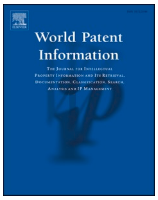
Contents lists available at ScienceDirect

World Patent Information

journal homepage: www.elsevier.com/locate/worpatin



The possibilities and limits of trade secrets to protect data shared between firms in agricultural and food sectors

Alfred Radauer[a,*], Nicola Searle[b], Martin A. Bader[c]

[a] *IMC University of Applied Sciences, Krems, Piaristengasse 1, A-3500, Krems, Austria*
[b] *Goldsmiths, University of London, New Cross, London, SE14 6NW, UK*
[c] *Technische Hochschule Ingolstadt, Esplanade 10, D-85049, Ingolstadt, Germany*

ABSTRACT

Both public policy and business management are increasingly interested in how to manage trade secrets. One of the driving forces is the growing significance of data as an asset, as 'oil of the 21st century'. Trade secrets are often seen as the major Intellectual Property (IP) tool for protecting data. There is also the understanding that the need to share data is increasing to allow for new types of innovation. This paper seeks to understand how data sharing practices and the use of trade secrets are evolving in the agricultural industries. Using explorative empirical data from four in-depth case studies, the paper develops a framework for data sharing practices, value sharing, and trade secrets use. We find that current data sharing practices pool around two scenarios, where data is not shared or shared only with limited partners (hence closed) and there are differences whether value created from the data is shared. We conclude that a nuanced view on the use of trade secrets in data sharing is mandated for both IP/data managers and scholars analysing the topic.

1. Introduction

Agriculture has become a rich playing field for digitalization and related digital innovations, suggesting an informational revolution in this industry dubbed even as "Agriculture 4.0" [1]. Agricultural digitalization entails the management of tasks throughout the value chain and food system, based on data from 'animals, soil, water, plants and people' to evaluate, predict, and improve efficiency [2].[1] Such data is collected and managed across a wide and heterogonous range of firms and organisations in the agricultural value chain.[2]

To leverage the full potential of digitization and data-driven innovation, it is imperative that data can be easily shared and accessed [5]. However, barriers to data sharing exist. For example, farmers may analyse their own data and aggregate with other farms to provide insights unfeasible under previous technologies. Yet farmers are often reluctant to share data due to questions surrounding, e.g., data ownership or equitable sharing of the benefits of data collection [6]. Protecting data and regulating access to shared data is a significant issue.

The optimal appropriation strategy for data is unclear. Referring to legal protection, and herein the system of formal intellectual rights, there are limited possibilities to protect data. Data as such is not patentable subject matter, and there are also limits as to the extent that copyright or trademark protection can apply to data (see also section 2.2). This situation has led many to point to and discuss trade-secrets as an alternative IP-like means to protect data [5,7].

Trade secrets are an important IP-like mechanism to reap the returns of innovative activities [8] and shore up Teece's [9] concept of appropriability. There is a balance between trade secrecy that incentivises innovation and trade secrecy that inhibits the flow of knowledge and innovation [10]. This is particularly true in the agriculture sector, where the flow of knowledge holds great potential to address pressing

* Corresponding author.
E-mail addresses: alfred.radauer@fh-krems.ac.at (A. Radauer), n.searle@gold.ac.uk (N. Searle), Martin.Bader@thi.de (M.A. Bader).

[1] The full quote is, "… that management tasks on-farm and off-farm (in the broader value chain and food system) focus on different sorts of data (on location, weather, behavior, phytosanitary status, consumption, energy use, prices and economic information, etc.), using sensors, machines, drones, and satellites to monitor animals, soil, water, plants and humans. The data obtained is used to interpret the past and predict the future, to make more timely or accurate decisions, through constant monitoring or specific big data science enquiries." [2] L. Klerkx, E. Jakku, P. Labarthe, A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda, NJAS-Wageningen Journal of Life Sciences 90 (2019) 100315.

[2] The agricultural value chain includes the producers of production inputs, farmers and grower, aggregators and processors, trades, distributors and retailers, consumer, and, finally, waste disposal, recycling, and composting [3] BASF, Food Value Chain Collaborations For Smarter Crop Protection, 2021. https://agriculture.basf.com/global/en/business-areas/crop-protection-and-seeds/services/food-value-chain.html. (Accessed 31 October 2021), [4], FAO, Developing sustainable food value chains – Guiding Principles, 2014. https://www.fao.org/3/i3953e/i3953e.pdf.

https://doi.org/10.1016/j.wpi.2023.102183
Received 31 October 2021; Received in revised form 4 February 2023; Accepted 27 February 2023

environmental and humanitarian concerns. Indeed, the WTO's Trade Related Aspects of Intellectual Property (TRIPS) agreement specifically references trade secrets in agriculture [11].

A challenge to analysis of trade secrets and data is measuring trade secret use [12]. While legal scholars have begun to analyse trade secrets in data-intensive environments, management literature has not. Trade secrets are discussed mostly as complementary or alternative to formal Intellectual Property Rights (IPRs) like patents [13–15]. There is a lack of theoretical/empirical studies on rationales and barriers to use trade secrets, particularly concerning data as protected asset. This is particularly a concern when data is or needs to be shared between and across different organisations, such as, as discussed, in modern agriculture. This paper seeks to address this gap, by developing empirical insights into the sharing of data.

We have two core research questions. Our first addresses the possibility of the existing IP framework, in the form of trade secrets, to protect data in collaborative or sharing environments. We ask: *To what extent are trade secrets a viable tool to protect data (in particular data that is shared across organisations) in agriculture?* To answer this fully, we need to understand the prevalent data sharing practices in agriculture. Our second question, therefore, is: *What are major data sharing practices in agriculture?*

To address these questions, we develop four qualitative case studies on the use of trade secrets by firms in different parts of the agricultural value chain to protect and appropriate value for their data. We place the strategies, tools, and practices into a theoretical framework.

The remainder of the paper is structured as follows: Section 2 gives the conceptual background. Section 3 details the approach and methodology employed for the empirical research. Section 4 presents the case studies. Section 5 provides a discussion of the empirical results, and section 6, eventually, our conclusions.

2. Conceptual background

In this section, we outline the conceptual background for the study. We approach our analysis by framing both data and IPR as integral to the resource-based view (RBV) of the firm. We start by providing the theoretical foundation and by describing in general the means available to businesses in agriculture to protect their assets with IP and IP-like instruments. We then continue with a specific section on trade secrets use by businesses in the context of data, mostly from an economic and business point of view. We outline accompanying and complementary measures specifically to trade secret protection. We extend the discussion of trade secrets as protection mechanism specifically to data and data sharing in agriculture. We close the section with a discussion on incentives and disincentives to share data in the light of the previous sections.

2.1. Theoretical foundations and the limited applicability of classic formal IP to confidential data in agriculture

Our focus on trade secrets maps nicely to the RBV, which holds that firms achieve a competitive advantage if they focus on internal factors, notably resources [16]. To qualify as a resource offering a competitive advantage, resources – which can be either tangible or intangible – must fulfil the VRIN criteria: they must be valuable, rare, costly to imitate, and non-substitutable. IPR are frequently seen as forms of intangible resource that fulfils the VRIN criteria. However, as we detail in this section, traditional means of IPR afford little protection to data.

IPR create protection for different aspects of firm's innovation activities and outputs through legal exclusion rights and include patents, trademarks, and copyright. Over the past thirty years, IPR in agriculture industry have undergone international harmonisation and the development and up-take of industry-specific forms of IPR, e.g., plant variety rights (PVR, a.k.a. plant breeder's rights), which allow firms to control propagating and harvested material from their new plant varieties.[3] Trade secrets for such plant innovations are ineffective as reverse-engineering of self-replicating biological products is moot, hence the industry's reliance on PVR [18]. PVRs cannot be used to protect many forms of data that is created and shared in digitalized agriculture.

Data enjoys scant options for IP protection. In some jurisdictions, including the UK and EU, data can attract protection from the sui generis database right. However, the introduction of this right was met with competition concerns [19] and the right itself has had surprisingly limited uptake [20]. Other IP rights, namely patents, copyright and trademarks also provide only limited protection for data. In the EU, copyright can be used in conjunction with database rights [21], although infringement can be difficult to detect. Copyrighted data still reveals significant information even if it cannot be copied. Trademarks and patents can provide indirect protection of data. Trademarks protect branding, which can increase the value of data if, for example, a data broker develops a reputation for high quality data. Patents can offer complementary protection for data as they can establish legal monopolies for the processes and products that lead to the creation of data, restricting the ability of competitors to gather such data.

To summarise, traditional forms of intellectual property rights are only of limited value when it comes to the protection of data. It may be questioned whether data without IP protection is a VRIN resource. Cuthbertson & Furseth [16] argue that data is an "operand resource" like raw materials, capital or components, while algorithms processing the data are an "operant resource" akin to processes, organisation and culture, with the latter transforming the former. Both authors assess the VRIN nature for data – they maintain that *"… while digital resources, such as data and algorithms, may be rare, and sometimes difficult to imitate or substitute, their value decreases over time"*. In the next section, we will show, however, that certain types of data – namely those protected by trade secrets, as well as the respective trade secrets themselves – fulfil very well the VRIN criteria.

2.2. The use and utility of trade secrets in a data context

Firms cite trade secrets as a preferred protection mechanism. Trade secrets are an important legal tool that enables firms to appropriate the returns from their innovative efforts [8], and enable firms to protect information, even while sharing it, by providing a legal solution to Arrow's information paradox [22]. Data – as a special form of information – must meet three tests to earn trade secrecy protection. It must be commercially valuable because it is secret, be known only to a limited group of persons, and be subject to reasonable steps taken by the rightful holder of the information to keep it secret, including the use of confidentiality agreements for business partners and employees.

We argue that the legally defining elements of trade secrets are well aligned with the VRIN criteria in RBV. The fact that a trade secret must show value satisfies the value criterion. The secrecy criterion implies rareness (as the data/information is not publicly known). Moreover, the fact that the value of the trade secrets must arise from the secrecy points also to the need of the protected asset to be difficult to imitate or

[3] In fact, industry specificity can be considered in itself to be an application of the resource-based view. According to [17], RBV *"… looks at industries as groups with similar competences and resources … it explains that there are industry-specific competencies and industry-specific 'recipes' for innovation."*

substitute.[4] Consequently, there would be no incentive to invest in "reasonable steps" to keep the information secret if the to-be-protected asset is easily imitable or substitutable.

Trade secrets are generally cheaper to maintain than alternatives, last indefinitely and do not require arduous legal processes [23]. Data itself is increasingly viewed as a self-replicating form of capital, where data enables the collection of further data [24]. Hence, the criticism of Cuthbertson & Furseth [16] of value declining with time falls short in the case of data that is protected through trade secrets. In line with this argument, literature shows that limited disclosure can extend lead-time advantages [25]. Interestingly, patenting firms tend to protect a larger portion of their innovation with trade secrets than non-patenting firms [26,27]. Trade secrets may enhance the efficacy of patents. A firm may choose to patent data-generating innovations but maintain underlying data as a secret and thereby extend the practical life of the patent [25].

The lack of disclosure afforded by trade secrets, in contrast to the required disclosure of patents and other IP, makes trade secrets a desirable protection instrument for firms to reduce knowledge spill overs to rivals and raise the cost of reverse engineering. Disclosure also influences the common approach of trade secrets preferred protection mechanism for processes, which are more difficult to reverse engineer or detect infringement, and patents for products, in which both are easier [12,28–30]. Firms are more likely to patent when trade secret laws are weaker [28,31,32], and less likely to patent when trade secret laws are stronger [10,33]. Both trade secrets litigation and jurisprudence are increasing, particularly in the United States [34].

Survey work confirms the early findings [28,29] that trade secrets are a preferred mechanism although more granular findings vary by population studied and demographic. Trade secret strategies are nuanced and influenced by a multitude of firm and industry characteristics [35]. Chang et al. [36] find service firms rank trade secrets as their preferred tool, followed by, in descending order of preference, lead-time, patents, lock-in and know-how. In the material and mechanical engineering industry, older firms prefer to protect process technologies with trade secrets rather than patents, whereas the reverse for product innovations [12]. Leiponen & Byma [37] similarly find preferences for trade secrets amongst small firms. Beukel et al. [38], via their finding that family-owned SMEs in the wine industry prefer patents to secrecy due to the relative certainty of patents, argue risk-adverse firms may prefer patents.

However, trade secrecy presents a conundrum for firms when addressing knowledge flows. Trade secrets are a useful tool for knowledge management [39], and while freely flowing knowledge within a firm is conducive to innovation [40], it exposes a firm to knowledge leakage [41]. To protect trade secrets, firms may limit employee's access to said knowledge, which can create a culture of mistrust [42]. Firms are less likely to share information in industries with fast-paced technology change [43].

Trade secrets are generally considered to be weaker IP-like rights by design, so that it is more difficult for firms to maintain monopolies based on the secrecy of this IP and consequently undermine the incentive-to-innovate framing of IP. Trade secret protection is not iron-clad, once factual secrecy is lost, so is trade secrecy. Trade secrets also offer, as said, no remedies against independent invention or reverse engineering. Misappropriation of trade secrecy can also lead to loss of protection, but here the law allows for trade secret owners to seek damages.

To summarise, the literature generally points to trade secrets as being a surprisingly useful tool for firms, despite the uncertainty surrounding the efficacy of trade secrets as a protection mechanism. The question is whether efficiency and efficacy can be increased through complementary measures. We assess this (affirmatively) in the next section.

2.3. Complementary measures for trade secret protection

For trade secret protection to work, accompanying measures are necessary, particularly in relation to the third requirement for trade secret protection, namely the necessity to implement reasonable steps to ensure confidentiality. Against this backdrop, contracts need to be mentioned specifically.

Contracts are helpful non-IP, legal structures for the protection of data. In addition to trade secrets and reasonable protection measures, firms may use related contracts such as non-disclosure agreements (NDA) [44]. Securing data, educating and contractually obliging employees to maintain confidentiality, and careful management of relationships with vendors also bolster protection for farm data [44]. Related means include Covenants Not to Compete (CNC), litigation and gardening leave, which deter the movement of employees and consequently information spill-overs [45].

It is important to note that not all data qualifies, or indeed needs, trade secrecy protection. Some confidential business data, such as company strategies, may be 'factually secret[5]' but not qualify for trade secrecy itself. As noted by Sandeen & Aplin [46], the Waymo v. Uber[6] case started with the misappropriation of 14,000 factually secret documents but concluded with only eight disputed trade secrets. In other cases, maintaining confidential business information as factual secrets through practical protections, rather than IP protection, may provide adequate protection to meet a firm's needs.

2.4. Incentives and barriers to data sharing using trade secrets

Data sharing is an important enabler of Open Innovation. Secrecy, however, can be seen as incompatible with openness [26]. Trade secrecy, as an innovation appropriation mechanism, presents prima facie a contradiction in data sharing: by sharing data, firms may benefit but lose secrecy, by not sharing data, a firm maintains secrecy but foregoes potential benefits. More broadly, firms choose between using trade secrecy to limit spill overs and signalling openness to collaboration partners by not using trade secrecy. In this 'Paradox of Openness,' Arora et al. [26] find leading firms are more concerned about spill overs, whereas followers are more focused on being perceived as valuable collaborators.

Over the last years, open data has emerged as a specific field particularly in the context of research/scientific data and data owned by public bodies (open government data). Openness is hereby defined in a way that it *"… means anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness)"* [47]. In a paper by the OECD, benefits of (open) data sharing include *"i) greater transparency, accountability and empowerment of users, for instance, when open data are used for cross-subsidising the production of public and social goods; ii) new business opportunities, including the creation of start-ups and in particular for data intermediaries and mobile app developers; iii) competition and co-operation within and across sectors and nations, including the integration of value chains; iv) crowdsourcing and user-driven innovation; and v) increased efficiency thanks to linkage and integration of data across multiple sources."* [48].

While the above points to a picture where trade secrets are an "enemy" of open approaches, the true nature of trade secrets must be

[4] In this context, it is important to note that trade secret law provides for an exception for reverse engineering. This means that it would be perfectly legal for a competitor to study a trade secret and eventually break it fully on its own and independently by means of R&D and experimentation. By contrast, trade secret law would penalize the breaking of a trade secret by means of industrial espionage.

[5] Sandeen and Aplin [46] define 'factual secrecy' as being the opposite of 'public information,' and is a similar concept to confidential business information.

[6] Waymo LLC v Uber Technologies, Inc, 2018 WL 646701, United States District Court, N.D. California No. C 17–00939 WHA.

viewed in a more differentiated manner. Lack of trust between collaboration partners, transaction costs and the shortcomings of existing protection mechanisms create economic barriers to sharing. Inter-organisational trust matters [49], however trust can be difficult to develop [50]. Trade secrecy policies allow firms to rely on legal protection beyond the minimum threshold of reasonable measures, rather than disproportionately investing in practical protection measures. In collaborative environments, this enables firms to share data at a lower cost. Trade secret's creation of a legal right establishes a foundation for firms to appropriate the returns to their innovative efforts without inefficient spend on secrecy.

2.5. Trade secret protection and data sharing in agriculture

As agriculture moves towards a more digital technology basis, trade secrets have become an important tool for the protection and management of data in this sector. In agriculture, trade secrets also protect the substantial agricultural know-how required to use this asset in practice [51]. In some jurisdictions, such as the U.S., trade secrecy is essentially the only legal IP-like protection for farm data [52].

When it comes to the sharing of data across organisations, there is the question of how to organise and govern the sharing. In the EU, and for the agricultural industries, a code of conduct has recently been developed [53]. The respective document *"will look at general principles for sharing agricultural data within the agro-food chain. To this end, the co-signatory organisations* [a variety of different associations located at different parts of the agricultural value chain, ed.] *hereby have been working together to produce a non-binding code that sheds greater light on contractual relations and provide guidance on the use of agricultural data.*" [53]. The code also mentions trade secrets, but only in general terms, when it calls for contracts to respect different forms of IPR. While the code of conduct is relatively young, it has drawn already the attention of scholars. In their analysis of the code, van der Burg et al. [54] in principle acknowledge the utility of a contract to improve trust-relationships but argue that additional measures in an amended version of the code may be necessary if there is a (larger) know-how or resource imbalance between the sharing parties.

Similar to a code of conduct is the creation of data intermediaries, known as data platforms or data exchanges.[7] Perkmann & Schildt [55] argue that intermediary data organisations may enable data sharing. They find these organisations serve as mediating vehicles that enable firms to reveal information while minimizing costs arising from the competitive consequences. While these 'trusted intermediaries' can help facilitate sharing and lower barriers-to-entry, concerns about lack of transparency and the aggregation of market power limit their potential [56].

3. Empirics –methodological approach

The general role and relevance of trade secrets in the agricultural and food sectors has already been described earlier [57–59]. However, the concrete application and relevance especially about data sharing and value creation and protection remains open.

This lack of evidence-base in a complex environment motivated an exploratory approach. Against this backdrop, we opted for a case-study approach to account for the exploratory, inductive nature of our analysis. Case studies are in this context of particular use as they are an "*… empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident*'' [60]. Limitations arise due to lack of statistical representativeness, but even with these limitation in mind they are seen as useful in exploratory approaches [61]. They help understand the *"how*'' and *"why*'' [62].

Our case studies were based on semi-structured interviews with European agricultural firms to identify their data management and sharing practices, their trade secrets use, and complemented by an analysis of selected company documents. Four in-depth interviews were conducted in July 2021 with the IP managers companies, i.e., one interview per case company. Each interview lasted for approximately 1 h. The case studies were furthermore informed by data gathered from firm documents, e.g., their websites, annual reports, etc., as well as occasional industry-specific publications. The case studies were selected to represent major different parts of the agricultural food and value chain and to demonstrate the spectrum of data creation and use across the agriculture value chain, including the choice of the level of openness in data sharing depending on the types of data shared.

For our case study analysis, we focused on the first three steps of the agricultural value chain. These are: the producers of production inputs sector: agricultural science and biotechnology industry (one case study); the farming and growing sector: agricultural machinery industry (one case study); and, for processors and aggregators we address two sectors: nutrition and food ingredient industry (one case study), food industry (one case study). This covers the start of the value chain before products are distributed.

Firms were large firms (not SMEs), and all operated internationally. The interviews were transcribed and analysed through coding of themes and approaches of the firms' data and trade secret management practices. To preserve anonymity, minimal details on the interviewee or the firm itself are included. An overview of the interview guide can be found in the Appendix.

4. Analysis

In the following, we present the individual case studies. Each case study features a short introduction to the firm, a description of data sharing practices and trade secrets use and reflections on the implications.

4.1. Case study A: agricultural science and biotechnology

4.1.1. The case study firm at a glance

Case study A looks at a large firm in agricultural science and biotechnology. Historically, farmers have been using selective breeding technologies to improve the yield of plants and their resistances, e.g., pest resistance, drought resistance, and herbicide resistance. Beside traditional breeding, new techniques, such as Genome editing, have been discovered and exploited by agricultural research and crop science industry, including our case study company A.

4.1.2. Data use, data sharing and the role of trade secrets

With respect to the examined industry sector, current state-of-the-art crop science is based on the genetic sequence raw data from plant sources. Although genetic sequencing as such is no longer a difficult step, access to and availability of genetic resources is considered valuable. The value of crop science data can be ranked by four categories with increasing perceived value:

1. Availability: the genetic resource as such (tangible) and its genetic sequence raw data (intangible), e.g., from plant sources.
2. Quality: further information on the source of the raw data and its processing, e.g., frequency sequencing, single sequence steps, consensus sequence, signal-to-noise ratio.
3. Correlation: related, parallel data sets that are in connection with the raw data, e.g., phenotype related data.
4. Causality: further data sets that may be relevant to explain causalities, e.g., environment related information, related to, e.g., soil, weather, climate.

There exists an international agreement covering data sharing, the

[7] Related terms include data pooling or data marketplaces.

Convention on Biological Diversity (CBD), originally initiated by the United Nations. It has been signed by more than 190 countries worldwide. As part of the strategic goals CBD claims that "*benefits arising out of utilization of genetic resources are shared in a fair and equitable manner*" [63]. Nevertheless, although the owners of these data sets generally would be interested in providing and sharing their data sets on different levels, the issues come regarding the benefit sharing for shared data sets. The interviewee commented that *"it's a pity that we cannot offer our data to third parties …"*.

Our interviewee noted the sharing of data sets in the agriculture science sector in this context currently fails because the industry players lack a pragmatic, safe and low-cost procedure to share the benefits that would come from a sharing of these kind of data sets. On one hand, a potential data set user has first to check and apply a data set before knowing which value it is creating. On the other hand, the data set owner has first to provide the data set and then later hope for a potential user to fairly estimate its value share and wait for its compensation. The latter is especially tricky as it is generally difficult for the data set owner to track and trace the later use and value creation of its data set, making the data set owner fully depending on a data set users' credibility and fairness.

The data sets are likely to be considered as trade secrets if treated accordingly by the data set owners. However, the trade secret laws in place do not solve the 'disclose first' and then 'establish and share benefits' dilemma. With a general publication in data bases the trade secrets would lose their trade secret status, although might still engender database rights and/or copyrights. At present, the dilemma can only be overcome by lengthy and elaborate bilateral, contractual agreements, which in general are burdened with too high transaction costs compared to the value created by a sharing. As a result of that, especially large companies rather create and establish their own data sets even if they know that they possibly could get ones that someone else are already owning but not sharing due to the above-mentioned transaction issues.

We consider that a possible vision for how to overcome the dilemma barrier could be the creation of an open data sharing system: e.g., offering and sharing data sets and bases within a group of 'registered' sharing partners (so trade secret status could be kept opposite to third parties that are not participating). There already exists a practical example in Brazil for the use of their indigenous genetic bio-resources which, however, is bound to a physical handover of tangible biosamples. The establishment of suitable business models for fair and equitable benefit compensation for the use of data sets might be another vision, but the question remains open what kind of business model this could be.

4.2. *Case study B: agricultural machinery*

4.2.1. *The case study firm at a glance*

This case describes a large, family-owned agricultural machinery manufacturer. The case study is derived from a group interview with two managers from the company, one responsible for R&D and one for open innovation.

4.2.2. *Data use, data sharing and the role of trade secrets*

The company discussed the challenge of digitalization in agriculture, and investments in respective R&D. In terms of data sharing, sensor-generated data from the machines are one key issue. Examples of respective innovations where data sharing occurs – which not only the company itself, but also competitors are working on – concern, for example, revolving harrows. Harrows are tools used for aerating soil; removing moss and weeds; leveling soil and sand, breaking up and spreading manure; as well as for seedbed raking.[8] New sensors built into modern harrows can now measure important properties of the soil (e.g., through image recognition), hereby creating data.

The ensuing data is used to adapt the harrow operation to the specific characteristics of the specific piece of soil the harrow is, at a given time, working on. This is done by, e.g., varying rotational frequency or harrowing speed. Important in the context of data sharing, the sensors can also provide commands to the tractor (a different machine) which is pulling the harrow, e.g., to regulate the speed with which the tractor is travelling across the field. That way the soil is optimized in a tailor-made manner for later seeding. Another example of a possible innovation is in harvesting of grassland (pastureland). After the grass is cut during the hay harvest, the task is to dry the grass to produce hay. Weather and sensor data can be used in conjunction to determine exactly the time when a machine is to upend the grass so it can better (faster) dry.

These innovations, and similar ones, require that data be shared between different agricultural machines. The data sharing leads to a situation where the focus is not solely to exercise control over the operation of an individual machine anymore, but to control an entire agricultural process involving different process steps and a full range of differently involved agricultural machines. The data sharing is hereby seen as an important means for business model innovation by catalysing the development of machinery ecosystems, in the sense of entire farm management systems.

Data sharing that leads to optimal combinations of different types of agricultural machines is a selling proposition for farmers to buy the different machines from the same vendor and machinery ecosystem. Major revenue streams for the vendors still stem from the sale of machines. As one interview partner said, *"… our company is still operating in the machinery industry."* (interview partner). Against this backdrop, there is also a race in terms of economies of scope and scale in the industry on-going to develop such ecosystems. The leading agricultural machinery manufacturer, John Deere, is said to be "… *the likes of Apple in agriculture, developing its own rather closed ecosystem*" while "… *the smaller manufacturers team up to create a more open ecosystem of the like of Android, and there is a clear need to collaborate.*" (ibid.) To this end, the company studied in the case study has multiple R&D collaborations ongoing, with manufacturers of other agricultural machinery equipment, but also with R&D organisations and farmers.

With respect to trade secrets and shared data it leaves the question of where the trade secrets kick in, and how trade secrets and/or other IP may help protect or appropriate the shared data. The company hereby points to the aforementioned EU code of conduct on agricultural data sharing from 2020 [53]. According to the generally laid out principle in this document, data produced by a farmer due to farming activity (as 'data originator') is to be assigned to ('owned by') the farmer, while machine data and sensitive data "… *only relevant to the correct functioning of the machinery …*" (ibid.) is 'owned' by the machine producer.

At first glance, this seems to create a very proprietary environment for data created by the farmer. Such data could be partly also considered trade secrets, if the respective requirements – commercially valuable, not known to the general public, adequate protection measures – are fulfilled. However, the document notes: *"There is a common political view that assumes that increasing data sharing is only possible by making it mandatory, due to the originators' unwillingness to share data. The opposite is true: farmers and agri-businesses are more than willing to share data with each other and engage in a more open data mind-set. However, they will only do so if the potential benefits and risks are made clear and when they can trust that these are settled in a proper and fair way through contractual agreements."* (ibid.)

Hence, the code recommends setting up contractual agreements based on the laid-out principles between farmers (or other data

[8] https://www.countrysmallholding.com/in-focus/five-reasons-to-harrow-1-4443316, last assessed 6 June 2021.

originators in the agricultural value chain) and users of this data. In doing so, a situation ensues where data is shared by many farms, which is useful because the sharing allows for detection of certain patterns only notable across many farms, hereby providing insights helpful also for optimising the operation of an individual farm. In essence, this means that the raw data from the sensors, but also the processed data after it was processed/computed and analysed, as long is not solely relates to the correct functioning of the machine, is typically shared rather openly and hence not considered a trade secret by our interview partners. This is if the principles of the code, whose application is voluntary, are applied. However, *"… the big trade secret is actually how the raw data is processed, such as the algorithms behind the software in the machines. This is what needs to stay secret"*, according to the interview partners.

Matters might change, however, with the advent of Artificial Intelligence (AI). If there is a need to have, for example, complex and large databases of images in place from which AI algorithms must learn how to discern specific types of weed from legit useful plants in the field, it is questionable for our interviewee whether smaller players have enough resources to develop such databases themselves. We were told that one of the big tech companies has in this context already placed an eye on the agricultural machinery/farm of the future market. Eventually, this may lead to a situation where even more data sharing may be necessary, and this is where trade secret protection specifically for shared data could have significant value in the future. For the time being, however, the case study company argued this data sharing *"… is not yet there."* (interview partner).

4.3. Case study C: nutrition and food ingredients

4.3.1. The case study firm at a glance

This case study concerns the nutrition division of a large firm. The division engages mainly in the development and production of food ingredients such as vitamins, fatty acids, including nutritional supplements that are used both in food for humans as well as for animals/livestock. The case study is based on an interview with the IP manager of that division.

4.3.2. Data use, data sharing and the role of trade secrets

Data sharing was said by the interview partner to be an absolute necessity in this industry. Much of this data is data relating to know-how on production processes, such as details on the process steps, on physical parameters of the production processes like on the right temperatures and pressures or flow rates. Much of the respective data is subject to trade secret protection. The necessity to share data manifests itself in four distinct situations:

1. When the customers demand both data and know-how. As described by the case study interview, when *"… a client does not only want to have a raw product but also some know-how of what to do with the raw material* [we ask ourselves]: "*What can we share under what conditions?"* In particular, the need to share know-how poses a problem.
2. When regulatory data needs to be shared with authorities (such as with toxicological data)
3. When data may need to be shared also during R&D collaborations, including also in partnerships for very niche applications, such as for research into types, formulations and dosages to feed certain types of fish in aquacultures (which requires a very specialized R&D partner and also a specific collaboration with a fish farmer).
4. Particularly in the international context, when data is shared with production partners who produce a certain ingredient to the specifications of the company (make-to-order), and where the partners are not able to produce the product without the know-how of the company.
5. When there are instances of second sourcing, such as where clients need to have more than one supplier for security reasons. This requires also certain levels of data sharing with the client and/or with a second source.

In essence, the data sharing procedures involve a careful weighing of which kinds and parts of the trade secrets are to be divulged. There are also different levels of trade secrets, which range from *"nice to have and know that"* to the *"crown jewels, of which there may not be that many, but it would really hurt if these secrets were to leak"* (interview partner). This also influences the extent of the trade secrets and trade-secret protected data that are to be shared.

The instruments by which trade secrets are implemented are mostly contracts, particularly in the form of non-disclosure agreements (NDAs) or incorporated into material transfer agreements (MTAs). They also form part of licensing deals as combined patent and know-how licenses, where – for example – the terms of the licensing contract can differentiate between the patent (the term is here limited by the maximum running time of the patent) and trade secret (for which a longer term of non-disclosure can be defined). Apart from the legal tools, there are also technical and practical procedures such as physical access controls, IT security measures as well as measures such as to cover certain machines with blankets when authorities visit the company premises.

Generally, when asked about where leakages occur, the interview partner stated that classical industrial espionage is not very widespread, *"… either because the spies are so professional that we do not notice security breaches or because they really have a lesser role in practice (despite, of course, many competitors being no doubt interested in the secrets)"*. (interview partner). The more eminent danger for trade secrets comes in the form of former employees, who carry the secret to a competitor or – perhaps more menacingly – who set up a firm of their own to compete with their former employer.

Up to this point, shared data subjected to trade secret protection is clearly data relating to know-how and/or even embodies know-how. Shared data not incorporating know-how – e.g., sequences of numbers and signs generated by sensors – is more of a future scenario for the firm. It could come, for example, when sensors monitor fermentation processes and can hereby help, through predictive AI modelling, creating optimized production processes or sound the alarm if sub-optimal results are to be expected in the production. However, the company *"… is still working to make such scenarios susceptible and useable through trade secrets."* (interview partner).

It is important to underline that, apart from data generated/owned within the company, there is also the complementary situation to consider when the company gains access to data protected by trade secrets of third parties. Two situations stand out in this context: First, when the company completes a takeover, regulatory/antitrust rules may require the company to have a 'firewall' established between the acquired firm and the parent company. Secondly, there is a danger that the company becomes *"contaminated"* (interview partner) with a foreign trade secret of a collaboration partner: *"A case in point could be a client, who seeks new compositions/recipes for its products, informs us of what they are up to and look into our databases. In such cases, we could get knowledge of data and trade secrets of the pharma firm, which we could otherwise have developed and maybe then patented on our own"* (interview partner). For respective situations, contracts may include some sort of Anti-NDA clauses that stipulate that if the company gets knowledge of respectively defined trade secrets, this should be considered an act of disclosure.

Despite the firm's highly professionalised system of handling of trade secrets, our interview partner stated that there has been still a considerable learning curve to take. The reason lies in specifics of trade secret protection *"… which do not come with well-defined deadlines and hence, there is less of a sense of urgency compared to,* e.g.*, patents."* In addition, as trade secret law in the past was covered in different parts of the law, so where different aspects of trade secret protection handled by different departments, e.g., the legal department, the IP department, the IT department and/or corporate security. Eventually, trade secret protection comes also with costs, which is those costs associated with implementing the 'adequate' measures to maintain secrecy. Taken all together, a situation ensued in the past where nobody felt truly responsible for trade secrets, the topic was felt as cumbersome, expensive, and not urgent (compared to other day-to-day duties), so it was put at the bottom of the agenda. For our interview partner, the new European Trade Secret Directive had a significant impact in that it unified and standardised the topic to an extent and created the sense of urgency needed. Therefore, trade secrets have now also a clear institutional ownership (in the IP department).

Finally, in the light of the above, our interview partner pointed to the need for a *"classic, well defined"* (interview partner) change management process implemented in the firm (and recommended also for other firms) to raise awareness and skills of employees with respect to trade secrets. This includes topics such as on how to identify trade secrets. In the company under scrutiny, this is sometimes done in the form of a war game and role play. The scenario played is that the workshop participants want to leave the firm and set up their own company – what would they then need to take with them in terms of information and data not known to the public? To what extent would that hurt the company? In addition, awareness increasing measures include longer trainings or short teaser films.

4.4. Case study D: food

4.4.1. The case study firm at a glance

Case study D concerns a large player in the food industry. The specific activities analysed concern the development of new nutrition formula and food ingredients to investigate and understand nutrition needs and effects of nutrition ingredients.

4.4.2. Data use, data sharing and the role of trade secrets

An important basis to the development of new nutrition formula and food ingredients is to investigate and understand nutrition needs and effects of nutrition ingredients. Typically, the industry conducts research along two levels: primary and secondary observations. Primary observations ('raw data'), e.g., clinical studies that generate clinical data to understand how nutrition ingredients work in human bodies, where observations are created by humans, so data is based on human input. Secondary observations ('end data') are conducted in a series of observation steps interpreting from a certain point of view, e.g., how the effects of an ingredient correlate with health conditions and eating habits, leading to data sets of transformation levels; the goal is to transform the raw data of the first level into something meaningful, e.g., to find and to define the characteristics for new product requirements.

Primary studies are either conducted by third parties, e.g., clinical research institutes, on behalf of the contractor or can even be bought on the market. Secondary studies instead are more complex and are normally conducted in a closed consortium with several contributors, or with partners. Whereas service providers are directly paid-off for their services, contribution partners that deliver own input want to use and exploit the created data and insights for their own purposes. So, an aligned data creation and shared use scheme is necessary. It is important to the consortium partners to get clarity and a common understanding of the future exploitation by each partner already upfront, which gets fixed in a contractual agreement before research is conducted.

An important restriction on consortia is imposed by antitrust laws that limit agreements between big segment competitors, therefore firms must be careful with whom they collaborate.

The industry claims itself to have an exclusive rather than sharing mindset: *"Our industry is still very protective – we want to have control about the data and its use"*. (interview partner). However, there are typically two common situations to share data that are also settled contractually upfront: as some of the consortium partners are often universities, these aim to publish. The food companies aim to build sustainable business models based on their research that include – if technically possible – patent protection, e.g., applications of the research outcome in the nutrition and food environment. To achieve a legally viable and enforceable patent it is necessary to include the relevant underlying data of an invention in the patent application that gets later published by the patent authorities. It therefore often is agreed upon that first the patent is to be filed, e.g., by the food company, then followed by related scientific publications, e.g., by the university research partners. Only minimal use of computer-generated data or artificial intelligence-based techniques was reported.

An open-data economy is not used in practice: Although a data sharing approach might sound very interesting, it, however, is currently not considered by the industry, at least not yet. Challenges are among others, *"How to get value out of it?*", and *"How to share but not to share with competitors?"* (interview partner) – the latter mainly with regard to antitrust law restrictions. Of course, there are areas where data is unlikely ever to be shared. Production operations data, which also contains know-how and do-how, is generally kept as a trade secret and deliberately not patented to avoid sharing of the information via the patent disclosure. Consumer research data and company data (such as strategy plans and privileged financial data) is not public, is not shared and is not patentable.

Trade secret protection on the context of shared data therefore seems only to be relevant for the intermediate and not published data sets of level two (see above) that are covered under the contractual agreement umbrella binding the consortium partners anyways.

5. Discussion

Our four cases suggest several themes: the first is value. We find that data value is dependent on the availability, quality, correlation, and causality of the data. As is consistent with the literature, trade secrets are a helpful tool but not a full solution. Data sharing is limited by the high costs to protect value, which means that much of the value from sharing data is not realised. Second comes the nature of the shared data at hand: Shared data that exhibits or incorporates know-how is more susceptible to trade secrets protection than data as such. Thirdly, trade secrets, through some of their features, may exhibit subtle challenges for IP management, where awareness of these challenges may need to be built with firms.

Fig. 1 provides a simplified, static model of what the decision making can be for the food and agriculture industries. From an IP managerial point of view the industry, along its value chain, seems to make a basic distinction whether commercially valuable data is supposed to be better kept secret or to be shared. Data that is not destined for sharing is treated as a trade secret. By contrast, data intended for sharing may be treated as a trade secret with the expectation contracts will be used. There is a trade-off between the benefits of protection provided by contracts and the high transaction costs associated with drafting often mostly individual/tailor-made contracts. Trade secrets underpin contracts as a protection measure and reduce the transaction costs.

While this model is simple, it indicates that firms may initially sort data into shared or not-shared paths. Three options, as per the Open Data Institute ODI [64], are available: closed (not shared), shared and open (which are both shared paths). Open Data is currently seen as a possible means to tackle upcoming global challenges to agricultural productivity, nutrition, and food security. The data is used to improve decision making, increase transparency and support innovation [65]. Therefore, the decision to use trade secrets as protection mechanism is related to the three options of the ODI. Together, the three options of the ODI form one dimension or spectrum that needs to be taken into consideration for decision making purposes. Closed data is very well susceptible to trade secret protection, with the decision to use or not to use this legal instrument depending on issues such as practicability or enforceability. At the other end of the spectrum, open data is not susceptible to trade secret protection, because fully open data cannot be confidential in the meaning of the legal definition of a trade secret. The

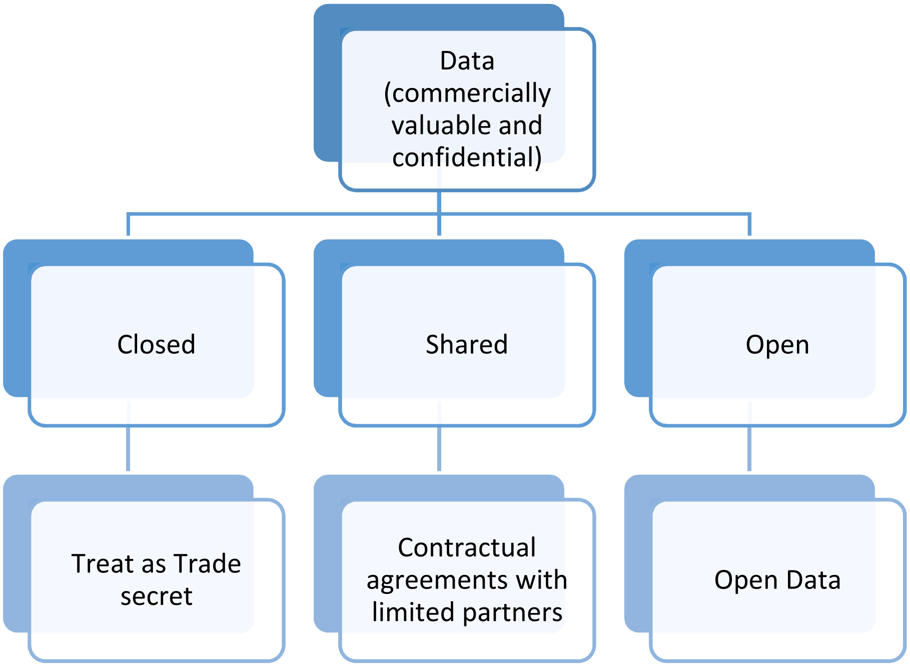

Data (commercially valuable and confidential)
Closed
Shared
Open
Treat as Trade secret
Contractual agreements with limited partners
Open Data

Fig. 1. Firm Data-Sharing Decision Tree
Based on ODI [64] ODI, The Data Spectrum, 2018. https://theodi.org/about-the-odi/the-data-spectrum/.
Source: authors, based on ODI, 2021.

question remains with respect to the shared ODI mode, whether trade can be seen as an incentive and/or conducive to sharing of agricultural data.[9]

To answer this question, we turn our attention to our first recurring theme in all four case studies, which is value. If we plot the degree of openness (as one decision dimension) against the dimension of value sharing as a second decision dimension, we obtain four quadrants which together form a value and data sharing matrix with four distinct types of data and trade-secret/IP appropriation strategies (see Fig. 2 and Fig. 3). Our horizontal axis builds on the ODI Data Spectrum [64], which places data, as said, on a range from closed to open. This economic role of value sharing forms our vertical axis. Finally, we identify the legal, contractual, and self-regulatory mechanisms that support value sharing in each quadrant.

All four of the quadrants are identified in our case studies. Quadrants I and II, both of which have closed regimes, are used by all our case studies, which is in keeping with firm's incentives to control value sharing. I and II are well supported by trade secret and contract law, in addition to mechanisms that ensure factual secrecy. Quadrants III and IV are less observed. Quadrant IV, which is truly open data, is dismissed by the industry, at least in our case study sample. Instead, as in Quadrant III, discussed by cases A, B, and D, firms want to share data but feel there is no support for value sharing.

Our study confirms trade secrets work for the closed, no sharing environment (Quadrant I), but on the other hand may be currently limited to that application. Trade secrets have a supportive role in closed environments with shared values (Quadrant II), e.g., the breach of contractual agreements. Contracts and trade secrets are mutually supportive; contracts build on trade secrets, and trade secrets are governed by contracts.

Firms treat different types of data differently. Our case studies demonstrate trade secrets are more likely to be used with know-how and do-how, potentially in combination with data. If the data is raw data ('data as such'), then trade secrets are viewed as less important as per our case studies – one issue seems to be that unprocessed data has lesser value than processed data. The processing steps of the data (software, algorithms) certainly qualify and are protected through trade secrets. There is a less clear direction on the outputs of the analysis of the raw data, where we can see in different industry segments also different approaches. Information to inform marketing and organisational innovations, such as market research or business strategy information, is also typically protected by trade secrets.

Fig. 4 expands on our simplified model in Fig. 1, of an agricultural firm's decision-making. Firms largely focus on choosing between closed and shared. However, we have noted a new space where firms would like to share both data and value, but currently lack the legal and managerial means to make it a viable option under commercial terms.

The decision to keep data secret is taken, e.g., for data production operations, consumer research data, company data like strategy plans and financial data (see case study D), particularly for data involving process know-how (case studies B and C).

We were surprised to find such limited evidence of open-data approaches to data sharing (quadrant IV). The exception was the discussion of open data approaches in the agricultural machinery case (case study B), which is in part influenced by the EU code of conduct and has in part a quasi-open-data approach. In this case, both raw and processed data are shared. The data itself is not the trade secret, but the processes to create/process it is. The EU code of conduct on agricultural data sharing may be at least in parts a model for other parts of the industry as regards elements of "open data"-style data sharing. To note, however, that the code of conduct is, first, rather new and second, its application is voluntary. There is a need to evaluate the application of this code in

[9] Generally, the most common barriers to the sharing and re-use of data identified by Center for Agriculture and Biosciences International (CABI) and the Open Data Institute (ODI), are: policy, data-sharing and access, data collection and stewarding, data-security and privacy, and trust [66] ODI, Case study enabling data access to support innovation in agriculture, 2021. https://theodi.org/article/case-study-enabling-data-access-to-support-innovation-in-agriculture/, [67], F. Smith, L. Dodds, C. Day, R. Musker, M. Parr, Creating FAIR and open data ecosystems for agricultural programmes, Gates Open Res 2 (42) (2018) 42. It can be seen that legal trade secret protection pertains to at least several of these barriers, e.g., trust or data-security, which means that trade secrets could, at least theoretically, tackle some of these barriers.

Value Sharing ↑		
Sharing	**(II) Closed data & shared value** *Value Shared-Closed* Contractual agreements to share confidential data/TS Cases: A, B, C, D Comments: Data in this quadrant is shared under a closed regime between parties. Our case studies indicate, particularly for market-dominating companies, this sharing may be limited by competition or anti-trust laws.	**(III) Open data & shared value** *Value Shared-Open* Data is open and value is (somehow) shared Cases: *aspiring* A, B, D Comments: This quadrant is where our case studies identified a lack of legal or other mechanisms to facilitate value sharing.
No Sharing	**(I) Closed data** *No Value Sharing-Closed* Data is kept by firm as legally and/or factually secret TS Cases: A, B, C, D Comments: Data includes business confidential data, trade secrets and data without value in the legal sense to qualify for trade secrecy.	**(IV) Open data** *No Value Sharing -Open* No exclusivity, mechanism for maintaining openness Cases: *Absent but observed in practice*[11] *and discussed in the literature* Comments: The value of Open Data, "better use of data helps small and medium farms improve their insight in the farming and market processes with a view to supporting competiveness and improving sustainability." (Precision Agriculture, p.53) Elements of open data can be found in the Codes of Conduct.
	Closed	Open

Data Sharing Regime →

Fig. 2. The Value and Data Sharing Matrix
Source: authors

Value Sharing ↑		
Sharing	**(II) Closed data & shared value** *"What can we share under what conditions?* (C) *"Our industry is still very protective – we want to have control about the data and its use"*(D)	**(III) Open data & shared value** *"It's a pity that we cannot offer our data to third parties…"* (A), as the industry lacks a procedure to share the benefits arising from sharing of this data *"…farmers and agri-businesses are more than willing to share data with each other and engage in a more open data mind-set. However, they will only do so if the potential benefits and risks are made clear and when they can trust that these are settled in a proper and fair way through contractual agreements."* (B)
No Sharing	**(I) Closed data** *"… crown jewels, of which there may not be that many, but it would really hurt if these secrets were to leak … "*(C) Types of closed data (D): secondary observations data, production operations data, consumer research data, and company data.	**(IV) Open data** Not considered by case study firms, e.g., discussion in (D) that the industry does not view it as viable option open, because, "How to get value out of it?" Partly discussed in case study B, too.
	Closed	Open

Data Sharing Regime →

Fig. 3. Examples of Quadrants from case studies.
Source: authors

practice after some time.

Data is shared when there is explicit need for it and a concrete, individual benefit (value) is expected, e.g., to create processed data from raw data the latter having a significantly higher value (quadrant II). That happens, e.g., by bilateral partnerships (see case study B, when farmers share data to detect patterns that can help optimise individual farms; or case study C, when the nature of the relationship with the client warrants sharing) or in multilateral consortiums (see case study D). However, before data sharing and processing, bilateral or multilateral agreements must be negotiated that typically regulate background and foreground knowledge, confidentiality and use and value sharing (the process has already been earlier described in literature [68]).

Third parties outside these agreements generally would not get access to the raw data sets (background) or to the processed data (foreground) – i.e., the open approaches of quadrants (III) and (IV) would not materialize. One can conclude the sharing parties keep treating raw and processed data as confidential and possibly as trade secrets (see case study D; this also applies to the situations described in case study C in the instances of second sourcing or particular client demands). Nevertheless, the parties might upfront agree to apply further protective means, e.g., patents, or subsequent value extractions, e.g., scientific publications (see case study D).

Moreover, an interesting 'bycatch' of the analysis is that there are also administrative management issues to consider. The fact that trade

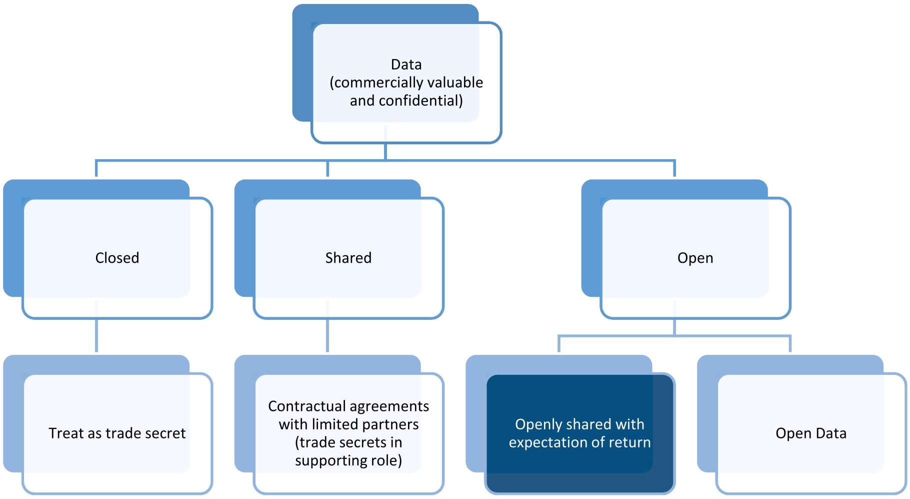


Fig. 4. Expanded firm data-sharing decision tree.
Source: Authors, based on ODI [66].

secrets have been historically a result of a mixture of many pieces of law has created (see case study C) a situation where many firms may have not acted yet on trade secrets. One reason is the lack of terms and deadlines to observe with trade secrets (as opposed to, e.g., patents) hereby not creating a sense of urgency. The topic is also fragmented with different aspects being dealt by different departments within the firm (and none taking the lead). There are considerable costs and efforts for identifying trade secrets and developing and maintaining adequate protection measures. Our analysis supports these considerations and complement other study results finding generally observe low awareness levels of the topic of IP, particularly with smaller firms [69]. Measures to raise awareness on this issue, as well as institutionalising clear ownership of trade secrets within the organisational structure of firms, should be considered good practice.

If a decision is taken to share data we argue, based on our evaluation of the agriculture value chain cases, that considerable segments of the industry have so far not yet developed a sustainable *open data* or open sharing model in practice – which is why our case studies are mostly found in quadrants (I) and (II). On the one hand that is possibly due to a cultural history, as reflected in the seminal quote that *"..our industry is still very protective – we want to have control about the data and its use"* (interview partner for food case study B). On the other hand, there seems to be a lack of a suitable and sustainable sharing model that works for the industry players along the value chain and that fulfils the understandable requirement of data sharers for practicable and executable value and benefit sharing: *"It's a pity that we cannot offer our data to third parties."* (see also case study A, or generally quadrant (III)).

On a theoretical level, it becomes clear that the results are in line with the resource-based view (RBV) in that the industry players regard data in agriculture as their resource, and the more valuable this resource is, the more there is the desire to keep control over it. Trade secrets may be one tool to achieve such control. When trade secrets are used, the legal requirements for trade secret protection align well with the theoretical foundations of the RBV, also in the respective scenarios for "shared" data. Our analysis therefore indicates that the theoretical discussion on the nature of digital assets and their competitive advantages in a resource-based view, as summarised and elaborated on in the literature review of Cuthbertson & Furseth [16], needs a more nuanced view regarding different types of data and algorithms – with distinctions in particular to be made between data that is trade-secret protected and not trade secret-protected, amongst others.

6. Conclusions

We asked two research questions. To answer the first, where we ask to what extent are trade secrets a viable tool to protect data (in particular data that is shared across organisations) in agriculture, we find an important but nuanced role of trade secrets in supporting agriculture firm's use and protection of (shared) data. The case studies we present confirm previous work [35] exploring the strategies firms adopt to appropriate the returns from their innovation. We find firms are reluctant to share data, despite the potential benefits. Trade secrets overcome some of this reluctance, but only when supported by contractual agreements with partners and non-IP mechanisms [44,45]. We also highlight the challenges of more open data approaches, as addressed by Permann & Schildt [55] or Richter & Slowinski [56]. However, the results also indicate that literature should take a closer and more differentiated view towards trade secret protection when sharing data, as there seem to be many specific set-ups where trade secrets are an enabler for data sharing and others where they are not. Eventually, the results also indicate a need in the theoretical discussion on the applicability of the resource-based view (RBV) to digital assets such as data and algorithms to differentiate more between different types of data/algorithms, in particular differentiating between trade-secret protected data and data not protected by trade secrets.

Our second research question was: What are major data sharing practices in agriculture? To answer this, we developed a typology of data sharing practices along the two dimensions of data value and degree of openness when/for sharing data. The case studies suggest that closed models are still somewhat preferred, and that fully open data approach have likely a long way to go. We further develop understandings of the barriers to sharing data when value sharing cannot be guaranteed, e.g., by van der Burg et al. [54]. We observe the agricultural industry is observing shared data economy models but has yet to find suitable business models that would satisfy the involved players along its industry value chain. One major reason is the lack of track-and-traceability of shared and used data, which results in insecurities about a fair value sharing. These imperfections have so far been overcome with lengthy and extensive bilateral or multilateral contractual agreements supported by trade secrecy, that generally limit sharing and using of data to the contractual parties.

For managers, our work points to an increasingly complex world of data management and sharing, in which trade secrets can serve as a mechanism to protect valuable data from misappropriation. While there is not a one-size-fits all approach to the use of trade secrets, our agriculture case studies suggest that data holds much potential value for firms and that trade secrets are but one weapon in the arsenal of IP protection. Good administrative practices involve awareness-raising on trade secrets with and in companies, as well as institutionalising clear ownership of the trade secrets topic within the firms.

Trade secrets remain an under-researched area in IP management and an increasing area of interest in data. Empirical analysis, such as ours, is relatively sparse. We have only looked at the agricultural industry, and there is research emanating also specifically on the use of trade secrets in other industries [70]. There is hence scope to assess differences between agriculture and other industries in a more thorough manner in future research. Having said that, limitations of case study research apply even in the industry-specific setting of this paper. The core tensions limiting the use of trade secrets and the sharing of data are not unique to the agriculture industry. There is a need for further evidence, also to be able to triangulate the findings better, in the respectively analysed segments of the agricultural value chain. Here, further survey and interview-based studies, but also additional case studies, could prove helpful to increase the evidence base. While we covered major parts of the agricultural value chain, analysis of the later parts of the value chain may uncover further insights.

Authorship statement

Alfred Radauer: conceptualisation, investigation, formal analysis, writing – original draft, writing – review & editing, supervision, Nicola Searle: conceptualisation, formal analysis, writing – original draft, writing – review & editing, visualisation, Martin A. Bader: conceptualisation, investigation, formal analysis, writing – original draft, writing – review & editing, visualisation.

Statements

All persons who meet authorship criteria are listed as authors, and all authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted or published in any other publication before its appearance in World Patent Information.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Alfred Radauer reports a relationship with European Commission that includes: consulting or advisory. Martin Bader reports a relationship with European Commission that includes: consulting or advisory. Nicola Searle reports a relationship with European Commission that includes: consulting or advisory.

Acknowledgements

All persons who have made substantial contributions to the work reported in the manuscript (e.g., technical help, writing and editing assistance, general support), but who do not meet the criteria for authorship. are named in the Acknowledgements and have given us their written permission to be named. If we have not included an Acknowledgements, then that indicates that we have not received substantial contributions from non-authors.

Appendix

Interview Guide Outline.

1. Demographic information
2. Familiarity with data sharing and trade secrets
3. Use, motives and barriers to data sharing
4. Identifying the types of data shared (e.g., personal, commercial, machine-generated)
5. Situations in which the firm shares or does not share data
6. Processes to identify valuable data assets
7. Steps taken to protect data
8. Conditions of data sharing (e.g., contracts, business relationships)
9. Sharing of data across jurisdictions (e.g., international data flow)
10. Open question (opportunity for interviewee to address any topics not discussed)

References

[1] R. Abbasi, P. Martinez, R. Ahmad, The digitization of agricultural industry – a systematic literature review on agriculture 4.0, Smart Agricult. Technol. 2 (2022), 100042.

[2] L. Klerkx, E. Jakku, P. Labarthe, A review of social science on digital agriculture, smart farming and agriculture 4.0: new contributions and a future research agenda, NJAS - Wageningen J. Life Sci. 90 (2019), 100315.

[3] BASF, Food Value Chain Collaborations for Smarter Crop Protection, 2021. https://agriculture.basf.com/global/en/business-areas/crop-protection-and-seeds/services/food-value-chain.html. (Accessed 31 October 2021).

[4] FAO, Developing sustainable food value chains – Guiding Principles. https://www.fao.org/3/i3953e/i3953e.pdf, 2014.

[5] M. Leistner, L. Antoine, IPR and the Use of Open Data and Data Sharing Initiatives by Public and Private Actors, Study Commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the Request of the Committee on Legal Affairs, 2022.

[6] L. Wiseman, J. Sanderson, A. Zhang, E. Jakku, Farmers and their data: an examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming, NJAS - Wageningen J. Life Sci. 90–91 (2019), 100301.

[7] J. Pooley, Secrets: Managing Information Assets in the Age of Cyberespionage, Verus Press, 2015.

[8] D.D. Friedman, W.M. Landes, R.A. Posner, Some economics of trade secret law, J. Econ. Perspect. 5 (1) (1991) 61–72.

[9] D.J. Teece, Profiting from technological innovation: implications for integration, collaboration, licensing and public policy, Res. Pol. 15 (6) (1986) 285–305.

[10] I.P.L. Png, Secrecy and patents: theory and evidence from the uniform trade secrets act, Strat. Sci. 2 (3) (2017) 176–193.

[11] OECD, Economic and social benefits of data access and sharing. https://www.oecd-ilibrary.org/sites/90ebc73d-en/index.html?itemId=/content/component/90ebc73d-en, 2014.

[12] M. Holgersson, Patent management in entrepreneurial SMEs: a literature review and an empirical study of innovation appropriation, patent propensity, and motives, R&d Manage. 43 (1) (2013) 21–36.

[13] M.A. Bader, An introduction to intellectual property rights and formal and informal protection strategies, in: M. M.S, S. Bader (Eds.), Intellectual Property Management for Start-Ups – Value-Enhancing Approaches and and Practices for Leveraging the Potential, Springer Nature, 2023.

[14] A. Bonakdar, K. Frankenberger, M.A. Bader, O. Gassmann, Capturing value from business models: the role of formal and informal protection strategies, Int. J. Technol. Manag. 73 (4) (2017) 151–175.

[15] O. Gassmann, M.A. Bader, M.J. Thompson, Patent Management: Protecting Intellectual Property and Innovation, Springer, 2021.

[16] R. Cuthbertson, P. Furseth, Digital services and competitive advantage: strengthening the links between RBV, KBV, and innovation, J. Bus. Res. 152 (2022) 168–176.

[17] S. Broring, Developing innovation strategies for convergence-Is' open innovation'imperative? Int. J. Technol. Manag. 49 (1) (2010) 272.

[18] M.S. Clancy, G. Moschini, Intellectual property rights and the ascent of proprietary innovation in agriculture, Ann. Rev. Res. Econ. 9 (2017) 53–74.

[19] J.H. Reichman, P. Samuelson, Intellectual property rights in data, Va. Law Rev. 50 (1997) 49.

[20] E. Derclaye, Database Rights: Success or Failure? the Chequered yet Exciting Journey of Database Protection in Europe, Constructing European Intellectual Property, Edward Elgar Publishing, 2013, pp. 340–354.

[21] M. Koščík, M. Myška, Database authorship and ownership of sui generis database rights in data-driven research, International Review of Law, Comput. Technol. 31 (1) (2017) 43–67.

[22] K.J. Arrow, Economic Welfare and the Allocation of Resources for Invention, the Rate and Direction of Inventive Activity, Princeton University Press, Princeton, 1962, pp. 609–626.

[23] N. Searle, The Economic and Innovation Impacts of Trade Secrets, UK Intellectual Property Office Research Paper, 2021, 2021/01.

[24] J. Sadowski, When data is capital: datafication, accumulation, and extraction, Big Data Soc. 6 (1) (2019), 2053951718820549.

[25] D.S. Levine, T. Sichelman, Why do startups use trade secrets, Notre Dame Law Rev. 94 (2018) 751.

[26] A. Arora, S. Athreye, C. Huang, The paradox of openness revisited: collaborative innovation and patenting by UK innovators, Res. Pol. 45 (7) (2016) 1352–1361.

[27] N. Wajsman, F. García-Valero, Protecting Innovation through Trade Secrets and Patents: Determinants for european union Firms, European Union Intellectual Property Office, 2017.

[28] A. Arundel, I. Kabla, What percentage of innovations are patented? empirical estimates for European firms, Res. Pol. 27 (2) (1998) 127–141.

[29] W.M. Cohen, R.R. Nelson, J.P. Walsh, Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (Or Not), National Bureau of Economic Research Working Paper Series, 2000. No. 7552.

[30] O. Granstrand, The Economics and Management of Intellectual Property, Books, 1999, p. 1651.

[31] M.A. Klein, Secrecy, the patent puzzle and endogenous growth, Eur. Econ. Rev. 126 (2020), 103445.

[32] I. Kwon, Patent races with secrecy, J. Ind. Econ. 60 (3) (2012) 499–516.

[33] N. Dass, V. Nanda, H.D. Park, S.C. Xiao, Intellectual property protection and financial markets: patenting versus secrecy, Rev. Finance 25 (3) (2020) 669–711.

[34] D.S. Almeling, Seven Reasons Why Trade Secrets Are Increasingly Important, 2012.

[35] E.-P. Gallié, D. Legros, French firms' strategies for protecting their intellectual property, Res. Pol. 41 (4) (2012) 780–794.

[36] Y.-C. Chang, J.D. Linton, M.-N. Chen, Service regime: an empirical analysis of innovation patterns in service firms, Technol. Forecast. Soc. Change 79 (9) (2012) 1569–1582.

[37] A. Leiponen, J. Byma, If you cannot block, you better run: small firms, cooperative innovation, and appropriation strategies, Res. Pol. 38 (9) (2009) 1478–1488.

[38] K. Beukel, B. Tyler, E.M.G. Fernandez, A.D. Cruz, B. Lahneman, PROACTIVENESS AND THE USE OF SECRECY IN FAMILY AND NONFAMILY SMES: EVIDENCE FROM THE WINE INDUSTRY, 2018.

[39] R. Wang, Information asymmetry and the inefficiency of informal ip strategies within employment relationships, Technol. Forecast. Soc. Change 162 (2021), 120335.

[40] A.W. King, Disentangling interfirm and intrafirm causal ambiguity: a conceptual model of causal ambiguity and sustainable competitive advantage, Acad. Manag. Rev. 32 (1) (2007) 156–178.

[41] P. Ritala, H. Olander, S. Michailova, K. Husted, Knowledge sharing, knowledge leaking and relative innovation performance: an empirical study, Technovation 35 (2015) 22–31.

[42] S.D. James, M.J. Leiblein, S. Lu, How firms capture value from their innovations, J. Manag. 39 (5) (2013) 1123–1155.

[43] M.M. Appleyard, How does knowledge flow? Interfirm patterns in the semiconductor industry, Strat. Manag. J. 17 (1996) 137–154.

[44] S.L. Ferrell, Legal issues on the farm data frontier, Part I: managing first-degree relationships in farm data transfers, Drake J. Agric. Law 21 (2016) 13.

[45] A. Azevedo, P.J. Pereira, A. Rodrigues, Non-compete covenants, litigation and garden leaves, J. Bus. Res. 88 (2018) 197–211.

[46] S.K. Sandeen, T. Aplin, Trade Secrecy, Factual Secrecy and the Hype Surrounding AI, Research Handbook on Intellectual Property and Artificial Intelligence, Edward Elgar Publishing, 2022, pp. 443–460.

[47] O.K. Foundation, Open Definition, 2021. https://opendefinition.org/. (Accessed 31 October 2021).

[48] OECD, Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, 2019.

[49] A. Zaheer, B. McEvily, V. Perrone, Does trust matter? Exploring the effects of inter-organizational and inter-personal trust on performance, Organ. Sci. 9 (1998) 141–159.

[50] D. Gambetta, Can we trust trust, Trust: Making and breaking cooperative relations 13 (2000) 213–237, 2000.

[51] M. Blakeney, J.I. Cohen, S. Crespi, 18 intellectual property rights and agricultural biotechnology, in: Managing agricultural biotechnology: addressing research program needs and policy implications, 1999, p. 209, 23.

[52] A. Ellixson, T.W. Griffin, S. Ferrell, P. Goeringer, Legal and economic implications of farm data: ownership and possible protections, Drake J. Agric. Law 24 (2019) 49.

[53] Copa-Cogeca, EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement, 2020. https://cema-agri.org/images/publications/brochures/EU_Code_of_conduct_on_agricultural_data_sharing_by_contractual_agreement_2020_ENGLISH.pdf. (Accessed 31 October 2021).

[54] S. van der Burg, L. Wiseman, J. Krkeljas, Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing, Ethics Inf. Technol. 23 (3) (2021) 185–198.

[55] M. Perkmann, H. Schildt, Open data partnerships between firms and universities: the role of boundary organizations, Res. Pol. 44 (5) (2015) 1133–1143.

[56] H. Richter, P.R. Slowinski, The data sharing economy: on the emergence of new intermediaries, IIC - Int. Rev. Intellect. Property and Competition Law 50 (1) (2019) 4–29.

[57] J. Dodds, A. Krattiger, The Statutory Toolbox: an Introduction, Intellectual Property Management in Health and Agricultural Innovation: a Handbook of Best Practices, vols. 1 and 2, 2007, pp. 337–350.

[58] K.F. Jorda, Trade Secrets and Trade-Secret Licensing, Intellectual Property Management in Health and Agricultural Innovation: a Handbook of Best Practices, vols. 1 and 2, 2007, pp. 1043–1057.

[59] A. Krattiger, R.T. Mahoney, L. Nelsen, J.A. Thomson, A.B. Bennett, K. Satyanarayana, G.D. Graff, C. Fernandez, S. Kowalski, Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practices, vol. 1, 2007.

[60] S. Ebneyamini, M.R. Sadeghi Moghadam, Toward developing a framework for conducting case study research, Int. J. Qual. Methods 17 (1) (2018), 1609406918817954.

[61] M.B. Miles, Qualitative data as an attractive nuisance: the problem of analysis, Adm. Sci. Q. 24 (4) (1979) 590–601.

[62] R. Yin, The SAGE Handbook of Applied Social Research Methods, SAGE Publications, Inc., Thousand Oaks Thousand Oaks, California, 2009.

[63] S.o.t.C.o.B, Diversity, Convention on Biological Diversity, 1993. (Accessed 31 October 2021).

[64] ODI, The data spectrum. https://theodi.org/about-the-odi/the-data-spectrum/, 2018.

[65] GODAN, About godan. https://www.godan.info/godan-action/about, 2021.

[66] ODI, Case study enabling data access to support innovation in agriculture. https://theodi.org/article/case-study-enabling-data-access-to-support-innovation-in-agriculture/, 2021.

[67] F. Smith, L. Dodds, C. Day, R. Musker, M. Parr, Creating FAIR and open data ecosystems for agricultural programmes, Gates Open Res. 2 (42) (2018) 42.

[68] M.A. Bader, Intellectual Property Management in R&D Collaborations : the Case of the Service Industry, Physica-Verlag, Heidelberg, 2006.

[69] A. Radauer, L. Walter, Elements of good practice for providers of publicly funded patent information services for SMEs–Selected and amended results of a benchmarking exercise, World Patent Inf. 32 (3) (2010) 237–245.

[70] A. Radauer, M. Bader, T. Aplin, U. Konopka, N. Searle, R. Altenburger, C. Bachner, Study on the Legal Protection of Trade Secrets in the Context of the Data Economy, 2022.

Alfred Radauer is Head of the Institute for Business Administration and Management at the IMC University of Applied Sciences, Krems. His research interests lie in innovation, IP, standardisation and SMEs. Within these topics, he focusses on applied issues in funded as well as contract research in the fields of innovation policy and management, IP policy, IP management and standardisation.

Dr. Nicola Searle is an EPSRC Digital Economy Fellow and Senior Lecturer at ICCE. An economist who specialises in the economics of intellectual property and the creative industries, Nicola joined ICCE in 2015. Dr. Searle is a member of the RCUK Digital Economy Programme Advisory Board, a member of the UK Intellectual Property Office's (IPO) Research Experts Advisory Group and an Honorary Research Fellow at the School of Management, University of St Andrews.

Martin A. Bader is a European and Swiss Patent Attorney. As well as being Partner and Co-Founder of the specialized innovation and intellectual property management advisory group BGW AG St. Gallen, he is Professor for Technology Management and Entrepreneurship at the University of Applied Sciences Ingolstadt (THI). Previously, he was Vice President and Chief Intellectual Property Officer at Infineon Technologies, Munich, incl. its IPO, and Head of the Intellectual Property Management Competence Center at the Institute of Technology Management at the University of St. Gallen (HSG). He is a mediator at the Mediation Center for Alternative Dispute Resolution at the World Intellectual Property Organization (WIPO) and has for many years been regarded as being among the top 300 intellectual property strategists worldwide according to the Intellectual Asset Management magazine's IAM strategy 300 index.