LEGAL AND ECONOMIC IMPLICATIONS OF FARM DATA: OWNERSHIP AND POSSIBLE PROTECTIONS

Ashley Ellixson†, Terry W. Griffin††, Shannon Ferrell†††, and Paul Goeringer††††

† Ashley Ellixson (aellixson@udaz.org) is VP of Legal and Environmental Affairs, United Dairymen of Arizona, Tempe, Arizona.

†† Terry W. Griffin (twgriffin@ksu.edu) is Associate Professor, Department of Agricultural Economics, Kansas State University, Manhattan, Kansas.

††† Shannon Ferrell (shannon.l.ferrell@oklstate.edu) is Professor, Department of Agricultural Economics, Oklahoma State University, Stillwater Oklahoma.

†††† Paul Goeringer (lgoering@umd.edu) is Senior Faculty Specialist and Extension Legal Specialist, Department of Agricultural and Resource Economics, University of Maryland, College Park, Maryland.

ABSTRACT

Farmers' ability to "own" data has been debated, along with its value and consequences of misappropriation. Although no specific law or precedent addresses farm data, it may be protectable as a "trade secret" if farmers actively protect it. Questions remain if seeking protection is practical or if highest value may be realized by sharing data.

ACKNOWLEDGEMENTS

We appreciate informal reviews and editorial comments by Jacob Maurer, Noah Miller, Jayce Stabel, and Debbie Haugan. We appreciate constructive criticisms from participants of the 2016 International Conference on Precision Agriculture, as well as numerous Extension meetings across the United States.

DISCLAIMER

In many cases, the potential uses of data generated by farm equipment or created through the activities of a technology service provider will be governed by a service contract. Farmers should read such service contracts carefully before entering them and seek the assistance of a licensed attorney if needed. An attorney consulting with a client on a misappropriation of data case will need to carefully consider all the differences between the Uniform Trade Secrets Act, other state laws, and the federal Defend Trade Secrets Act. Whether to pursue the lawsuit at the state level or the federal level will be decided by specific facts, and an experienced attorney will be able to guide the farmer as to which method is best for a particular situation.

I. INTRODUCTION

Continuing advancements in data acquisition, transmission, and storage technologies deployed on farms have enabled the agricultural industry to generate large volumes of site-specific and farm-level data that may be stored digitally on online servers. When aggregated over thousands of farms, this data may prove to be very useful to the agricultural industry, but due to limited high-quality broadband access and farmers still using outdated equipment, adoption of such a system has been slow.[1] When analyzed and interpreted, this data can help farms, businesses, researchers, and governments address local, national, and global

1. KEITH COBLE ET AL., MISS. SOYBEAN PROMOTION BD., ADVANCING U.S. AGRICULTURAL COMPETITIVENESS WITH BIG DATA AND AGRICULTURAL ECONOMIC MARKET INFORMATION, ANALYSIS, AND RESEARCH EXECUTIVE SUMMARY, https://perma.cc/AZ3H-TSKR.

issues. Substantial value in farm data is expected at the aggregate level, although uncertainty exists as to how much value data may have at the farm level.[2] The potential value farms receive from farm data may depend upon farmers' ability to maintain exclusivity of that data.

The ability to maintain exclusivity with respect to access of a resource such as farm data typically derives from property law and the rights given to owners of a resource. Most current intellectual property laws do not adequately address resources such as farm data. This Article highlights portions of the current intellectual property framework relevant to farm data and shows that applying existing laws to farm data often provides farmers with unworkable solutions. Trade secret protections may be one answer if farmers wish to maintain exclusive access to data from their farm, but only if farmers actively protect data as a secret.[3] If farmers wish to use the trade secret approach to claim exclusive rights to use data, their argument rests on the idea that farm data is a type of intellectual property that provides a competitive advantage to the farm business that has access to it.[4] The successful application of trade secret law to farm data would provide a measure of protection to farmers by offering them special legal remedies in the event data were misappropriated.[5] Specifically, any unauthorized use of data would give farmers the right to recover damages in court if their argument holds.[6]

II. BACKGROUND ON FARM DATA AND CURRENT ISSUES

Big Data in agriculture refers to aggregated farm data assimilated from numerous farming operations into a single database or repository.[7] For example, corn growers may collect site-specific geospatial and metadata (information that describes, explains, or locates data to make it easier to retrieve, use, or manage) across many acres.[8] On the small data or farm scale data, site-specific geospatial

2. *Id.* at 8.

3. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).

4. *Id.*

5. Ashley Ellixson et al., 13th INT'L CONFERENCE ON PRECISION AGRIC., *Ownership and Protections of Farm Data* 5, (2016), https://ispag. org/proceedings/?action= abstract&id=2141 &search=authors.

6. *Id.* at 5.

7. Keith H. Coble et al., *Big Data in Agriculture: A Challenge for the Future*, 40 APPLIED ECONO. PERSP. & POL'Y 79 (2018); Otto C. Doering et al., *Agricultural Conservation & Environmental Programs: The Challenge of Data-Driven Conservation*, CHOICES (2013), https://perma.cc/6DDX-SYTP; Terry W. Griffin et al., *Big Data Considerations for Rural Property Professionals*, J. AM. SOC'Y FARM MANAGERS & RURAL APPRAISERS 167 (2016); Brian E. Whitacre et al., *How Connected Are Our Farms?*, CHOICES (2014), https://perma.cc/JF75-TBPC.

8. *See* Coble et al., *supra* note 7, at 79.

data may include soil nutrient information, as-applied seeding rates, and yield monitor data.[9] Metadata may include the number of acres, and when, where, and which inputs were applied and cultivars planted.

Agribusiness and technology firms have invested billions of dollars in acquiring and developing farm data aggregation and analysis systems.[10] This level of investment demonstrates these companies' belief that aggregated farm data hold significant value. Many farmers have taken note of this, and wonder not only how they can capture the value of the data they generate for themselves, but also what value they may be losing through the sharing of data.

Farmers may be justified in their concerns about what protections are available for their data, particularly with respect to what legal protections exist. Courts often struggle in applying existing laws and previous rulings to modern technology, and the case of farm data is no exception. For example, Vacek argued that current laws provide limited protections to privacy from remote sensing drones.[11] States have also struggled with access to social media and other digital accounts (which include accounts that could be used to store and share farm data) upon a person's death when the terms of service may limit access to only the original user.[12] As of 2018, no existing laws address farm data ownership or implications of misappropriation of that data.[13] However, in the long run, case law and/or federal legislation are likely to be the deciding factor in determining the rights and protections associated with farm data. Alternatively, state legislatures may help by clearly defining rules to guide courts in handling new technology.[14]

9. Griffin et al., *supra* note 7, at 167.

10. JONATHAN DYER, THE DATA FARM: AN INVESTIGATION OF THE IMPLICATIONS OF COLLECTING DATA ON THE FARM 16 (Sept. 2016), https://www.researchgate.net/profile/Dickson_Adom/post/What_can_be_some_aplications_of_big_data_analysis_to_Farmers_decision_making/attachment/5aa0d0e5b53d2f0bba56a5f7/AS%3A601787283288067%401520488677794/download/1476921199JonathanDyerReportFINAL.pdf; Bruce Upbin, *Monsanto Buys Climate Corp For $930 Million,* FORBES (Oct. 2, 2013), https://perma.cc/34WN-W67Q.

11. *See* Joseph J. Vacek, *Remote Sensing of Private Data By Drones Is Most Likely Unregulated: Reasonable Expectations of Privacy Are At Risk Absent Comprehensive Federal Legislation* 90 N.D. L. REV. 463, 467 (2014).

12. Kristina Sherry, *What Happens to Our Facebook Accounts When We Die?: Probate Versus Policy and the Fate of Social-Media Assets Postmortem*, 40 PEPP. L. REV.185, 192-93 (2012).

13. Allison Wilton, *Farm Data Privacy Issues: Legal Aspects and Data Trespass*, Presentation to Kan. Agric. Tech. & Research Conference (Jan. 19, 2018).

14. Ashley Ellixson, *Lawsuit Challenging Wyoming's Data Trespassing Law Filed in Federal District Court*, MD RISK MGMT. EDUC. BLOG (Oct. 13, 2015), https://perma.cc/LHP9-3WBP; PAUL GOERINGER ET AL., PRIVACY ISSUES AND THE USE OF SUAS/DRONES IN MARYLAND, UNIV. OF MD. (Nov. 2015), https://perma.cc/6GWC-SGYL.

III. TYPES OF FARM DATA

Farm data can be assigned to one of at least three distinct categories. These different categories of farm data must be defined before discussing pertinent legal or economic aspects; and can be distinguished as (1) data deliberately collected for the farm by the farm, (2) data collected by a second party at the request of the farmer, and (3) data collected about the farm by an outside party. Although these are typically lumped together in general discussions on the topic, the majority of the debate arises from the first type, although considerable deliberation surrounds the remaining two.

A. Farm Data Collected by the Farm for the Farm

Farmers deliberately collect agronomic and economic data regarding farming practices and productivity. Substantial proportions of farmers invest financial capital and, more importantly, human capital into collection of geospatial or precision agricultural data such as yield monitor, soil sampling, and as-applied data.[15] Financial and production data at the enterprise and farm levels also fall under this category.[16]

B. Data Collected by a Second Party at the Request of the Farmer

The second type of farm data comprises data collected by someone other than the farmer. Although not as heavily debated as the first category, considerable interest exists in this data, especially as contracts with service providers such as agricultural retailers are examined and knowledge of telematics increases. Such data can also be classified into two subcategories: data collected by service providers, and data collected by equipment manufacturers via telematics.

Some outside parties, such as crop consultants, may be engaged specifically to collect data. For example, a crop consultant may collect soil-sample data as part of services offered by an agricultural retailer. In this case the service provider enjoys the initial access to the data and potential insight into soil fertility levels across acreages larger than any individual farm. In other instances, custom operators such as harvesters, planting, and pesticide applicators may collect data about a farm simply as a result of providing their services. 80% of service providers

15. Terry Griffin et al., *Farm's Sequence of Adoption of Information-Intensive Precision Agricultural Technology*, 33 APPLIED ENGINEERING AGRIC. 521 (2017); DAVID SCHIMMELPFENNIG, ECON. RESEARCH SERV., FARM PROFITS AND ADOPTION OF PRECISION AGRICULTURE(Oct. 2016), https://perma.cc/UF4C-K7LV.

16. Brady Brewer & Allen M. Featherstone, *Agency Cost of Debt: Evidence from Kansas Farm Operations*, 77 AGRIC. FIN. REV. 111, 112-14 (2017); TERRY GRIFFIN ET AL, ECONOMICS OF PRECISION FARMING (D.K. Shannon et al. eds., 2018).

offer variable rate fertilizer application,[17] the type of data that a service provider could retain in addition to potentially providing a copy to the famer or landowner. Such data retention could be intentional as part of a data collection, management, and analysis program; however, it could be unintentional simply as a result of a failure to clear the memory of the equipment used for the service. Other unintentional data from the farmers' perspectives is machinery diagnostic collected by equipment manufacturers. In either case, though, another party has a copy of data relevant to the farm.

The collection of data by equipment manufactures is largely automated and occurs in the background of many agricultural operations, many times without the notice of the farmer. Since 2011, many tractors and combine harvesters have wirelessly transmitted farm equipment data to manufacturers of the equipment,[18] including a host of parameters about the equipment's engine operation, fuel consumption, and location. Using the same technology, data on equipment field efficiency and performance rates such as how many acres can be planted per hour,[19] can be transmitted to manufacturers or their partners as well.

C. Data Collected about the Farm by an Outside Party

Substantial amounts of information regarding a farm could be collected from publicly available sources, such as satellite and aerial imagery. Even using free tools, such as Google Earth, combined with readily available public-domain data, one can derive or infer information about a farm's planted or harvested acreages, crop mix, livestock stocking rates, and a host of other parameters. Historically, such data has been provided specifically to benefit public institutions and to afford farmers access to tools (such as aerial imagery) that were prohibitively expensive in many cases.

Continuing with the example of aerial imagery, advancements in unmanned aerial systems (UAS, often called "drones" in the popular press) have increased interest in remotely sensed imagery. While farmers can certainly purchase a UAS to image their farm, other parties could use a UAS to collect data about the farm without even flying over it. In such a case, the data was collected without the request or consent of the farmer but potentially violated no law.

One example of federal legislation protects farm-level geospatial data. Specifically, with the enactment Section 1619 of the 2008 Farm Bill, the United States Department of Agriculture (USDA) Farm Service Agency (FSA) was no

17. BRUCE ERICKSON ET AL., PURDUE UNIV., 2017 PRECISION AGRICULTURE DEALERSHIP SURVEY (2017), https://perma.cc/ZG7Q-V892.

18. DYER, *supra* note 10, at 19.

19. GRIFFIN ET AL., *supra* note 16, at 223-24.

longer allowed to make available to the public geospatial data, including the Common Land Unit (CLU) records.[20]

Aerial and satellite imagery are an example of data derived from direct observation of a farm using a sensor system. Many forms of economic data are also publicly available or can be derived from data about the farm (or the farmer) without the farmer's request or consent. Freedom of Information Act (FOIA) requests can be made to determine the amount of publicly funded payments a farm receives.[21] The three major credit-reporting services collect data about credit and account balances to derive a credit score often used by lenders to make credit decisions for the farmer.[22] To carry the example a bit further, an individual has a right to access their credit report once per year (i.e. to access the data from which their credit score is derived), but does not have a right to their credit score (i.e. to access the results of a third party's analysis of the underlying data).

IV. LEGAL ASPECTS OF FARM DATA

It is useful, as a first step in discussing data ownership, to consider what it means to own something. Legally, ownership provides the right to (1) possess – physically occupy or have access to the property; (2) use – interact with and/or alter the property; (3) enjoy – receive the economic benefits from use of the property; (4) exclude – to prevent the possession of the property by another property; (5) transfer – to sell, give, or transfer at death the property; and (6) consume or destroy – to "use up" or annihilate the property.[23]

When considering ownership of an intangible asset such as farm data, the rights and responsibilities of the parties are less clear. While one can easily imagine concepts, such as exclude and consume with a physical asset such as a bushel of grain, ownership of farm data should be considered in terms of rights and responsibilities of the parties with access to the data. Two of the above rights are particularly problematic when discussing intangible farm data, specifically the right to exclude and consume. It has already been shown that excluding others from enjoying data is not possible once data is shared in a community or with another party. It is unlikely that farm data would not be shared with a group consisting of, at the very least, the farmer, landowner, and service provider. Consumption of farm

20. 7 U.S.C. §8791(b)(2) (2018).

21. *Subsidy Database Back, Bigger than Ever*, FARM FUTURES (June 12, 2007), https://perma.cc/M747-KQDB.

22. Ashley Ellixson, *Protecting Your Farm Data: Non-Disclosure Agreements*, MD RISK MGMT. EDUC. BLOG (June 7, 2016), https://perma.cc/Q8JS-VE7R; *What is a FICO Score*? CONSUMER FIN. PROTECTION. BUREAU (June 13, 2016), https://perma.cc/B6CW-5835.

23. Anna di Robilant, *Property: A Bundle Of Sticks Or A Tree?*, 68 VAND. L. REV. 869, 879 (2013).

data does not destroy that intangible good, and more to the point, digital data is difficult if not impossible to completely destroy (i.e. no copies exist anywhere). Individual deletion of data files is possible, but digital data almost always exists as multiple copies in multiple locations that an individual may or may not have access to, nor know of its existence.

Property is only able to be owned to the extent the law will recognize and enforce ownership rights, and typically, the type of property determines the associated rights and responsibilities. In the case of farm data, no legal classification has yet been provided. Convincing arguments can be made that farm data would not be recognized as subject to ownership under the three federally legislated areas of trademark, patent, or copyright law.[24]

A. Can Farm Data be Protected as a Trade Secret?

With trademark, patent, and copyright out of the running, the remaining theory available for protecting ownership of farm data requires proving the data is properly classified as a trade secret.

The Uniform Trade Secrets Act (UTSA) provides a relatively consistent legal framework to better protect trade secrets for U.S. companies operating in multiple states. UTSA has been adopted in forty-eight states, with New York and North Carolina as the remaining states not adopting the act.[25] Under UTSA, a trade secret must meet the following three conditions:

> 1. It must consist of information, including a formula, pattern, compilation, program, device, method, technique, or process;
> 2. It must derive independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and
> 3. It must be the subject of efforts that are fair, proper, or moderate under the circumstances to maintain its secrecy.[26]

24. *See* Shannon L. Ferrell, *Legal Issues on the Farm Data Frontier, Part I: Managing First-Degree Relationships in Farm Data Transfers*, 21 DRAKE J. AGRIC. L. 13, 27-41 (2016).

25. *Trade Secrets Act,* UNIFORM L. COMMISSION, https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 (last visited Apr. 17, 2019).

26. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985); *Trade Secrets Laws & the UTSA: 50 State &Federal Law Survey*, BEEK, REED, & RIDEN, https://perma.cc/Y5PQ-TSLR (archived Apr. 17, 2019).

Could farm data be considered a trade secret under these three conditions? Consider the application of these conditions to the farm data used to grow and harvest a corn crop.

1. Is the manner and strategy in planting, harvesting, and otherwise cultivating corn a formula or pattern?

Arguably, yes, they are. The data collected over many years and fields of crop rotations, applied input products and rates, timing of applications, and equipment settings collectively becomes a holistic pattern that may not be readily observed without advanced analyses. Taken together, a strong argument can be made that these elements constitute a business process, and business processes are routinely recognized as protectable trade secrets.[27]

2. Does growing corn in this manner derive economic value from not being generally known?

In good years, absolutely. It is generally accepted that a farmer's specific process for growing and raising corn is based in part on experience (i.e. data) from previous years (soil conditions, fertilizer use, irrigation practices, etc.) that is "generally not known or readily ascertainable" to other people in or outside of the industry.[28] This knowledge can increase production and/or improve efficiencies, thus providing economic value to the farmer although profits will approach $0 in the long run. However, showing that data has value is a necessary but insufficient condition for satisfying this element of the UTSA. Rather, one must show that the data "derive independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use."[29] Put another way: is farm data from a farmer's field more valuable because other farmers don't know it?

On one hand, if a farmer has discovered a truly unique way to grow corn with fewer inputs or to drive yields upward, he or she could capture additional profit in the short run that would not be available if all other producers knew it. Conversely, if other farmers could get access to data to show that the farmer was underperforming on a crop share lease, they might be able to bid leased land resources away from the farmer. Thus, one could argue data from a farm does have value from being secret.

27. MELVIN F. JAGER, TRADE SECRETS LAW Vol. 1, § 2:3 (2018).
28. 18 U.S.C. § 1839 (2018).
29. *Id.*

On the other hand, though, one could argue that anything done in corn production is a mere variation on farm processes that are subject to significant research and examination available in the public domain and thus are "readily ascertainable."[30] This argument relies upon the notion that the practices, including inputs, rates of inputs, and timing are well known and publicly available via Land Grant System and Extension services. The courts have recognized that where information is publicly available in other formats (e.g. an individual's address and contact information in a phone book), the data is not protected by trade secret law because that data is "readily ascertainable".[31] Consider a public database that contains information on dairy cow genetics—this information would not be considered a trade secret, nor protected as such, because of the ease by which it can be ascertained. The increasing proliferation of data in different forms has become a focal point where current law needs improvement.

One could also argue that farm-specific data are just that: specific to the farm. The extension of this argument is that the data does not have economic value to another individual producers (though the value of aggregated data is discussed below) because it is essentially meaningless when applied to a farm with different soil types, hydrologic conditions, micro-climate considerations, and so on. While it might provide some general information to another individual producer, it would quickly lose most, if not all value if the owner tried to apply the information to his or her own farm. Put another way, the owner's manual of an electric car is of limited value to the owner of a diesel pickup. The basic techniques of steering and changing a flat tire are the same, but putting diesel or an extension cord into the wrong one will fail to yield desirable results. Similarly, trying to apply prescriptions from one farm to another may yield marginal improvements at best, or be damaging at worst. Given all this, there are significant questions around whether the second condition of trade secret protection could be satisfied with the data from the example.

3: Does the farmer actively protect data like it is a secret?

The UTSA requires the putative owner of a trade secret to undertake reasonable efforts to keep the data secret.[32] The specific reasonable measures that a court would require to consider farm data as a trade secret is uncertain; however, it is known that courts look for active measures taken to ensure privacy.[33] Ferrell

30. USAchem, Inc. v. Goldstein, 512 F.2d 163, 168 (2d Cir. 1975); 18 U.S.C. § 1839.
31. *Goldstein*, 512 F.2d at 168.
32. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).
33. *Id.*

suggests the following steps may potentially be considered as "reasonable measures" to protect farm data as a trade secret while the data is "on the farm":

> 1. Properly screen prospective employees for attitudes on confidentiality and proprietary information;
> 2. Ensure that employees understand the importance of maintaining confidentiality in data on the farm;
> 3. When creating backup copies of data, make sure no other entities have access to these backups;
> 4. Restrict employee access to sensitive information;
> 5. Introduce password protections for electronic servers and files;
> 6. Regulate visitor and employee access if possible to physical locations where sensitive data may be accessible;
> 7. Conduct ongoing employee training on the measures used to protect farm data; and
> 8. Require a majority vote by farm operators before data are shared with a third party.[34]

An additional issue arises when employees leave the farm operation or are otherwise no longer employed. The farmer should ensure that any access the employee had to farm data is denied, which may mean changing passwords, access points, etc. At the employee's departure, the farmer should consider conducting an exit interview including reviewing the signed Non-Disclosure Agreement and ensuring the employee knows the obligations regarding data secrecy and that such policy will remain in effect in the future.

All of this may sound like a significant amount of time and expense, and it is. Farmers would have to place a high value on the confidentiality of the information to justify the expense of such measures. Further, while there are measures farmers can take to protect data while it resides on the farm, in an era of automated telematics and wireless communication, the question posed by the third criteria for trade secret protection has two components. (1) Do farmers take steps to actively protect data from disclosure, and perhaps more importantly? (2) Can farmers take those steps?

First, do farmers treat data like a trade secret? Heretofore, the answer would appear to be "no." While they may not have broadcast the data for all to see, farmers, landowners, and their advisors historically have not employed efforts to maintain the secrecy of farm data or their farming practices. With the dramatic increase in discussion of farm data and its prospective economic value since the early 2010s, many farmers have started to ask questions about how they could keep

34. Ferrell, *supra* note 24, at 41-54.

data private. As their awareness of data collection and transmission technologies increases, some farmers may be more active in seeking to secure data.

The second question may be the most pertinent: Can farmers take steps to keep data secret? At one level, the answer to this question is tied to the fact that much of agricultural production occurs outdoors. A farmer producing corn outdoors would not have a reasonable expectation of privacy, making it extraordinarily difficult to argue that one is even capable of employing reasonable efforts to keep something secret when it is readily observable from a public vantage point, which also goes to the arguments of the second condition as to whether the secret is readily ascertainable. Still, there may be elements of the operation that are not easily observable or determinable without direct access to the farm data that is not readily observable to the public but is rather collected and stored within the farm's telematics systems.

Importantly, though, data is not merely stored in telematics systems; it is often transmitted to equipment manufacturers through automated processes requiring no operator intervention whatsoever under an "opt out" (as opposed to "opt in") arrangement. Since about 2011, many new tractors roll off the assembly line equipped with cellular modems that automatically transmit a broad range of machine parameters back to the manufacturer.[35] While these arrangements can provide many benefits to equipment owners, such as enhancing the effectiveness of preventative maintenance and shortening equipment downtime, one could also argue that the farmer has no claim to a trade secret in farm data since a significant amount of the data composing the secret has already been shared with other parties through the equipment's telematics systems.

The disclosure of data to another party is not necessarily the death knell for any trade secret claim, though. Trade secrets are routinely disclosed to other parties while maintaining their status as trade secrets, so long as an agreement to retain the secrecy of the data is maintained.[36] The value of trade secrets would be diminished if they could not be shared with consultants and other advisers aiding the trade secret owner in determining how to maximize their use of the secret, and thus, trade secret law recognizes that trade secrets can be disclosed to others so long as appropriate measures are taken to make sure the party receiving the information also keeps it secret. "Information known by persons in addition to the trade secret owner can retain its status as a trade secret if it remains secret from others to whom it has potential economic value… the precautions required of the trade secret owner may increase with increasing dissemination."[37]

35. DYER, *supra* note 10, at 19.

36. *Trade Secrets Protection*, FENWICK & WEST LLP 3 (2001), https://perma.cc/N7CV-LXW2.

37. RESTATEMENT (THIRD) OF UNFAIR COMPETITION §39 cmt. f-g (1995).

The question remains, though, as to whether the user agreements between equipment manufacturers and farmers would be sufficient to satisfy the "secrecy efforts" requirements of the UTSA and cases interpreting it. Granted, "the owner [of a trade secret] is not required to go to extraordinary lengths to maintain secrecy; all that is needed is that he or she takes reasonable steps to ensure that the information does not become generally known."[38] A non-disclosure agreement between the farmer and the equipment manufacturer could be written to include sufficient restrictions on the uses made of the data as to satisfy the UTSA.

Equipment manufacturers, however, write most agreements not as non-disclosure agreements, but rather as "disclosure" agreements that define how the manufacturer may use the data, rather than defining what the manufacture may not do, while also failing to communicate the appropriate steps a farmer should take to safeguard data from unintentional disclosure.[39] Some manufacturers have gone so far as to suggest the farmer does not truly own the equipment itself, but rather operate under the theory that the tractor is simply subject to a user agreement.[40] Determining whether an equipment's user agreement would provide sufficient secrecy requirements to satisfy the third condition of trade secret protection is a case-by-case determination, but it is unlikely that many current user agreements would pass muster on this point. A farmer could still be able to execute a non-disclosure agreement with the manufacturer that would satisfy that condition.

Viewed together in this example of corn production, one can see it is unlikely that many farmers are actively taking the steps that would be necessary to claim trade secret protection for data. However, it can also be seen that under the right circumstances, a farmer could take those steps if they felt the increased value they would enjoy from retaining the exclusivity of data. This increased value would outweigh the cost of maintaining that secrecy. If they take those steps to protect their ownership of the putative trade secret, what do they get?

V. FARM DATA PROTECTIONS

The consequence of securing trade secret status for farm data is the farmer can pursue a misappropriation claim when farm data has been used in a way not allowed or has been acquired by an unauthorized party.[41] To successfully maintain a misappropriation claim, the farmer must first prove the data was indeed a trade

38. Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?* 22 SANTA CLARA HIGH TECH. L. J. 695, 724 (2006).

39. *See id.*

40. Kyle Weins, *We Can't Let John Deere Destroy the Very Idea of Ownership*, WIRED (Apr. 21, 2015), https://perma.cc/PV6Q-EMTR.

41. Ellixson & Griffin, *supra* note 5, at 4-5.

secret as discussed above.[42] Next, the farmer must prove the data was misappropriated, or wrongly obtained and used by another party.[43] The court will look at whether there were reasonable measures in place to ensure the secrecy of the data for the farmer to prevail in a trade secret lawsuit.[44] Although popular opinion seems to indicate farmers are expected to be endowed with ownership rights, the courts are likely to provide legal guidance unless laws are created that classify farm data.

If a farmer can prove a misappropriation claim, the court may allow them to recover one of the three types of damages, as described by:

> *1. Actual Damages*: These damages include lost profits to the farmers, typically calculated as net profits (i.e. gross profits minus operating costs). For example, if the data service provider used the data to manipulate prices of agricultural inputs and extracted profits directly from farmers, they could then potentially recover actual damages from the service provider.
> *2. Reasonable Royalty Rate*: These arise from the rate of return to the farmer that would have occurred had the data service provider properly negotiated a licensing agreement for the data at the point in time of misappropriation. This assumes that the farmer (who ordinarily may not have been willing to license this trade secret) did so willingly for a bargained-price.
> *3. Unjust Enrichment*: These damages include all the benefits the data service provider gained through misappropriation of the farm data. An example of this would be the profit the service provider made in the sale of the yield estimates. [45]

VI. AVOIDING PITFALLS IF FARM DATA IS NOT PROTECTED AS TRADE SECRET

Classifying farm data as trade secret offers farms legal protections born of statutory protections and case precedents. Whether courts agree or disagree with this designation, though, farmers can still create contractual protections for their data by placing provisions into nondisclosure agreements and other contracts (*e.g.* farmland leases) with their employees, service providers, cooperatives, and landowners to ensure that their data remains protected.

A. Contracts

Until the law catches up with technological developments, farmers wishing to keep data private can seek that privacy via a well-crafted contract. Farmers

42. Ferrell, *supra* note 24, at 32.
43. *Id.* at 38-40.
44. *Id.* at 440
45. Ellixson & Griffin, *supra* note 5, at 5.

should consider discussing a variety of issues with their attorney including, but not limited to, what control the farmer will have over the farm data, if the data can be shared if the service provider sells to a new company, how data will be kept anonymous, and if the service provider can modify the data.

B. Farmland Leases

To avoid pitfalls with landowners, a farmland lease should include plans for farm data.[46] Janzen identified three data ownership clauses that should be addressed in farmland leases:

> 1. A definition of the data;
> 2. A stipulation (preferably as early in the lease relationship as possible) of who owns the data and;
> 3. A specification of how and what types of data are to be shared between the landlord and tenant during and at the end of the lease period.[47]

These clauses can be customized to fit the specific needs of both landlord and tenant. The landlord may want data defined broadly to include all forms of data collected on the farm. Regardless of which party retains control of the data during the duration of the lease, landowners can make use of the third clause to ensure that the data ultimately stays with the land for future use. In the negotiating process, however, the landowner likely has incentive to provide the current farmer-tenant access to the data. This does not directly imply that the data should 'belong' to the land rather than the current landowner, but the opportunity for negotiation exists regarding the transferring of data between parties.[48] Economic theory suggests that, in the long run, the value of farm data will be built into the value of farmland in which case farm data would be expected to stay with the land.[49]

C. Nondisclosure Agreements

Another contractual protection for farm data is using a non-disclosure agreement.[50] A non-disclosure agreement is a legally enforceable contract that creates a confidential relationship between a person who holds some kind of information (the farmer) and a person/entity to whom the data is disclosed

46. Griffin et al., *supra* note 7, at 173; Todd Janzen, *Is Farm Data a Trade Secret*?, JANZEN AG L. BLOG (Sept. 30, 2015), https://perma.cc/4AVV-DWQK.

47. Todd Janzen, *Does Your Lease Address Farm Data?*, JANZEN AG L. (Oct. 2, 2015), https://perma.cc/ZT6A-QRQM.

48. Griffin et al., *supra* note 7, at 172.

49. *Id.*

50. Ferrell, *supra* note 24, at 48.

(employee, service provider, cooperative, etc.). The non-disclosure agreement must be executed before sensitive information is disclosed and contain key elements that an attorney with expertise in agriculture will be able to address.[51] Among these elements are definitions of the data to be protected, the steps that will be taken to maintain the privacy of the data, and the consequences of a failure to take those steps.[52]

VII. WHERE DO WE GO FROM HERE?

A limitation the farmer has with respect to the aforementioned contracts, farmland leases, and non-disclosure agreements is the comparative bargaining power that the farmer has or lacks in the negotiating process. Farmers have the most leverage when it comes to negotiating with employees (i.e. non-disclosure agreements). Depending upon the ferocity of the local farmland market, farmers may have some negotiating power with landowners. Individual farmers have very little to no negotiation power with service providers and vendors (especially multinational manufacturers of inputs and equipment).

Many farms will not have the resources needed to do what the law potentially requires to protect agricultural data on the farm, nor will they have the bargaining power to negotiate agreements with equipment manufacturers and service providers that may be receiving farm data by default. If policy-makers feel that farm data is worth protecting—that farmers need help in capturing the value of data at the farm level, and the risks of inadvertent data disclosure or deliberate acquisition of the data without farmer authorization are critical concerns—laws need to be developed to provide agriculture with protections that ensure data privacy can be maintained. Doing so requires, at a minimum, both defining what should be considered farm data and defining the policy justification for affording it protections that may not be afforded to other forms of business data. That said, the continuing growth of the debate around the propriety of Big Data applications in many arenas beyond just farm data suggests coming calls for data protections including both business information, including farm data, and personal information.

Until such legislation is enacted, there is a new statutory tool providing additional protections to intangible goods such as trade secrets. On May 11, 2016, President Obama signed the federal Defend Trade Secrets Act (DTSA)[53] into law. The DTSA sets out a federal cause of action instead of the patchwork state cause of action—which had previously been the only option for plaintiffs brining

51. Griffin et al., *supra* note 7, at 174.

52. *Id.*

53. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.

misappropriation lawsuits.[54] However, the DTSA does not preempt or invalidate the UTSA laws from individual states[55] Instead, it gives the plaintiff the option of using the federal law or the state law in pursuing a lawsuit.[56] Additional parts of the DTSA may be advantageous to farmers and farm data which are not typically present in the UTSA and other state-specific laws.

There are specific advantages to the use of the DTSA. First, it provides a more inclusive definition of trade secrets than the UTSA.[57] The DTSA definition appears to incorporate farm data more readily as the trade secret definition explicitly includes "intangible" items, data, as well as techniques and processes which arguably include information such as as-applied fertility or site-specific yield data.[58] Second, it allows for whistleblower protections, "which must be incorporated into employee contracts or non-disclosure agreements."[59] Third, it broadens damages awarded to potentially include injunctive relief (stopping the party being sued from using the secret).[60] Finally, it "applies to almost everyone, not just in cases where a trade relationship exists."[61]

VIII. CONCLUSION

Farm data issues are likely to become even more hotly debated in the short run. As the Big Data industry matures for agriculture, additional players will enter the debate. Farm data ownership and protections are expected to continue to be the focus of academia and industry, with a focus placed on court systems in determining value, ownership, and protections until state and/or federal legislation is passed to govern the access and utilization of farm data. Although no strict requirements exist yet to guide farmers to best data management practices, several common practices described earlier (e.g. employee agreements, limiting employee access to data, etc.) are worthwhile steps to take to safeguard farm data.

In the absence of statutory or other legal protections for farm data, farmers are in something of a challenging position. History and economic theory suggest that farmers will likely be able to extract some value from farm data in the short term, over the long term the share of that value that they can capture will diminish.

54. *Id.*

55. *See id.*

56. *See id.*

57. Ashley Ellixson, *Defend Trade Secrets Act 2016, Can It Help Protect Your Farm Data?*. MD RISK MGMT. EDUC. BLOG (Nov. 29, 2016), https://perma.cc/33FW-LCLX https://perma.cc/33FW-LCLX [hereinafter Can It Help Protect Your Farm Data?].

58. *Id.*

59. Ellixson, *supra* note 22.

60. *Can It Help Protect Your Farm Data*, *supra* note 57.

61. *Id.*

Resource constraints and disparities in bargaining power pose additional challenges for farmers who seek to protect and capture as much value from data as possible.

Many of these questions hinge on the value farmers are or should be placing on the exclusivity of data. But how exactly does one determine the value of that data at the farm level? Is it possible that farmers might realize more value from sharing data than keeping it exclusively to themselves?