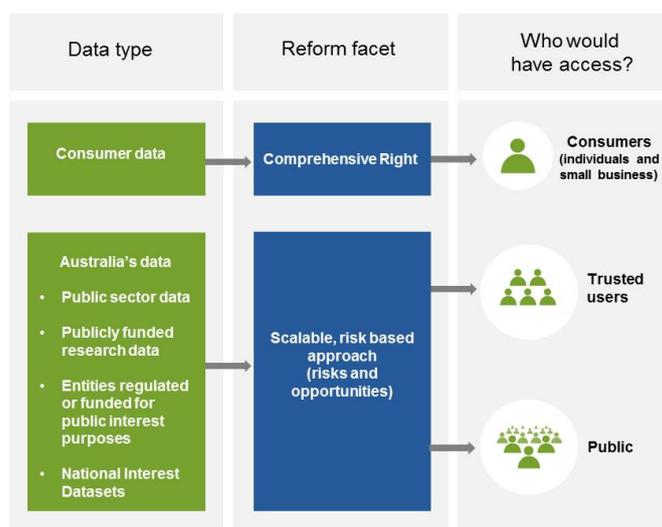


Figure 4: Framework for data access proposed by the Productivity Commission

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.

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.

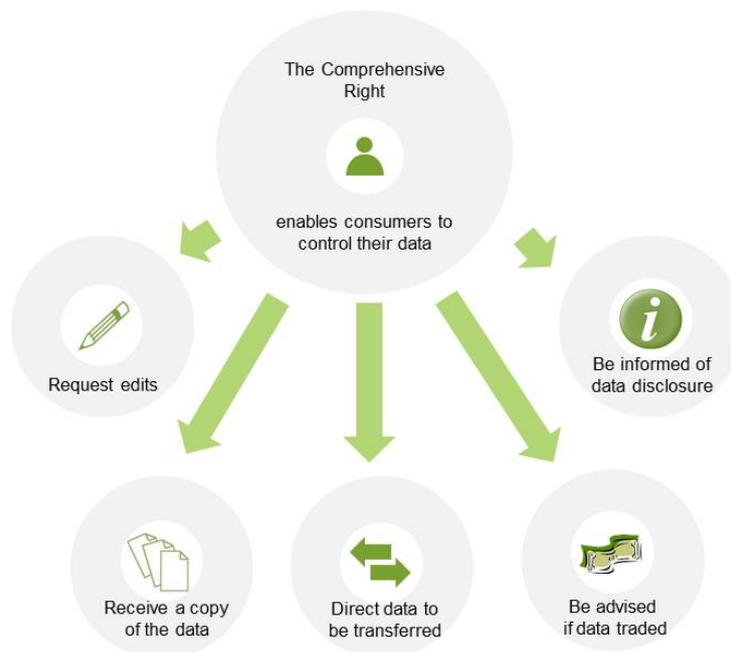


Figure 5: The comprehensive right for data access proposed by the Productivity Commission

At its broadest level, the Productivity Commission has indicated that consumer 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.

The Productivity Commission has envisaged a role for industry in determining what data will be consumer data. For example, data created by a data holder through the application of insights or analysis such that it cannot reasonably be considered the consumer's data should be included in consumer data *only* with industry negotiated agreement.

The creation of a data-sharing and release structure that indicates to all data custodians a strong and clear cultural shift towards better data use that can be dialled up for the sharing or release of higher-risk datasets

The Productivity Commission has proposed:

For datasets designated as national interest, all restrictions to access and use contained in a variety of national and state legislation, and other program-specific policies, would be replaced by new arrangements under the *Data Sharing and Release Act*. National Interest Datasets would be resourced by the Commonwealth as national assets.

A suite of Accredited Release Authorities (ARAs) would be sectoral hubs of expertise and enable the ongoing maintenance of, and streamlined access to, National Interest Datasets as well as to other datasets to be linked and shared or released.

A streamlining of ethics committee approval processes would provide more timely access to identifiable data for research and policy development purposes. (Productivity Commission, 2017 Key Findings)

While the Commonwealth Government intends to respond to the Productivity Commission's recommendations by the end of 2017, 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. Commenting on the Productivity Commission's recommendations, Mick Keogh, the Australian Farm Institute's Executive Director, stated:

Clearly, the agricultural sector has the potential to capture significant benefits from the rapid growth in digital technology, and the recommendations made by the Productivity Commission have established a very good framework for the sector to ensure that both productivity and competition benefits are secured. That said, there will need to be detailed discussions about these issues involving a wide cross-section of the industry to ensure that the potential benefits are able to be secured by as many as possible, and that decisions about data rights and access do not create impediments for technology and software developers (Keogh, 2017).

European Proposed Reform

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. 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. Legal developments of this sort are important for Australia to keep abreast of given the presence of internationally based agribusinesses in our market.

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.

Another interesting development is the right that Article 22 of the GDPR provides to persons not be subject to fully automated decisions based on profiling, when the decisions incur legal effects or similarly significant consequences.

The 2016 EU GDPR shows a very important change in 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.

2.1.4 International developments on agricultural data ownership and access

Legal issues arising from the volume of agricultural data that is being generated across the world have been the subject of much debate and examination in the international arena. It is useful here to highlight some of the international approaches being taken to these issues, as they provide a useful source of context and guidance for Australian agriculture.

It is helpful to begin by examining the open access movement that began over 25 years ago to provide open public access to publicly funded research, including agricultural research. Open access is defined as the free and unrestricted online availability of research and data. Open access is justified on the basis that the full social and economic benefits of agricultural research should be available to everyone who can use and build on the agricultural research to improve food security, and in turn society and people's lives.

Over the past decade, we have seen large funders of agricultural research (such as the UN body, the Consultative Group on International Agricultural Research (CGIAR, formerly the Consortium of International Agricultural Research Centres), the largest public good funder of agricultural research in developing nations in 2013, and the large philanthropic research funder the Bill and Melinda Gates Foundation in 2016, mandate that all funded research and its underlying data must be openly accessible.

Open access mandates have been adopted for publicly funded research in the United Kingdom, the United States and the European Union. For example, the greatest recent commitment made by the European Union to open access was part of its Horizon 2020, the biggest EU Research and Innovation program ever, with nearly €80 billion of funding available over seven years (2014–20); this opened access to the research and its underlying data funded through this program.

In Australia, the Commonwealth and state governments have followed suit. The most recent statement by the Australian Government is that all non-sensitive government data should be open by default, in line with Australian Government Public Data Policy Statement 2015. Non-sensitive data is data that does not identify individuals, reveal sensitive commercial information, or breach privacy or security requirements. Public data includes all data collected by government entities. This impacts on many of Australia's agricultural research funders.

Following the adoption and uptake of open access mandates, several initiatives have been created that are working towards implementing the open access mandates. One such initiative is Global Open Data for Agriculture and Nutrition (GODAN), which was created in 2013. GODAN supports the

proactive sharing of open data to make information about agriculture and nutrition available, accessible and usable to deal with the urgent challenge of ensuring world food security. It is a rapidly expanding group, currently with over 547 partners from national governments, non-governmental, international and private sector organisations that have made a commitment to opening access to agricultural data for the betterment of society. GODAN has developed a series of working papers on data ownership and data ecosystems (<http://www.godan.info/resources/research>).

Data: ‘as open as possible – as closed as necessary’

The consensus of many of the international organisations working towards opening access to publicly funded data is that data, as a general rule, should be ‘as open as possible – as closed as necessary’. This means that while publicly funded agricultural research should be made as open as possible, there is recognition that in some situations, privacy and intellectual property rights should be recognised as being valid reasons for non-disclosure of research and data.

We are seeing some of these international principles and approaches influencing Australian policy on data.

Australia is part of the Research Data Alliance (RDA), which was launched as a community-driven organisation in 2013 by the European Commission, the US Government's National Science Foundation and National Institute of Standards and Technology, and the Australian Government's Department of Innovation, with the goal of building the social and technical infrastructure to enable open sharing of data.

In 2016, the RDA released implementation guidelines on legal interoperability for open access. These guidelines address the legal complexities of open access, which are the work of the RDA-CODATA Legal Interoperability Interest Group. In September 2016, this group produced a set of principles and practical implementation guidelines on legal interoperability for open access.

The principles provide as follows:

1. Facilitate the lawful access to and reuse of research data,
2. Determine the rights to and responsibilities for the data,
3. Balance the legal interests,
4. State the rights transparently and clearly,
5. Promote the harmonization of rights in research data, and

6. Provide proper attribution and credit for research data.

Interestingly, these principles address some of the concerns that have been identified by producers in Australia in relation to the aggregation of their data.

Another important aspect of the Open Access Movement is the need to develop trustworthy data repositories. There are a large number of organisations working towards developing these, including the work of the Agricultural Information Management Standards (AIMS, <http://aims.fao.org/activity/blog/put-fair-principles-practice-and-enjoy-your-data>), which is implementing the work of Force 11, another community of scholars, librarians, archivists, publishers and research funders that has arisen organically to help facilitate the change towards improved knowledge creation and sharing. Force 11 has developed a general 'guide to FAIRness of data', the FAIR principles (i.e. that data must be Findable; Accessible; Interoperable; Reusable). It is accepted at the international level that it is not enough for research and data to be technically open; now the focus is on the need to ensure the interoperability of data so that the greatest benefit may be derived.

2.1.5 Key findings on data ownership, control and access

1. Many producers will own copyright in the datasets that they create, while many third parties will own copyright in the aggregated datasets. While Australian copyright law provides ownership rights to both producers and third parties in different situations, in practice, with digital agriculture, it is the contracts that are entered into between producers and third parties, such as advisers and agri-businesses, that will govern the ownership of their data, rather than copyright law.
2. Producers and their advisers and agri-businesses should note that mere payment for data services does not result in a transfer of data ownership, unless there is a contract that deals with data ownership.
3. A number of ag-technology providers encrypt their digital farming software. This restricts the ability of producers to access software that would inform them of the diagnostic and repair information of their farm machinery. This, in turn, prohibits producers from attempting to repair or modify their machinery.
4. Producers are unaware of the terms of data licences that they are entering. The general lack of discussion of the terms of the data licences at both a broad industry level and at individual points of sale of agricultural technologies contribute to the lack of trust about the management of agricultural data.
5. Agri-businesses that rely upon standard-form data licences should recognise that they have a

responsibility to ensure that their contractual terms are legible, transparent and fair, and they are readily available to contracting parties.

6. It is imperative that the terms of use that govern the aggregation, ownership, storage and dissemination of producers' agricultural data be made more transparent to producers prior to their entry into commercial relationships with third-party advisers and technology service providers. This is particularly the case where standard-form licences are used.
7. To support producers' continued willingness to supply their agronomic data to agri-businesses, producers need to see and be assured of the benefits that they are receiving in the form of improved goods and services or knowledge.
8. The Productivity Commission's *Final Report on Data Availability and Use* will, if implemented, have a fundamental impact on the way that agricultural data is managed in Australia. Open dialogue is needed between data contributors, data aggregators and industry stakeholders about the future management practices of data in the agricultural sector.
9. Open access to publicly funded research and its underlying data, including agricultural research, is now a well-entrenched mandate of governments around the world, and of public and private agricultural funders.
10. Australian agricultural industry must keep abreast of international developments in this field.

2.2 Data privacy, safety and security

One of the main concerns expressed by Australian producers is whether their data is private, safe and secure. During the P2D research workshop, participants consistently asked a range of questions around data privacy, safety and security, including:

- Should I trust the companies that have my data?
- Who is getting access to my data?
- How secure is my data? and
- Do I have privacy around my data?

In the P2D project survey, producers were asked about how much they trusted service/technology providers to maintain the privacy of their data. Results suggest that 32 % of respondents had no trust in providers maintaining privacy and only 6 % of producers completely trusted service/technology providers to maintain the privacy of their data (see Figure 6). Industries and sectors are not equally concerned with the privacy of their data, for example:

- the beef/grain mixed and poultry eggs/meat industries have the lowest trust in service/technology providers maintaining the privacy of their data
- the cotton industry has the most trust, and
- the remaining industries have little trust in providers maintaining their privacy.

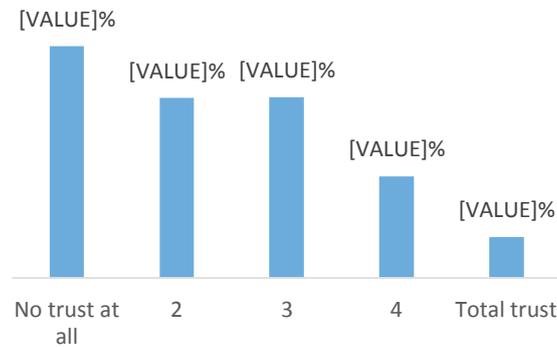


Figure 6: The extent to which producers trust service/technology providers to maintain the privacy of their data (n =895)

Addressing the concerns around the privacy, safety and security of data, this part of the report is divided into six sections:

- Distinguishing personal and non-personal data (2.2.1),
- Data that is ‘personal information’ (2.2.2),
- Personal information, the APPs and big data (2.2.3),
- Data and contracts (2.2.4),
- Other issues around privacy, security and safety (2.2.5), and
- Findings on data privacy, safety and security (2.2.6).

2.2.1 Distinguishing personal and non-personal data

Not all data is treated equally. While many Australian producers 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)

Generally, data such as agronomic (e.g. yield, nutrient, soil) and machine data (e.g. fuel consumption, engine performance) is not 'personal information' and is therefore not governed by the *Privacy Act 1988*. It is, instead, governed by the contract that producers enter with third-party providers.

So, when producers 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'. There are two main ways that govern the privacy of Australian producers' data.

1. **Australian Privacy Principles (APP) and associated privacy policies.** The Office of the Australian Information Commissioner has developed the draft *Guide to Big Data and the Australian Privacy Principles* to facilitate big data activities (see section 2.2.3) while protecting **personal information**. These apply to APP entities (e.g. private sector organisations, Australian Government and Norfolk Island agencies covered by the *Privacy Act*). The APPs apply to personal information. As noted above, this is data that can be used to identify a person, such as name and address. The APPs are available at: <https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>

In 2017, the *Privacy Act* was amended in relation to notification of breaches:

- Recognising that notification can limit damage, and can promote transparency and

trust, agencies and organisations governed by the *Privacy Act 1988* (Cth) **must** notify the Privacy Commissioner and affected customers ‘as soon as practicable’ after becoming aware that a data breach has occurred. Further, where an organisation suspects that a data breach has occurred, it is required to assess whether a breach has in fact occurred (see *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)), and

- There was also an attempt to criminalise the re-identification of de-identified personal information. Though, without the support of Labour and the Greens, this was Bill was not passed (see *Privacy Amendment (Re-identification Offence) Bill 2016*).

2. Contracts and licences. Other data such as agronomic data, machine data or weather and soil data tends not to be ‘personal information’. Therefore, it is not covered by the *Privacy Act 1988* and its APPs. This data and information are most commonly controlled by the contracts entered between producers, third parties and agri-businesses.

In the remainder of this part of the report, we provide an overview of how personal and non-personal data is governed.

2.2.2 Data that is ‘personal information’

Generally, the *Privacy Act 1988* and a RDC’s or company’s associated privacy policies and statements protect ‘personal information’. Therefore, producers must consider whether their data is ‘personal information’. As noted earlier, ‘personal information’ must be stored and used in accordance with the *Privacy Act 1988* and the APPs. ‘Personal information’ is defined to mean information about an identified individual, or an individual who is reasonably identifiable (*Privacy Act 1988*, section 6(1)).

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.

Rural Research and Development Corporations and many private agri-business companies (e.g. John Deere, New Holland and Case IH) 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.

2.2.3 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 producers’ 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 producer, their business and the agricultural data entity is vitally important.

2.2.4 Data and contracts

As noted above, data such as 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. During the P2D Project, many producers admitted to being unaware of the terms of their data contracts, and thus how their contracts dealt with the issue of data privacy and security (see section 2.1)

Some key terms of data licences that relate to the privacy, security and safety of data include:

- scope and limits on use of data,
- confidentiality and security of data,
- duration of the contract, and
- rights in relation to data on termination of the contract.

One strategy for facilitating transparent and fair data contracts is to encourage agricultural technology providers to engage in discussion around appropriate principles, policies and practices. An example of this comes from an 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.

More details about the American Farm Bureau Federation's Privacy and Security Principles for Farm Data can be found at: <http://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data>.

While the benefits of policy statements such as the AFBF's Privacy and Security Principles on Farm Data are widespread for both farmers and agri-businesses, they have also played a vital role in raising awareness among the agricultural sectors in many countries about the issues of data ownership, privacy and security of data; these must be addressed before the full benefits of digital agriculture can be realised.

2.2.5 Other issues around privacy, security and data

The P2D project also identified that some Australian producers are concerned about 'surveillance' and confidentiality around data. These concerns were particularly related to:

- data collection for monitoring, surveillance and compliance
- the use of imaging technologies such as drones (i.e. remotely piloted aircraft, RPA) and satellite imaging, and

- trade secrets and confidentiality.

Data collection for monitoring, surveillance and compliance

A range of monitoring and compliance systems exist that involve the collection of Australian producers' data. For example:

- Australian Fisheries Management Authority (AFMA) uses electronic monitoring (e-monitoring) to monitor fishing activities, which can be reviewed to verify what fishers report in their fishing logbooks, and allows AFMA to verify that fishers report all interactions they may have with threatened, endangered and protected species (see <http://www.afma.gov.au/monitoring-enforcement/electronic-monitoring-program>),
- The Australian Pork Industry has numerous regulatory and industry monitoring and reporting requirements related to biosecurity, food safety, farming practices, livestock traceability and chemical residue, and
- The Australian Sugar Industry has a voluntary 'best management practice' program (BMP) addressing concerns over the quality of water running from cane farms to the Great Barrier Reef. Sugarcane growers self-assess their practices to determine whether they are 'below', 'at' or 'above' the current industry standard. If their activities are below the industry standard, the system shows what they need to do to reach that standard.

Generally, these monitoring and compliance systems are required under regulation or industry frameworks, or are voluntarily agreed to. Some producers, however, are concerned that the data included in these monitoring and compliance systems can be released or used without their authorisation and consent. Importantly, and as noted above, any data that is 'personal information' is governed by the APPs and the RDC's or company's privacy policy or statement. For all other data, there may be legislation and/or contracts that stipulate whether and how the data can be used and shared. (See section 2.2.4 for a discussion of data and contracts.)

Another related issue that was raised by producers and workers in rural industries was the increasing use of surveillance and monitoring devices that might be included on digital agricultural machinery or technologies. These include a range of monitoring devices, such as:

- optical video (camera/video),
- tracking (e.g. Global Positioning System (GPS), and
- biometrics, particularly in respect of time and attendance (some involving the use of technology

to recognise people on the basis of innate physical characteristics).

The Australian Law Reform Commission has noted that, 'Workplace surveillance legislation is inconsistent across jurisdictions.' Workplace surveillance laws recognise that employers are justified in monitoring workplaces for the purposes of protecting property, monitoring employee performance or ensuring employee health and safety. However, the interests of employers must be balanced against employees' reasonable expectations of privacy in the workplace. Specific workplace surveillance laws (the workplace surveillance laws) exist only in New South Wales (*Workplace Surveillance Act 2005*), the Australian Capital Territory (*Workplace Privacy Act 2011*) and, to some extent, Victoria (*Surveillance Devices Act 1999 Pt 2A*) (see *Serious Invasions of Privacy in the Digital Era (DP 80)*, 2014).

While a detailed examination of the various laws on surveillance in the workplace is beyond the scope of this report, it should be noted that where surveillance and monitoring devices are in use on rural properties or rural businesses, employers or those using the devices should respect employees' reasonable expectations of privacy in the workplace. At the very least, employees should be made aware that such devices are in use in the business or on the rural property, and that in some states there are laws that govern the use of those devices.

Imaging technologies

Imaging technologies such as unmanned or remotely piloted aircraft can come in a range of shapes and sizes, such as small multi-rotor helicopters right up to large-winged aircraft that look and behave like aeroplanes. Drones or unmanned aerial vehicles (UAVs) are increasingly being used in agriculture, and can perform work that was previously dangerous, difficult or time-consuming. Data collected by sensors on surveillance technologies can be used for a multitude of purposes, and can provide multi-spectral imagery, show crop health and moisture content, accurately track the location of pipelines and power lines, detect crop stress or weeds, monitor land use or infrastructure and assist with property surveying and mapping (Cth House of Representatives, *Eyes in the Sky*, 2014).

There are various potential legal issues associated with the use of surveillance in agriculture, including safety risks to other aircraft, property, privacy or trade secrets. The main laws that govern UAVs are:

- CASA regulations,
- private nuisance,

- trespass to land, and
- trade secrets and confidentiality.

Civil Aviation Safety Authority (CASA)

The CASA Regulations stipulate that generally the use of drones above 2 kg in size require the user to have a remote piloted licence and operator's certificate. For example, activities could include aerial spotting, photography, spraying and carrying cargo. A private landowner or leaseholder can operate a medium-sized drone (between 25 and 150 kg), although a remote pilot licence is required for that size. Where the drone is being used on private or leasehold land, the regulations provide conditions of operation that need to be followed, including only operating during the day, up to 120 m, staying 30 m away from people and maintaining vision of the drone. Otherwise, a licence and clearance are required by CASA.

Private nuisance

If an interference with land is unreasonable and substantial, the tort of private nuisance might apply. A person wishing to sue in private nuisance must prove that they have an interest in or appropriate rights over the land at the time of the interference.

The key issue is whether the interference with the land is unreasonable. Factors that are taken into consideration are locality, duration, time and frequency, as well as whether there is some intent or malice on the part of the wrongdoer. The case law in this regard has generally been about loud noises, such as construction noise. Unless a drone or surveillance device was interfering with the landholder's daily activities, or creating substantial noise, private nuisance would be difficult to pursue.

Trespass to land

Trespass to land involves the direct and intentional or negligent interference with land in the exclusive possession of another without their consent or other lawful justification.

Air space constitutes land as far as it extends to a reasonable height as is necessary for the use and enjoyment of the land. However, a single or infrequent drone or surveillance flight over land is unlikely to constitute a trespass. What is likely to be required is persistent, noisy or low-flying interference, unless the interference is such that it is prohibiting the landholder's ordinary use of the land (i.e. neighbouring drones are interfering with the landholder's own drone activities or are disrupting livestock).

Trade secrets and confidentiality

Put simply, a trade secret is any secret commercial information that provides a business with an advantage. To be a trade secret, information must be used in trade or commerce, the owner of the information must limit its publication and, if disclosed to a competitor, it must have the potential to cause significant harm to the owner of the secret.

In determining whether information is secret, various factors are taken into account, including the extent to which the information is known outside of the business; the extent to which it is known by employees and others involved in the business; the extent of measures taken ... to guard the secrecy of the information; the value of the information; and the amount of effort or money expended ... in developing the information.

Surveillance laws

Laws at both the federal and state levels apply to surveillance devices, including audio, optical and visual devices; this would cover drones and other surveillance technologies. These laws are limited in their approach to Commonwealth and state agencies, and cover some organisations and corporations. In terms of private individuals using surveillance devices, these laws will not apply and the only recourse would be using the tort laws (e.g. private nuisance, trespass to land) discussed above, and possibly criminal law if the interference amounted to stalking.

Table 2: Key laws related to imaging technologies

Trade secrets and confidentiality

The question of whether data is a trade secret (or confidential information) is not just related to drones and other imaging technology. Trade secrets can relate to a broad range of information, including processes, methods and techniques (e.g. know-how on operating procedures), machines, plans, designs, customer lists and business information. As noted above, in determining whether information is secret, relevant factors include:

- the extent to which the information is known outside of the business,
- the extent to which it is known by employees and others involved in the business,
- the extent of measures taken to guard the secrecy of the information,
- the value of the information, and
- the amount of resources used to develop the information.

Trade secrets and confidentiality may be a consideration if employees change employers or when secret information is disclosed for a purpose (e.g. to obtain finance). In these instances, the use of contracts and non-disclosure clauses is important.

However, the law of trade secrets is unlikely to play a significant role in data. In its 2016 report, *The Implications of Digital Agriculture and Big Data for Australian Agriculture*, the Australian Farm Institute (AFI) concluded that:

It is probably reasonable to conclude that, except in very specific situations, it is highly unlikely that farm data would be considered to constitute a trade secret, and would therefore automatically be subject to project and confidentiality provisions on that basis. It is also worth noting that even in limited situations where this might be considered to apply, it would be likely that this protection would diminish over time if the information or the practice became more widely known or adopted. (AFI, 2016, p. 35)

2.2.6 Key findings on data privacy, safety and security

While Australian producers are concerned about the privacy, safety and security of their data, many of these concerns can be managed with appropriate data-management governance, policies and frameworks.

1. Australian producers are concerned about third parties gaining unauthorised access to their data. Their priority is to ensure that their data is kept private, safe and secure.
2. Not all data is treated equally, and under the *Privacy Act* a distinction is made between personal and non-personal information.
3. The current privacy policies used by businesses in digital agriculture tend to deal with personal information only. A consequence of this is that agricultural data, as it is generally not personal information, does not have the protections under *Privacy Act*. It is therefore vulnerable to unauthorised use unless protection is afforded by contract between the parties.
4. The absence of clear and consistent data governance within Australia's rural industries has the potential to expose Australian producers to threats to their privacy, security and safety of their agricultural data. This limits the potential benefits that can be derived from digital agriculture.

2.3 Data: Trust, transparency and certification

Trust is an essential component in the relationship between Australian producers and service providers. Australian producers want to know that their data is adequately protected and used fairly. Currently, however, many Australian producers do not trust service/technology providers with their data. Indeed, a lack of trust in the way data is treated was identified during the survey phase of the project, with 36 % of respondents having no trust whatsoever in service/technology providers not sharing their data with third parties (see Figure 7). Finally, throughout the workshops and discussions it was apparent that it was not all bad: with many producers talking about the positive and trusting relationships that they have with service providers, agronomists and others. And service providers were doing the right thing.

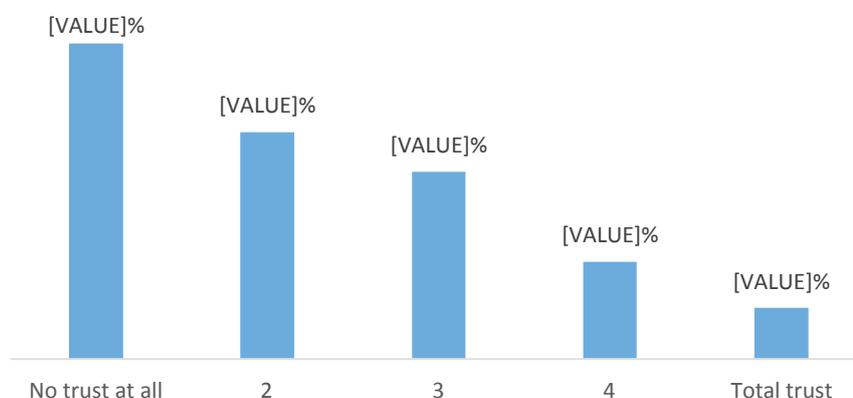


Figure 7: If the service/technology providers have direct access to your data, how much do you trust them not to share the data with third parties? – overall (n = 895)

Despite some positive and trusted relationships between producers and services providers, there is no denying that trust around data access and use is a major concern for Australian producers. A lack of trust is not unjustified, as there are examples of the challenges and misuses of data that have occurred. One example is the well-known data breach that occurred in 2014 where one of Monsanto's servers left exposed some customers' credit-card information and Monsanto employee data. More recently, in 2017, a class action was brought by a group of chicken farmers in the Oklahoma District Court against Tyson Foods Inc. (*Haff Poultry v Tyson et al.*) and other chicken processors for allegedly sharing production data (e.g. grower payments, broiler weights, type of feed and medicine used, and transportation costs) with third parties without the consent of chicken

farmers. Key issues for the chicken farmers were that the processors' data aggregation did not adequately anonymise the data and the data was unlawfully shared between the processors to reduce grower payments.

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. 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)

In addressing Australian producers' concerns over the way in which data is managed, this section of the report is divided into four parts:

- Contracts: Trust and transparency (2.3.1),
- Current attempts to develop trust around data practices, including the United States Ag Data Transparency Evaluator and New Zealand's Farm Data Code of Practice (2.3.2),
- Ag-Data co-operatives and other collaborative methods (2.3.3), and
- Findings on trust, transparency and certification around data (2.3.4).

2.3.1 Contracts: Trust and transparency

Building trusted relationships around agricultural data is critical to maintaining successful business relationships in digital agriculture (Newman and Briggeman, 2016). 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 producer's data.

Trust is more evident when parties are free to negotiate the terms of their commercial relationships themselves. Producers enter into many data contracts where they can negotiate the terms that govern the relationship. One example is the relationship between a producer and their adviser or agronomist. In these arrangements, best practice suggests that open dialogue between the service provider and the producer 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. 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. It should be noted that there are some advisers and agronomists who do encourage transparency and open dialogue about the management of the data they are collecting with their producers, however, this approach is neither widespread nor consistent across industries.

The situation is a little different when producers are presented with non-negotiable standard-form data contracts. These are most commonly used by larger agri-businesses. To develop trust between the producer and the technology supplier in these situations, the supplier should take steps to ensure the terms that govern the use of the data are transparent, as a lack of transparency can cause a significant imbalance in the parties' rights and obligations.

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.

While not every agri-business data licence may be subject to the ACL, the fact that 47 % of producers are unaware of the terms of the data licences that they enter points to the fact there is a long way to go before agri-businesses can claim that they are forthcoming about the way they manage and share producers' data.

To develop a *genuine* two-way street to support producers 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.

2.3.2 Current attempts to develop trust and transparency in data practices

While it takes time and resources to develop trust around data practices, it is important that producers feel comfortable that their data is being used in a fair and equitable way. Throughout the world, various initiatives have been taken to build trust and transparency with the aim of encouraging producers, industry, and research and commercial sectors to pursue certain objectives around ag-data. Importantly, many of these initiatives are not higher government regulation, nor do they rely directly on government regulation. While this might change in the future – particularly if the Productivity Commission's recommendations on data availability and use are adopted by the

Australian Government – any principles and standards around data use are up to the RDCs and/or industry. In this way, data principles and accompanying certification can be viewed as non-governmental market based initiatives and a form of “nudge”: helping producers make decisions by presenting options in particular (and simple) ways. According to the Thaler and Sunstein, a nudge is:

...any aspect of the choice architecture that alters people’s behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not. (Thaler and Sunstein, 2008: p. 6).

Certification is used in a wide range of fields (e.g. forestry, livestock, banking, agriculture and electrical goods), on a variety of products and services (e.g. food, financial and fridges) and to advance various goals and objectives (e.g. organic practices, labour conditions and sustainability). For data management, a certification scheme can indicate that the provider’s data practices comply with certain standards. Ag-data certification and labelling may reduce information asymmetry, and help transform a credence attribute (e.g. honest and transparent ag-data practices) into a visible attribute and therefore help consumers make an informed decision (Grolleau and Caswell, 2006). And in the process, improving transparency and trust in ag-data claims.

Globally, ag-data certification and labelling is being used to indicate to producers that service and technology providers meet certain data standards. In this section, we look at two of the most well-known attempts to develop transparency and trust in data use:

- Privacy and Security Principles for Farm Data, and Ag Data Transparency Evaluator, and
- Certification schemes, including New Zealand’s Farm Data Code of Practice (‘NZ Data Code’) and the United Kingdom’s proposed data quality certification mark.

Privacy and Security Principles for Farm Data and Ag Data Transparency Evaluator (United States)

As noted earlier in 2.2.4, established in 2014, the American Farm Bureau’s Privacy and Security Principles for Farm Data (‘Principles for Farm Data’) set out core principles around the agreement and disclosure, and aim to ensure that the ag-data is not misused. The voluntary *Principles for Farm Data* also provide companies that collect and analyse ag-data guidelines when constructing their contracts and technologies related to ag-data. The *Principles for Farm Data* set out thirteen key areas: (i) education; (ii) ownership; (iii) collection, access and control; (iv) notice; (v) transparency

and consistency; (vi) choice; (vii) portability; (viii) terms and definitions; (ix) disclosure, use and sale limitation; (x) data retention and availability; (xi) contract termination; (xii) unlawful or anti-competitive activities; and (xiii) liability and security safeguards (see <https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data>)

Based on the *Principles for Farm Data*, in 2016, the Ag Data Transparency Evaluator was launched. The Ag Data Transparency Evaluator is a tool designed to help US farmers understand how their data will be used when they adopt precision agriculture technologies. The tool was created by the American Farm Bureau Federation and backed by a consortium of farm industry groups, commodity organizations and ag technology providers to bring transparency, simplicity and trust into the contracts that govern precision agricultural technologies (Ag Data Transparent, FAQ).

Based upon the foundation laid by the American Farm Bureau Federation's Privacy and Security Principles for Farm Data (the Data Principles), the **Ag Data Transparency Evaluator** is a process by which ag technology providers voluntarily submit their data contracts to a simple 10-question evaluation. These questions are directed at discovering the approach taken by the technology providers to data management.

Answers are reviewed by an independent third-party administrator, the law firm of Janzen Agricultural Law LLC, with Todd Janzen as the administrator of the project. Once reviewed, the results are posted on the website for farmers and other ag professionals to consult and review. Only companies receiving approval can use the 'Ag Data Transparent' seal (see <http://www.agdatatransparent.com/ag-data-10-questions>). This approach is said to develop trust in the agricultural technology providers who are approved to use the seal.

This seal then serves to inform farmers whether the approach taken by the technology provider is in line with the American Farm Bureau's Data Principles. These principles include ideas around education; ownership; collection, access and control; notice; transparency and consistency; choice; portability; terms and definitions; disclosure, use and sale limitations; data retention and availability; contract termination; unlawful or anti-competitive activities; and liability and security safeguards.

The ability to use the seal indicating that the business is Ag Data Transparent provides an incentive for the agricultural technology providers to review and improve their contractual terms in light of the Data Principles.

The Ag Data Transparency Evaluator is provided free of charge to farmers to view, so they can make an informed decision about the data approaches taken by the businesses with which they choose to

deal. The cost of the Ag Data Transparency Evaluator is borne by the technology providers who want to use the Ag Data Transparent Seal. The cost is based first on the age of the company, and then on the size and profit that they make. For example:

- Start-up provider (a participant operating for less than four years): \$2,000.
- Regular provider (a participant that is not a start-up provider or large provider): \$4,000.
- Large provider (a participant with annual sales greater than \$100 million): \$6,000 (Ag Data Transparent, FAQ).

Currently, the approved companies are filtered by the type of data they collect: agronomic, land, farm management, machine and weather data. As at June 2017, there are eight companies and their products that have been evaluated and granted approval to use the Ag Data Transparent Seal. For each service, the business's profile is neatly laid out and has clear 'yes' or 'no' answers for the questions with further detail then provided. It is simpler for a farmer to glance at this service than to try to read and understand the companies' terms and conditions. This tool allows companies that are embracing the principles of openness and transparency in data licensing to show their prospective customers that they are reliable and trustworthy, as outlined in the Data Principles.

One of the main ways to indicate compliance with data standards is via labelling and the use of trade and certification marks.

Certification of data practices

A common feature of good governance of data practices is the demonstration of its effectiveness and quality to users, funders and the community. Accreditation or certification of ag-data practices is increasingly seen as an approach to ensuring data standards in agriculture. Put simply, by certifying their ag-data practices providers guarantee that their data-management practices adhere to the criteria set out by the accrediting body. This provides an opportunity for differentiation and a way to valorise the service or technology. These standards often ensure open and transparent data practices, particularly around:

- data collection, processing and sharing, and
- data storage and security.

A data certification scheme can enhance trust because producers are assured that an independent and objective party has evaluated the 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 producers verify the 'responsible' nature of the services and technologies they purchase (Bartiaux, 2008).

For example, companies receiving approval from the United States Ag Data Transparency Evaluator can use the 'Ag Data Transparent' seal (see Figure 8). The use of the seal is said to develop trust in the mind of the producers, who then have confidence in the agricultural technology providers approved to use the seal.



Figure 8: The US Ag Data Transparent Mark (permission to reproduce provided on 10 November 2017)

Data certification schemes may also benefit rural industries more generally. Highlighting the perceived and actual benefits of certification for business, the International Accreditation Forum conducted an empirical study into the benefits of certification, finding that 83 % of businesses felt that certification added value to their organisation; 17 % found a 'significant increase' in sales as a 'direct result' of certification; 32 % indicated a 'minor rise' in sales; and 16 % regarded it as important to 'direct customers' (International Accreditation Forum, 2012).

New Zealand Farm Data Code of Practice, Standards and Accreditation

Another example of a data certification scheme is the New Zealand Farm Data Code of Practice ('*NZ Farm Data Code*'), with complimentary standards and accreditation. The *NZ Farm Data Code* was established in 2014 to 'set of guidelines enabling effective sharing of data within the New Zealand agriculture industry' (Farm Data Code of Practice, Version 1.1: p. 4). The *NZ Farm Data Code* targets providers that manage farm data for agri-businesses in New Zealand, and focuses on disclosure with compliant organisations agreeing to:

make disclosures to primary producers and other end users about the rights that the parties have in the data, rules and processes for data sharing, about data security and the legal jurisdiction in which data is kept, and

implement a set of practices that provide primary producers with confidence that data pertaining to their farming operations is secure, managed according to agreed terms and for agreed purposes, and accessible under appropriate terms and conditions.

In June 2014, when the *NZ Farm Data Code* was launched, six industry organisations provided the mandate for its establishment (Beef + Lamb New Zealand; Dairy New Zealand; Dairy Companies Association of New Zealand; Federated Farmers New Zealand; Te Tumu Paeroa: The New Maori Trustee; and the New Zealand Veterinary Association). The *NZ Farm Data Code* targets providers that manage farm data for agri-businesses in New Zealand.

The *NZ Farm Data Code* requires organisations to outline the steps they take to safeguard farmer data. Under the *NZ Farm Data Code*, organisations agree to disclose their practices and policies around data rights, data processing and sharing, and data storage and security. By so doing, it is felt that farmers will have more trust and confidence that farm data is safe and is managed fairly. It is important to note that the scope of the *NZ Farm Data Code* extends to all farm data, which is recognised under the scheme to include non-personal information as well as personal information.

An ag-provider that complies with the Code's standards is authorised to display the Code of Practice mark on its website and documents. One of the ways in which compliance with these standards is communicated to consumers is by registering a word, words or image as a trade mark. For example, the *NZ Farm Data Code* seal is registered with the NZ Intellectual Property Office as a trade mark (IP Number 101886, accepted 21 May 2015) (see Figure 9).



Figure 9: The New Zealand Data Code Mark (permission to reproduce provided on 9 November 2017).

Accreditation of the *NZ Farm Data Code* is essential a form of self-regulation in which companies conduct a 'self-audit' and statutory declaration to confirm that they comply with the *NZ Farm Data Code*. Once companies have done this, their application is assessed and, if approved, they will receive an annual licence and certificate as well as the Farm Data Code of Practice trade mark to use. Then, if approved the companies receive an annual licence and certificate (see http://www.farmdatacode.org.nz/?page_id=20). So far, five ag-providers (i.e. Gateway Data

Services, Farmax, Farm IQ, Greenlea and apps on farm) have been accredited, and thus can display the Code's mark.

In addition to the *NZ Farm Data Code*, a set of technical NZ Farm Data Standards have been developed; with the hope of assisting data sharing across the dairy sector. These standards provide a 'a set of common data vocabularies that assist the business and industry organisations that serve NZ farmers to develop efficient technology applications and integrations' (see <http://www.farmdatastandards.org.nz/>). So far, there are standards for animal data; land application data; financial data; irrigation and effluent data; stock reconciliation data; farm features and attributes data; pasture, grazing and feed data; farm and model data; and health and safety data (see <http://www.farmdatastandards.org.nz/data-standards/>). New standards will be developed depending on industry need.

The United Kingdom's proposed data quality certification mark

Yet another example of certification of data practices comes from the United Kingdom. In January 2013, the UK Government introduced a Fair Data accreditation scheme. Based on 10 Fair Data Principles, companies can be accredited to show that they handle their customers' personal data fairly (see <http://www.fairdata.org.uk>). In addition to this, in 2016 a quality assurance scheme was proposed based on EU standards for dealing with personal data. The proposed voluntary scheme will allow 'sector-specific, third-party operators to evaluate the legal and ethical dimensions of how companies handle personal data' (Koene, 2016). Once the scheme is established, companies will be able to apply to have their data-handling procedures certified under the proposed quality certification scheme. To help communicate data certification to consumers and develop trust, various trade marks are being devised to communicate to consumers the different levels of control and protection over data provided.

Opportunities and challenges of data certification

Data certification such as the *NZ Data Farm Code* and US Ag Data Transparent seal provide an opportunity to develop transparency and trust around data uses. They also provide a chance to develop and implement standards around data-management practices. As noted above, certification is used in a wide range of fields (e.g. forestry, livestock, banking, agriculture and electrical goods), on a variety of products and services (e.g. food, financial and fridges) and to advance various goals and

objectives (e.g. organic practices, labour conditions and sustainability). In this vein, it is hoped that a certification mark for ag-providers would increase transparency and trust between producers and 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. 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 producers. 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 producer or agri-business demand. To date, only eight companies and their products have been evaluated and granted approval to use the Ag Data Transparent Seal and five companies have been accredited to use the NZ Farm Data Code mark.

In the following paragraphs, we briefly outline some of the key challenges of registering a data mark in Australia.

The need for appropriate and dynamic data standards and licensing arrangements

One of the most important aspects of an effective data certification scheme is establishing appropriate standards and licensing arrangements. Indeed, ag-data standards and certification are only as good as the standards and licensing arrangements that goes into them. This means that organisations and groups concerned with encouraging certain data practices need to identify and target the most important practices and policies around data rights, data processing, data sharing, and data storage and security. The US Ag Data Transparency Evaluator, for example, has standards around education; ownership; collection, access and control; notice; transparency and consistency; choice; portability; terms and definitions; disclosure, use and sale limitations; data retention and availability; contract termination; unlawful or anti-competitive activities; and liability and security safeguards.

Importantly, a data certification scheme could provide standards that are informed by the Australian privacy and data law principles (e.g. APPs) (see section 2.2). In other words, providers accredited under a data certification scheme could be required to guarantee that all their data practices are compliant with the principles (or similar principles) that underlie the APPs. This would be likely to enable an agri-business to place more trust in the provider responsible for managing its farm data.

The reason for this is that the provider's practices are approved under an objective scheme that mimics the position at law. Importantly, too, the certification standards could apply to both personal and non-personal information.

Independent third-party certification (versus self-declaration)

A key feature of good governance of data management is the demonstration of its quality to producers, industry and agribusiness. Not all certification is treated equal, nor does all certification build trust in the same way. One of the main ways of building trust and confidence in ag-data certification is through an independent third-party certification process. Third-party certification is generally recognised around the world as the highest and most credible type a certification or accreditation (Albersmeier et al, 2010). Indeed, the literature on certification indicates that self-declarations are less credible (D'Souza et al, 2007).

A big part of the advantage of independent third-party accreditation is that neutrality gives producers greater assurance and confidence in the process. It is felt that independent third-party schemes are less open to manipulation and deception.

That said, independence is not the only factor when developing a certification or accreditation scheme. Trust in certification will also depend on whether the ag-data certification clearly conveys 'good' data standards. Therefore, educating producers to help them understand ag-data standards and certification is essential. It is also important to design a logo (and message) that will capture producer and agribusiness attention.

Independent third-party certification may not always be possible or feasible. Therefore, independence must be weighed against other resources (e.g. finances). Importantly, too, research suggests that independence is merely one factor to be considered (Dekhili and Achabou, 2014)), and it is possible that ag-data certification can have a positive effect on producers regardless of whether it is independently certified or certified via self-declaration.

Registering a data trade or certification mark

When considering whether to register and use a data mark, it is important to realise that in Australia, under the *Trade Marks Act 1995* (Cth), there is a difference between a trade mark and certification mark. Key differences between a trade and certification mark include:

- **Registering an ag-data standard trade mark will provide more flexibility and be less onerous than a certification mark:**

When considering whether to register and use an ag-data logo here is a difference between a trade mark and certification mark. The procedures for registering a data certification mark are more demanding than those for a standard trade mark. While the grant of a standard trade mark generally is based on an examination by the Australian Trade marks Office of requirements centred on distinctiveness, and potential confusion and deceptiveness, the examination of certification marks consists of an additional distinct stage: the examination of the rules, standards or criteria that govern the use of the certification mark. These matters are examined by the Australian Competition and Consumer Commission (ACCC). In Australia, approval from the ACCC is required before certification marks can be registered under the *Trade Marks Act 1995* (Cth). Once established, any changes to the standards must also be approved by the ACCC.

- **Certification marks tend to be non-discriminatory, so there is greater discretion about who can use a data mark if it is registered as a standard trade mark.**

It is possible that a certified business might satisfy the standards related to a data mark, but may more broadly damage the credibility of data certification. The reason for this is that it is difficult, if not impossible, to refuse to license a certification mark to a company that has complied with the approved standards of the certification. In Australia, for example, the peculiar situation occurred when the National Heart Foundation Tick, which is registered as a certification mark, was awarded to certain approved McDonald's meals.

This would not be the case with a standard data trade mark, as it would be the owner (or the licensee) of the trade mark that would have the discretion to approve or deny the granting of the licence.

Finally, a word of caution. While there are different reasons for introducing an Australian data certification scheme, it is first necessary to have a clearly articulated set of goals and objectives. Without this, it will be difficult if not impossible to develop appropriate standards and processes of certification. Similarly, without specific goals and objectives it will be impossible to evaluate the effectiveness of such schemes and to conduct any meaningful review of the schemes once they are introduced. Further, if an ag-data scheme is introduced—and is to provide an instrument to promote good data management— then RDCs and industry must work hard to convince producers and agribusinesses that the standards and associated certification represent value. Currently, it appears that there is little incentive for agribusiness to seek certification and accreditation. That said, as Australian producers and agribusiness 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.

2.3.3 Ag-Data co-operatives and other collaborative initiatives

Other attempts to manage data and build trust and transparency include the establishment of data co-operatives and other collaborative models. In this part of the Report we consider ag-data co-operatives.

Ag-Data Co-operatives: A collaborative approach to collecting, using and sharing ag-data

Established in the 1800s, one of the first influential co-operatives was the Rochdale Society of Equitable Pioneers: a co-operative of cotton mill weavers aimed at providing food and other goods at affordable prices (Restakis, 2010). Since the 1800s, co-operatives have been used in a wide range of fields including wholesale, retail, finance and agriculture.

What is a co-operative? Put simply, a co-operative is a legal entity owned and run by and for its members. Co-operatives are defined by the International Co-operative Alliance (ICA) as: "...an autonomous association of persons united voluntarily to meet their common economic, social and cultural needs and aspirations through a jointly-owned and democratically-controlled enterprise" (ICA, 2012). Co-operatives can take a variety of forms and legal structures such as:

- distributing co-operatives (formed to carry out commercial ventures where members can share in profits), and
- non-distributing co-operatives (often "not-for-profit" organisations, which are prohibited from distributing surplus funds to members from profits).

At the heart of co-operatives, however, is collaboration and people with common interests banding together. Co-operatives are generally member-owned and member-controlled, and distribute benefits equitably to their members (Barton, 1989). Often, they are formed when it is felt that the market fails to provide the needed goods and services. Significantly, co-operatives are not new to agriculture and are seen in a range of sectors including dairy, grains and wine.

Why ag-data co-operatives? In terms of ag-data, co-operatives provide a means by which collaborative effort can be harnessed to serve producers, producer organisations and other organisations to create collaboration around ag-data collection, storage and use.

Before looking at some specific examples and challenges of ag-data co-operatives it is helpful to provide some background on their legal and regulatory frameworks including:

- international co-operative principles, and
- the introduction of a National Co-operatives Law in Australia.

International Co-operative Principles

Generally, co-operatives are bound by a common set of principles established by the International Co-operative Alliance (ICA), which are like those expressed by the Rochdale Society of Equitable Pioneers in the 1800s (ICA, 2017). The principles are:

1. **Voluntary and Open Membership:** Co-operatives are voluntary organisations, open to all persons able to use their services and willing to accept the responsibilities of membership.
2. **Democratic Member Control:** Co-operatives are democratic organisations controlled by their members, who actively participate in setting their policies and making decisions.
3. **Member Economic Participation:** Members contribute equitably to, and democratically control, the capital of their cooperative.
4. **Autonomy and Independence:** Co-operatives are autonomous, self-help organisations controlled by their members.
5. **Education, Training and Information:** Co-operatives provide education and training for their members and others so they can contribute effectively to the development of their co-operatives.
6. **Co-operation among Co-operatives:** Co-operatives serve their members most effectively and strengthen the co-operative movement by working together through local, national, regional and international structures.
7. **Concern for Community:** Co-operatives work for the sustainable development of their communities through policies approved by their members.

For further details on these principles see the International Co-operative Alliance website (<https://ica.coop/>).

A National Co-operatives Law (CNL)

Informed by the ICA Principles discussed above, a uniform set of national laws for co-operatives has been introduced by the Australian States and Territories (except Queensland). This has been achieved by each State and Territory: either by adopting the template Co-operatives National Law

(CNL) or passing alternative legislation consistent with the CNL (See Table 3). The CNL aims to harmonise co-operative law in Australia and to, for example, provide for national registration. The CNL has created a two-tiered system—small and large co-operatives—to allow for more appropriate financial reporting. Importantly, under the CNL a co-operative that is legally registered in one jurisdiction can now operate on a national basis without the need for any further registration or reporting requirements in each State.

Therefore, before deciding to form an ag-data co-operative, it is essential to understand and comply with the requirements set out in the relevant State and Territory law (see Table 3). These laws set out the requirements around:

- Types of co-operatives,
- Formation of co-operatives (including establishing the co-operatives registered rules, primary activities and financial involvement of members),
- Legal capacity of co-operatives,
- Membership of co-operatives,
- Governance and management of co-operatives, and
- Legal and other responsibilities that a co-operative must follow once registered.

Ag-Data Co-operatives

As noted earlier, co-operatives are not new to agriculture and they have been used in dairy, fishing, fruit and vegetable, sugar and grains to pool and share resources. Acknowledging the importance of farming co-operatives, in 2016, the Australian Government invested \$14,934,000 into a project on farm co-operatives and collaboration called *Farming Together*. The aim of which is to provide farmers with knowledge, skills and materials on collaborative ideas, co-operative structures and collective strategies. For more details on the *Farming Together* project see <https://agworks.com.au/>.

An ag-data cooperative is an organisation that is owned and controlled by its members for their mutual benefit; generally, control comes via membership. One of the projects funded by *Farming Together* involves a data co-operative being established by the Birchip Cropping Group (BCG) (Farming Together, 2016). Established in 1992, the BCG is a Victorian farmer (from the Wimmera and Mallee regions) not-for-profit agricultural research and extension organisation. Set up to focus on the adoption of new technology and practices, the BCG has turned its attention to data, particularly a data co-operative. Chris Sounness, CEO of the BCG, believes in the power of a data co-operative and says that big data drawn from farm operations is a commodity worth collecting, and a co-op

could be the structure to store it (see <https://agworks.com.au/birchip-cropping-group/>). At this stage, approximately 40 member-farmers have installed weather stations whose data will be collected and shared.

Other examples of ag-data co-operatives come from overseas, most notably the United States. Here, it is important to again point out that ag-data co-operatives come in different shapes and sizes: many of which can be considered hybrids, in that they are not 100 percent producer run and sometimes include involvement and/or investment from agribusiness. Some United States ag-data co-operatives or collaborative approaches to data include:

- **The Agricultural Data Coalition (ADC):** A non-profit organisation established to connect ‘the data dots across food & agriculture’ and that aims to give farmers the ability to control their data and share it with those they want. The ADC seeks to help farmers control and manage their data, and do so primarily through the provision of a ‘safe and secure’ data repository. See <http://agdatacoalition.org/>
- **The Grower Information Services Cooperative (GiSC):** a grower run data co-operative that aims to ‘free data from proprietary silos to bring the big data opportunity to every farmer in the US. GiSC attempts to do this by linking growers, data partners, technology companies and data consumers. See <https://www.gisc.coop/>
- **Winfield Data Silo:** established by a collaboration between WinField and Google Cloud Platform, the Winfield Data Silo is a data management tool that lets farmers store and share data, particularly with agronomists and using propriety tools and applications.
- **AgGateway:** is a ‘a non-profit consortium of businesses serving the agriculture industry, with the mission to promote, enable and expand eBusiness in agriculture’. At the time of writing, AgGateway has more than 230-member companies working. See <http://www.aggateway.org/>

There is also some discussion of ag-data co-operatives in the Australian Farm Institute (AFI) P2D Report, which is available at <http://farminstitute.org.au/p2dproject>.

Key features of ag-data co-operatives

Ag-data co-operatives must be established in accordance with the CNL noted above, and be registered with the relevant body (e.g. in the ACT, Access Canberra; in NSW, NSW Fair Trading; in VIC, Consumer Affairs Victoria; and in QLD, Fair Trading). More specifically focus should be on establishing an ag-data co-operative that:

- Is owned and democratically managed by their members, and not be external investors,

- Exists to serve their members,
- Benefits its members,
- Is motivated by providing a service, not by profit,
- Has clear objectives such as pursuing a common need and opportunity, and increasing bargaining power, and
- Utilises the legal advantages of being a co-operative such as members have limited liability; registration is inexpensive.

Key questions for ag-data co-operatives

There are several important questions for those looking to establish an ag-data co-operative including:

- What are the aims and purpose of the ag-data co-operative?
- What is the advantage of an ag-data-cooperative?
- Do you have the skill and expertise to form and manage an ag-data co-operative?
- Are there any conflicting interests (e.g. overlapping or conflicting responsibilities) that need to be eliminated or reduced?
- Are there adequate resources (including finances) to ensure the data co-operative can succeed in the marketplace, and compete against other organisations?
- What is the best way to facilitate participation and trust in the ag-data co-operative? For example: the way in which a data co-operative defines membership and develop its rules will affect trust, and
- How can adequate supply chain management be established to best facilitate upstream and downstream linkages?

Finally, more research needs to be done to assess the impact and effectiveness of ag-data co-operatives. It is important that Australian industries or individuals do not blindly follow what is happening elsewhere (e.g. in the United States). Indeed, it is difficult to distinguish the ag-data co-operative marketing and hype from their substance and effectiveness. While it is hard to argue with the aims and ideals of data co-operatives (e.g. the pooling of farmer ag-data for their benefit) the devil is in the detail, particularly around: ag-data co-operative rules and formation; the difficulty of attracting and retaining members and/or investment; and how, and with whom, the data will be shared.

Table 3. Australian State and Territory Co-Operative Legislation

State/Territory	Key Laws
NSW	<i>Co-operatives (Adoption of National Law) Act 2012</i> , and <i>Co-operatives National Law (NSW) (CNL)</i> . See, http://www.fairtrading.nsw.gov.au/ftw/Cooperatives_and_associations/About_cooperatives.page
ACT	<i>Co-operatives National Law Act 2017</i> . See, https://www.accesscanberra.act.gov.au/app/answers/detail/a_id/2102/~/~co-operative-registration
VIC	<i>Co-operatives National Law (CNL) 2014</i> . See, https://www.consumer.vic.gov.au/licensing-and-registration/co-operatives
QLD	<i>Queensland Cooperatives Act 1997</i> . See, https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/associations-charities-and-non-for-profits/cooperatives
WA	<i>Co-operatives Amendment Act 2016</i> . See, https://www.commerce.wa.gov.au/consumer-protection/co-operatives
NT	<i>Co-Operatives (National Uniform Legislation) Act 2016</i> . See, https://nt.gov.au/industry/licences/cooperatives
SA	<i>Co-operatives National Law (South Australia) Act 2013</i> . See, https://www.sa.gov.au/topics/family-and-community/community-organisations/types/co-operatives
TAS	<i>Co-operatives National Law (Tasmania) Act 2015</i> . See, http://www.consumer.tas.gov.au/registrations/co-operatives

2.3.4 Findings on trust, transparency and certification

Without question, there is a demand for increased transparency, disclosure and trust between data providers and Australian producers. Importantly, organisations and companies that can convince producers that their data will be used fairly and honestly will be more likely to benefit from new opportunities arising from emerging digital technologies and data. In this section of the report, we have considered numerous issues and initiatives around trust and transparency of data. On this basis, we make the following findings:

1. Many Australian producers lack trust in service and technology providers when collecting and sharing their data.
2. In Australia, there are no governing principles that clarify and build trust in producers around the access and use of agricultural data. An absence of appropriate and dynamic ag-data standards and licensing arrangements contributes to the lack of trust producers have towards data contracts.
3. There is an urgent need for a genuine two-way relationship between agri-businesses and Australian producers. This will facilitate a willingness to supply and share agricultural data. To achieve this, third parties and agri-businesses should ensure that their terms governing data are more transparent and available, and that this is clearly communicated to producers.
4. Globally, ag-data certification and labelling is being used to indicate to producers that service and technology providers meet certain data standards. For example: in the United States (with the Ag Data Transparency Evaluator) and New Zealand (with the NZ Farm Data Code). While the process by which third parties' data licences are certified can instill confidence and trust in producers the evidence on this is unclear.
5. A trade or certification mark can be used to develop and communicate certain standards around data practices. A data certification scheme can involve a registered trade or certification mark; registering a standard trade mark provides more flexibility and is less onerous than registering a certification mark.
6. While there are different reasons for introducing an Australian ag-data certification scheme, it is first necessary to have a clearly articulated set of goals and objectives. Without this, it will be difficult if not impossible to develop appropriate standards and processes of certification. Similarly, without specific goals and objectives it will be impossible to evaluate the effectiveness of such schemes and to conduct any meaningful review of the schemes once they are introduced. Further, if an ag-data scheme is introduced—and is to provide an instrument to promote good data management—then RDCs and industry must work hard to convince producers and agribusinesses that the

standards and associated certification represent value.

7. Other collaborative models, including data cooperatives, have been used to manage ag-data access and use. More research needs to be done to assess the impact and effectiveness of ag-data co-operatives. It is important that Australian industries or individuals do not blindly follow what is happening elsewhere (e.g. in the United States). Indeed, it is difficult to distinguish the ag-data co-operative marketing and hype from their substance and effectiveness. While it is hard to argue with the aims and ideals of data co-operatives (e.g. the pooling of farmer ag-data for their benefit) the devil is in the detail, particularly around: ag-data co-operative rules and formation; the difficulty of attracting and retaining members and/or investment; and how, and with whom, the data will be shared.

References and Further Reading

- ABC News (2016) "CASA develops new regulations for drone operation".
<http://www.abc.net.au/news/rural/2016-04-01/new-drone-regulations-to-benefit-farmers/7293392>.
- ABC News (2016) "Drones could be the answer to early disease detection in banana crops".
<http://www.abc.net.au/news/rural/2016-07-18/drones-may-detect-banana-disease/7637312>.
- Ad Exchanger (2015) "Adroit: 'Data Co-Ops Try to Answer The Question: What If You Knew More?'" <https://adexchanger.com/data-exchanges/adroit-data-co-ops-try-to-answer-the-question-what-if-you-knew-more/>.
- Ad Week (2016) "Adobe Is Creating a Data Co-Op to Compete with Google and Facebook".
<http://www.adweek.com/digital/adobe-creating-data-co-op-compete-google-and-facebook-170347/>.
- Adam, B., et al. (2016) "Enhancing Food Safety, Product Quality, and Value-Added in Food Supply Chains Using Whole-Chain Traceability". *International Food and Agribusiness Management Review*, 19(A): 191–213.
- Ahearn, M. Armbruster, W and Young, R. (2016) "Big Data's Potential to Improve Food Supply Chain Environmental Sustainability and Food Safety". *International Food and Agribusiness Management Review*, 19(A): 155-172.
- Aims (2016) "Put Fair Principles Into Practice and Enjoy Your Data".
<http://aims.fao.org/activity/blog/put-fair-principles-practice-and-enjoy-your-data>.
- 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.
- Alexander, C., et al. (2009) *Serving Producers in Volatile Times* (Working Paper no 09-09, Department of Agricultural Economics, Purdue University).
https://www.researchgate.net/publication/46468678_Serving_Producers_In_Volatile_Times_Report_From_The_2008_Large_Commercial_Producer_Survey
- 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>.
- Anderson, L. (2015) "The sky's the Limit: UAS regulation and changing applications in agriculture". *Kentucky Journal of Equine, Agriculture, and Natural Resources Law*, 8(2): 401.
- Antle, J, Capalbo, S and Houston, L. (2015) "Using Big Data to Evaluate Agro-Environmental Policies". *Choices*, 30(3): 1-8.
- Asphalt and Rubber (2016) "It's Legal To Hack Your Motorcycle for the Next Two Years".
<http://www.asphaltandrubber.com/news/legal-hack-motorcycle-code/>.

- Asphalt and Rubber (2017) "OEMs Are Trying to Block "Right to Repair" Laws". <http://www.asphaltandrubber.com/oped/mic-blocking-right-to-repair-laws/>.
- Australian Automotive Aftermarket Association (2015) "Defending the Repair Defense". <https://www.aaaa.com.au/advocacy/defending-the-repair-defense/>.
- Australian Farm Institute (2016) *The Implications of Digital Agriculture and Big Data for Australian Agriculture*, Research Report. <http://www.crdc.com.au/publications/implications-digital-agriculture-and-big-data-australian-agriculture>
- Australian Government (2015) "Australian Data Policy Statement". <https://www.pmc.gov.au/public-data/public-data-policy>
- Australian Law Reform Commission (2014) "Serious Invasions of Privacy in the Digital Era". March 2014 (Discussion Paper).
- Auto Service World (2010) "Right to Repair Agreement Arrives on Time". <http://www.autoserviceworld.com/jobbernews/right-to-repair-agreement-arrives-on-time/>.
- Auto Service World (2017) "Is the Right to Repair Agreement in Canada Working?" <http://www.autoserviceworld.com/carsmagazine/is-the-right-to-repair-agreement-in-canada-working/>.
- Bartiaux, F. (2008) "Does environmental information overcome practice compartmentalisation and change consumers' behaviours?" *Journal of Cleaner Production*, 16(11): 1170-1180.
- Barton, D. (1989) "Principles". In *Co-operatives in Agriculture*, David Cobia (Ed), (Englewood Cliffs).
- Birchall, J. (1997) *The International Co-operative Movement* (Manchester University Press).
- Birchip Cropping Group (2017), *Connectivity Capability Trust: Creating Farmer Driver Traceability for Victorian Grain Exports using Precision Agriculture*.
- Box, P., Sanderson T., and Wilson, P. (2017) "National Soil Data Project: Recommendations for a Farmers' Data Market". (CSIRO).
- Carbonell, I. (2016) "The ethics of big data in big agriculture". *Internet Policy Review*, 5(1).
- CASA (2017) "Flying over your own land – excluded RPA". <https://www.casa.gov.au/aircraft/standard-page/excluded-remotely-piloted-aircraft-flying-over-your-own-land>.
- CASA (2017) "Part 101 Amendments – Cutting red tape for remotely piloted aircraft". <https://www.casa.gov.au/aircraft/standard-page/part-101-amendments-cutting-red-tape-remotely-piloted-aircraft>.
- Castillo, M., Boucher, S., and Carter, M. (2016) "Index Insurance: Using Public Data to Benefit Small-Scale Agriculture". *International Food and Agribusiness Management Review*, 19(A): 93-114.

CHS Midwest Cooperative (2016) "Big Data Innovations in Agriculture".
<http://www.chsmidwestcooperative.com/about-us/news/big-data-innovations-agriculture/>

Competition and Consumer Act 2010 (Cth).

D'Souza, C. et al. (2007) "Green decisions: demographics and consumer understanding of environmental labels". *International Journal of Consumer Studies*, 31(4): 371-376.

Daily Mail Australia (2017) "Future of farming? Driverless tractors and drones attempt to grow crops without humans setting foot on the land in a world first".
<http://www.dailymail.co.uk/sciencetech/article-4496498/Hands-free-farming-using-autonomous-tractors-drones.html>.

Data Commons Cooperative (2012) "Vision". <http://datacommons.coop/vision/>.

Dekhili, S and Achabou, M. (2014) "Eco-Labeling Brand Strategy: Independent Certification versus Self-Declaration". *European Business Review*, 26(4): 305-329.

Dries, L., et al. (2014) "Keeping Your Secrets Public? Open Versus Closed Innovation Processes in the Hungarian Wine Sector". *International Food and Agribusiness Management Review*, 17(1): 147-162.

DTN The Progressive Farmer (2016) "Right to Repair? Fair Repair Act".
<https://www.dtnpf.com/agriculture/web/ag/news/equipment-tech/article/2016/08/04/fair-repair-act>.

Dyer, J. (2016), "The Data Farm: An investigation of the implications of collecting data on farm" (Nuffield Australia).

Electrek (2016) "Tesla victim of its own success in Denmark: 2 to 3 months wait for service, some owners are furious". <https://electrek.co/2016/08/10/tesla-denmark-2-3-months-wait-service-owners-furious/>.

Ellixson A., and Griffin, T. (2016) "Ownership and Protections of Farm Data". (Kansas State University Department of Agricultural Economics Extension Publication).
<https://www.agmanager.info/machinery/precision-agriculture/farm-data-ownership-and-protections>.

New Zealand Farm Data Code of Practice (2016) "Farm Data Code of Practice".
http://www.farmdatacode.org.nz/wp-content/uploads/2016/03/Farm-Data-Code-of-Practice-Version-1.1_lowres_singles.pdf.

Farm Institute (2017) "Data: The New Productivity and competition catalyst".
<http://www.farminstitute.org.au/ag-forum/data-the-new-productivity-and-competition-catalyst>.

Farming Future (2016) "Strategy to drive innovation in Australian and Japanese agriculture".
<http://farmingsfuture.com/strategy-to-drive-innovation-in-australian-and-japanese-agriculture/>.

Farming Together (2016) "Birchip Cropping Group – A Modern Co-operative".
<https://agworks.com.au/birchip-cropping-group/>.

- Fox News Tech (2016) "Farmers fight for the right to repair their own tractors". <http://www.foxnews.com/tech/2016/07/25/farmers-fight-for-right-to-repair-their-own-tractors.html>.
- Freedom to Tinker (2013) "The New Freedom to Tinker Movement". <https://freedom-to-tinker.com/blog/felten/the-new-freedom-to-tinker-movement/>.
- GiSC Coop (2016) "GiSC Data Partners". <https://www.gisc.coop/benefits/data-partners/>.
- Griffin, T. (2016) "Value of Farm Data: Proving Damages Based on Trade Secret Protections". (Kansas State University Department Of Agricultural Economics Extension Publication). <https://www.agmanager.info/machinery/precision-agriculture/value-farm-data-proving-damages-based-trade-secret-protections>.
- Griffin, T., et al. (2004) "Adoption, Profitability, and Making Better Use of Precision Farming Data". (Staff Paper No 04-06, Department of Agricultural Economics, Purdue University, June 2004).
- Griffin, T.W., et al. (2016) "Big Data Considerations for Rural Property Professionals". *Journal of the ASFMRA*: 167.
- Grolleau, G. and Caswell, J.A. (2006) "Interaction between food attributes in markets: the case of environmental labelling". *Journal of Agricultural and Resource Economics*, 31(3): 471-484.
- Hellberg-Bahr, A and Spiller, A. (2012) "How to Treat Farmers Fairly? Results of a Farmer Survey". *International Food and Agribusiness Management Review*, 15 (3): 87-98.
- Huffington Post (2016) "Big Tech Squashes New York's 'Right To Repair' Bill". http://www.huffingtonpost.com.au/entry/right-to-repair-new-york_us_57641b5ce4b0853f8bf097fc.
- ICA (2017). <https://ica.coop/>.
- iFixitORG (2015) "John Deere Responds to Copyright Mess it Made@". <http://ifixit.org/blog/7192/john-deere-mess/>.
- Jakku, E., Taylor, B., Fleming, A., Mason, C., and Thorburn, P. (2016) "Big Data, Trust and Collaboration: Exploring the socio-technical enabling conditions for big data in the grains industry" (CSIRO Australia). <https://publications.csiro.au/rpr/download?pid=csiro:EP164134&dsid=DS2>
- Jóźwiak, A. (2016) "A Network-Science Support System for Food Chain Safety: A Case from Hungarian Cattle Production". *International Food and Agribusiness Management Review*, 19 (A): 17-42.
- Lincoln Journal Star (2016) "Farmers lobbying for the right to fix own tractors". http://journalstar.com/business/agriculture/farmers-lobbying-for-the-right-to-fix-own-tractors/article_f106d41c-d3a2-57d3-b4fb-c2dbd7835797.html.
- Manning, L. (2015) "Setting the Table for Feast of Famine: How Education Will Play a Deciding Role in the Future of Precision Agriculture". *Journal of Food Law & Policy*, 11: 113-156.

Mark T., Griffin, T., and Whitacre, B. (2016) "The Role of Wireless Broadband Connectivity on 'Big Data' and the Agricultural Industry in the United States and Australia". *International Food and Agribusiness Management Review*, 19 (A): 43-56.

Modern Farmer (2016) "Farmers Demand Right to Fix Their Own Dang Tractors".
<http://modernfarmer.com/2016/07/right-to-repair/>.

Newman, N. (2014) "Search, Antitrust, and the Economics of the Control of User Data". *Yale Journal on Regulation*, 31 (2): 401-454.

Newman, N. (2015) "Data Justice: Taking on Big Data as an Economic Justice Issue". Executive Report, March 2015. (Data Justice).

O'Donoghue, C, et al. (2016) "A Blueprint for a Big Data Analytical Solution to Low Farmer Engagement with Financial Management". *International Food and Agribusiness Management Review*, 19 (A): 131-154.

Ohio Country Journal (2015) "OSU working on new data cooperative"
<http://ocj.com/2015/06/osu-working-on-new-data-cooperative/>.

Open Data Manchester (2016) "What is Open Data?"
http://www.opendatamanchester.org.uk/?page_id=38.

Open Government Data (2016) "Welcome to Open Government Data"
<https://opengovernmentdata.org>.

Precision Ag (2016) "Ensuring Data Privacy in Agriculture".
<http://www.precisionag.com/systems-management/data/ensuring-data-privacy-in-agriculture/>.

Privacy Act 1988 (Cth).

Protopop, I and Shanoyan A., (2016) "Big Data and Smallholder Farmers: Big Data Applications in the Agri-Food Supply Chain in Developing Countries". *International Food and Agribusiness Management Review*, 19 (A): 173-190.

RCR Wireless (2016) "Case study: Drones give data, visibility to French farming cooperative".
<http://www.rcrwireless.com/20160829/big-data-analytics/drones-case-study-tag31-tag99>.

Regulation (EU) No 2016/679 of the European Parliament and of the council of 27 April 2016 on General Data Protection [2016] OJ L 119.

Restakis, J. (2010) *Humanizing the Economy: Co-operatives in the Age of Capital* (New Society Publishers).

Samuelson, P. (2015) "Freedom to Tinker". Research Paper no. 2605195 (UC Berkeley Public Law).

Sanderson, T., Reeson, A and Box, A. (2017) "Cultivating Trust: Towards an Australian Agricultural Data Market" (CSIRO Australia).

- Sawant, M., Urkude, R., and Jawale, S. (2016) "Organized Data and Information for Efficacious Agriculture Using PRIDE™ Model". *International Food and Agribusiness Management Review*, 19 (A): 115-130.
- Sonka, S. (2014) "Big Data and the Ag Sector: More than Lots of Numbers". *International Food and Agribusiness Management Review*, 17 (1): 1-20.
- Spina, A. (2014) "Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?" *European Journal of Risk Regulation*, 5(2): 248-252.
- Sputnik International (2017) "In Move Toward Air Safety, China to Require Drone Owners to Register UAVs". <https://sputniknews.com/asia/201705181053720307-china-uav-register-safety/>.
- Standing Committee on Social Policy and Legal Affairs (2014) "Eyes in the Sky: Inquiry into drones and the regulation of air safety and privacy" July 2014 (Commonwealth of Australia: House of Representatives).
https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Drones/Report.
- Stucke M., and Grunes, A. (2015) "Debunking the Myths over Big Data and Antitrust". *CPI Antitrust Chronicle*, May (2): 2-12.
- Sudduth, J. (2001) "Where The Wind Blows: Genetically Altered Seed And Neighbouring Farmers". *Duke Law and Technology Review*.
<https://scholarship.law.duke.edu/dltr/vol1/iss1/15/>
- Surveillance Devices Act 1999* (VIC).
- Sykuta, M. (2016) "Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services". *International Food and Agribusiness Management Review*, 19 (A): 57-74.
- Tech Dirt (2015) "Library of Congress Releases DMCA Anti-Circumvention Exemptions... And It's A Hot Mess" <https://www.techdirt.com/articles/20151027/10131232649/library-congress-releases-dmca-anti-circumvention-exemptions-hot-mess.shtml>.
- Thaler, R and Sunstein, C. (2008) *Nudge: Improving Decisions about Health, Wealth and Happiness* (Penguin Books).
- The Age (2016) "Man Faces \$9,000 fine for using drone to pick up a Bunnings sausage".
<http://www.theage.com.au/victoria/man-faces-9000-fine-for-using-a-drone-to-pick-up-a-bunnings-sausage-20161108-gsl3q2.html>.
- The Australian (2017) "Farmers fear new pests: activists' spies in the skies".
<http://www.theaustralian.com.au/business/farmers-fear-new-pests-drones-spying-on-land-clearing/news-story/2c29e70f79bc75eb376a47fd3205c444>.
- The Cooperatives UK (2015) "World's first data co-op launches browser protection app".
<http://www.uk.coop/newsroom/worlds-first-data-co-op-launches-browser-protection-app>.
- The Land (2016) "Drones take flight again".
<http://www.theland.com.au/story/4048267/drones-take-flight-again/>.

Torrance A, and Von Hippel, E. (2015) "The Right to Innovate". *Michigan State Law Review* 793-830.

United States Digital Millennium Copyright Act, 17 U.S. Code § 512 (1998).

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

Wall Street Journal (2017) "Why Big Data Hasn't Yet Made a Dent on Farms". <https://www.wsj.com/articles/why-big-data-hasnt-yet-made-a-dent-on-farms-1494813720>.

Whitacre, B, Tyler B. Mark, T, and Griffin, T. (2014) "How Connected are Our Farms?". *Choices*, 29 (3): 1-9.

Wired (2015) "New High-Tech Farm Equipment Is a Nightmare for Farmers". <https://www.wired.com/2015/02/new-high-tech-farm-equipment-nightmare-farmers/>.

Workplace Privacy Act 2011 (ACT).

Workplace Surveillance Act 2005 (NSW).

ACCELERATING PRECISION AGRICULTURE TO DECISION AGRICULTURE - P2D PROJECT RESEARCH PARTNERS



PROJECT LED BY



Australian Government

**Cotton Research and
Development Corporation**