Ownership and Protections of Farm Data

Ashley Ellixson, J.D., LL.M. (*aellix@umd.edu*)

University of Maryland Department of Agricultural and Resource Economics

Terry Griffin, Ph.D. (*twgriffin@ksu.edu*)

Kansas State University Department of Agricultural Economics

http://www.agmanager.info/crops/prodecon/precision/FarmData.pdf

A paper from the Proceedings of the
13th International Conference on Precision Agriculture
July 31 – August 4, 2016
St. Louis, Missouri, USA

Abstract. Farm data has been a contentious point of debate with respect to ownership rights and impacts when access rights are misappropriated. One of the leading questions farmers ask deals with the protections provided to farm data. Although no specific laws or precedence exists, the possibility of trade secret is examined and ramifications for damages discussed. Farm management examples are provided to emphasize the potential outcomes of each possible recourse for misappropriating farm data.

Keywords. *farm data, trade secret, intellectual property, ownership, privacy rights, property rights*

Introduction

Discussions of farm data are a topic of conversation heard on local and national news stations, newspapers, and the corner coffee shop or gas stations. But what actually is “big data” or “farm data,” and what do agriculturalists need to know about it?

In short, “big data in agriculture” can be thought of as aggregated farm data gathered from numerous farming operations into a single databank or repository. This repository archives data into a community and hosts tools to analyze the data. For example, a corn grower may collect site-specific geospatial and meta-data across many acres under their control, then submit that data to the community to be combined with many other growers’ data. Site-specific geospatial data may include applied seeding rates, soil nutrient information, and yield monitor data. Meta-data includes the number of acres, and when, where, and which inputs applied and cultivars planted.

The general consensus in agriculture is that combining data into a community with many other growers’ data across a geographic region is considered big data. These data are then shared with an agricultural technology provider (ATP), such as startup companies, cooperatives of farmers, or other public or private sector entities, through a cloud-based system.

The benefits of agricultural data can be vast but as of yet largely unproven. Farm data has the potential, for example, to assist in developing prescriptive planting programs, customized fertilizer if data has to do with soil, pesticide application, hybrid seed selection, and so on. Besides farm and industry benefits, farm data can potentially benefit society as a whole by examining issues for the public good which may otherwise go unaddressed. Although improved societal welfare such as clean water and reduced pollution benefits everyone, ATPs and the like do not directly address these issues. Public entities such as the Land Grant University System, however, do have incentives to address these concerns and are now empowered to do so with ample farm data.

Data from best management practices surrounding manure and waste, for example, may help researchers determine which practices best enhance the health of waterways. On the flip side are concerns and risks surrounding farm data. History shows the law rarely keeps up with technology and farm data are no exception. Courts often struggle when applying existing laws and previous rulings to modern technology. State legislatures can help by clearly defining the rules to guide courts in handling new technology (Goeringer et al., 2015).

Background: What Is Farm Data?

Due to its digital nature, farm data are considered *intangible*. Unlike most physical goods which can be touched, such as grain, livestock, machinery, and land, copies of digital data may be considered identical to the original. Multiple entities may have access to copies of data-a very different scenario than farmers’ grain stored in an elevator.

Data are also *irreplaceable,* similar to family heirlooms. Farm-level data may not be recovered if lost during data transfer or equipment malfunction, unless a backup copy is available. Since data are often lost during manual transfer, wireless cellular communication systems such as telematics are becoming an increasingly favorable feature. The market demand for data security, to prevent data loss, is growing.

Data are also considered “*non-rival*” because one person’s consumption or usage of data does not alter another person’s ability to consume or use the same data. A classic agricultural example of non-rival goods may be weather reports or market information on commodity prices. When one farmer uses reports on local weather or publicly available spot commodity prices, other farmers can utilize the same reports without loss of value to any one farmer (Griffin et al., 2016). In these examples, the value to a given farmer is not affected by another farmer using the information regardless of the

number of other users. The same is true of farm data especially in a community. A farmer can consume the data without reducing the value initially enjoyed by any one farmer.

Once the notion that farm data are non-rival is understood, the next logical question is whether data can be considered "*excludable*" or "*non-excludable*" (Griffin et al., 2016). Excludability depends on several factors including whether the data has already been shared with a third-party or within a community, and if ownership can be maintained. Ownership of "excludable" goods carries the owner's right to exclude others from having access. Most privately held goods typically are excludable.

Using the non-rival example of commodity price reports, price data may be privately held rather than publicly available if those reports were only available to subscribers. When a government entity, such as USDA, reports commodity price data, then that data would be non-excludable. Privately held agricultural data can be excludable while solely in the possession of the party which generated it; however, once the data are shared with other parties or aggregated into a community, excludability has been eliminated at least from the farmer's perspective.

Who Owns the Data?

What does ownership of data mean? One of the major questions when discussing "farm data" is: Who owns the data the ATP gathers from a farm? Is it the farmer's? Does the ATP now own it? This question of ownership may best be described with an analogy to FICO scores. If an individual financed a purchase such as property, equipment, or even animals, the lender probably purchased the individual's FICO score to evaluate their financial status. The interesting fact is the FICO score is data collected about the individual (financial history, assets, etc.) which is not necessarily owned by FICO. However, after FICO collects that data and conducts the analysis to derive a FICO score usable for creating a value for lenders and consumers for financing purposes, it created a "good" that FICO is now the owner of despite the data not being originally owned by FICO. Something similar can be said for the data after the ATP, cooperative or other technology provider has gathered data about farmers and created a use for that data.

Digital data are identical to the original data gathered at the farm level, and can be considered, unarguably, "property" of the farmer. Given that digital data are considered identical to the original, once another party has a copy, then the original owner of the data has lost control, i.e. the data has lost its exclusivity. This is why farm data ownership is such a hotly debated topic. To sort out some of the issues concerning ownership, let us look at what it means to "own" something. Legally speaking, when someone owns something they generally have the following rights:

– Right to POSSESS
– Right to USE
– Right to ENJOY
– Right to EXCLUDE OTHERS FROM
– Right to TRANSFER
– Right to CONSUME or DESTROY

In the context of something tangible like a bushel of grain, this definition is easier to understand. The bushel of grain was purchased or produced and the owner has the right to possess it, the right to use the grain for his or her own purposes, and the right to enjoy its ability to increase the efficiency of the farm operation. The owner also has the right to exclude others from using the grain as well as the right to transfer or sell that bushel of grain to another. Lastly, the owner has the right to consume or destroy the grain, which may sound unreasonable but because of ownership rights, is a right the owner maintains.

However, when considering the ownership of "farm data," and any item for that matter, it might be

better to ask: *What are the rights and responsibilities of the parties with respect to the data?* Because farm data are an intangible asset, it does not fit squarely into the box of a tangible asset, like the bushel of grain. With that in mind, it is easier to think of farm data in terms of rights and responsibilities of the parties with access to the data in order to describe ownership. The type of property in question will help determine the kind of rights and responsibilities in question in order to resolve the issue. Although presently, farm data has not been legally classified, a strong argument can be made that it may be classified as intellectual property and more specifically, trade secret.

What Is a Trade Secret?

Trade secret law is different from state to state. With that said, many states have adopted the majority of the Uniform Trade Secrets Act (UTSA) provisions. To date, 47 states, and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted UTSA. New York, North Carolina, and Massachusetts continue to apply their own definitions and standards (Legislative Fact Sheet). Since the majority of states have applied the UTSA as the trade secret standard, courts in those states will look to that definition to resolve conflict surrounding farm data. The UTSA defines a trade secret as:

1. Information, including a formula, pattern, compilation, program, device, method, technique, or process;
2. Which derives 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. Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

When applied in agricultural data context, these three aspects of the definition have more meaning. Consider this definition in the context of growing soybeans. With respect to Part 1: Is the manner and strategy in planting and harvesting soybeans a formula or pattern? We would argue, yes, they are. With respect to Part 2: Does growing soybeans in this manner derive economic value? In good years, absolutely. Is the plan for growing and raising soybeans "generally not known or readily ascertainable" to other people in or outside of the industry? Possibly. This is one part of the definition where farm data does not exactly fit and where the law must catch up with technology. However, when looking at whether the data are "readily ascertainable," courts have recognized that where information is available by other means (like a phone book as opposed to a company's customer list), the data are not protected by trade secret (USAChem, Inc. v. Goldstein, 512 F.2d 163 (2d Cir. 1975)). For example, if dairy cow genetics are available on a publicly available database, the genetic data would not be considered a trade secret, nor protected.

The third aspect of the trade secret definition deserves further consideration. With respect to Part 3: Farmers, landowners, and their advisors are unlikely to employ reasonable efforts to maintain secrecy of their data or practices. A farmer who has grown and harvested the same crops on the same property for several years and understands a particular piece of land better than others potentially has a good argument that his or her farm data are a trade secret, as long as he or she has taken reasonable steps to maintain its secrecy. When considering what reasonable steps are, courts will look to the actions of the farmer. This is done on a case-by-case basis and may be different depending on the data and on the farm operation.

Now, the question which logically follows is, "what if I share this data with my seed company, ATP provider, or my cooperative?" This sharing has the ability to destroy "secrecy" unless done anonymously. So, is farm data protected under the UTSA and considered a trade secret? The facts seem to weigh in favor of the farmer, but unfortunately until laws are created to categorize agricultural data, the courts will give the legal guidance.

What Protections Does Trade Secret Status Give?

If farm data falls under trade secret status and the farmer is determined to be the owner, what kinds of protections are the farm data afforded? Trade secret protection may give a farmer with farm data a

recourse in equity and law if the farm data are misappropriated (Uniform Law Commission). For example, if farm data are used without permission in any way (e.g. market manipulation for a certain crop or selling to third parties for land leasing purposes) damages may be able to be recovered. Damages may be one of three types:

1. *Actual damages* may include lost profits, which are typically calculated as net profits (meaning gross profits minus overhead and expenses required to run the business).
2. *Reasonable royalty* rate is determined by constructing a hypothetical negotiation for licensing the trade secret, or farm data, between the parties at the time misappropriation began. The law assumes this hypothetical negotiation occurred and that the farmer, who ordinarily would not license his trade secret to the misappropriator, did so willingly for a bargained-for price.
3. *Unjust enrichment* seeks to return the benefit the misappropriator gained from his actions to the farmer.

Actual Damages

Actual damages in a farm management context may be difficult to prove. Little quantitative evidence exists on the benefits of farm data to the farm operation. This is further compounded by farms which collect but never use data (for example, combine data which are not downloaded at least once per season). Unused data has zero value to farm operations. Farms successfully using data are uncommon and estimated benefits to the farm are marginal at best. Individual farms would not expect to find it worthwhile to prove 'actual damages'. However if resource-based theory (Grant, 1991) applied to loss or disclosure of data, then competitive advantage with respect to local bargaining power may be lost (Griffin et al., 2016). Proving damages may not be worth it to the individuals, however, a collective group of farmers may have a better chance at recovery considering their collective data set has more value than the individual data set. If a group, or cooperative, of farmers' data are misappropriated, proving actual collective damages may be easier than proving individual damages due to the value added when there is, for example, regional data, rather than one farm's data.

Reasonable Royalty

Again, it is going to be very difficult to prove reasonable royalty in the case of misappropriating one farm's data. Economic theory suggests that the aggregator sees no value in a single farm's data and therefore negotiation would be equal to $0. But if the aggregator negotiated with all farmers collectively, then they would arrive at some value greater than $0. However, there's no 'let's negotiate' button on an end-user license agreement (EULA, the agreement that usually accompanies software downloads). Farmers have no bargaining power with an aggregator once the data system has a critical mass of farms/acreage. However, farmers consistently place implicit value on their data much like they do for their herd genetics. The farmer who values farm data positively would not accept the $0 offered by data aggregators. Essentially, farmers' reservation prices or willingness-to-accept for their farm data will likely differ from the price that aggregators are willing to pay.

In the case of farm data, the value to the community is greater than the sums of the individual benefits each member received. In other words, the value of the whole is greater than the value of the sum of the parts. Given this characteristic of the 'network effect' where the value of the system is a function of the number of members of the system, the aggregator enjoys much greater benefits than any individual or even collective group of individuals. Therefore the 'reasonable royalty' may be difficult to estimate given that the individuals were only going to enjoy relatively small value. Furthermore, from the perspective of the aggregator, it makes very little to no difference if any given farmer participates in the network. Also in this case, the 'bargained-for' price may be greater than the value to the farmer but less than the value to the aggregator. But this is where the estimation becomes tricky. We know that the value to the aggregator is greater than the summation of all the individual benefits; however we also know that any given farmer can withdraw from the network without

causing the aggregator to lose value with respect to the network. Therein lies the problem; the aggregator can argue that the value of any given farm is $0 to the aggregator.

Unjust Enrichment

Given the network effects of farm data valuation, unjust enrichment is the most likely candidate for farmers to claim damages. The marginal value of an individual farm is very small but in the aggregate, the 'big data repository' has an opportunity for "unjust enrichment."

As an extreme example, the nefarious aggregator benefits disproportionately compared to individual members of the network, i.e. the farmers. Even though individual farmers may have already captured a majority of the potential farm-level benefits from their farm data, aggregators may benefit more than the sum of all individual farmers and even to the point that competitive advantage of individual farms were lost. In addition, the "Unjust Enrichment" may have been received as part of an intentional breach, at least from the farmer's perspective. Any use of a trade secret (in this case, farm data) without permission from the farmer or farm data owner, which results in disclosure of the data, means the farmer has the legal capacity to recover damages. In this way, trade secret protects the farm data owner from his or her farm data from being disclosed or improperly used.

Consider Protections of a Well-Worded Contract

Trade secret currently appears to be the best argument for categorizing farm data, however the possibility exists that trade secret would not apply to farm data and not provide those protections afforded by trade secret law. In that case, farmers may consider placing protections into *contracts* with their ATPs, cooperatives, and other service providers to protect their farm data. Although this list is not exhaustive, some items to consider and discuss with an attorney are:

1. What control will the farmer have over the data?
2. Is the data portable?
3. Can the farmer share the data if switching to another ATP?
4. How will the data be aggregated and kept anonymous?
   a. Can the data later be deleted after use? What measures are used to delete that data or otherwise make it unusable?
   b. Does the contract require affirmative consent before data are shared with an ATP or a third party or modified? Will the farmer be notified of changes to ATP's privacy policies?
5. Does the agreement prohibit ATP from using data for speculation in commodities markets?
6. Can the ATP modify the data? Remember, if the ATP changes the data itself, the ATP can claim ownership, thus destroying original ownership.
7. What security measures does the ATP use to prevent data breaches? What internal and external auditing procedures are in place?

Another document to consider when protecting data is a *nondisclosure agreement*. A nondisclosure agreement (NDA) is a legally enforceable contract that creates a confidential relationship between a person who holds some kind of information (arguably, the farmer) and a person to whom the trade secret is disclosed (ATP, cooperative, etc.). The NDA must be executed BEFORE the information is disclosed. NDAs contain a few key elements including:

1. Defining who is disclosing and who is receiving
2. Defining the trade secrets (in detail)
3. Excluding what is NOT protected as a trade secret (e.g.: publicly available information)
4. Establishing a duty to keep information secret
5. Specifying allowed uses / prohibited uses
6. Setting an enforcement period (usually defined by event rather than time)

Some additional items to consider including in a NDA are:

7. Data destruction requirements
8. Injunctive relief
9. Indemnity clause
10. Integration clause
11. Attorney's fees
12. Alternative Dispute Resolution, requiring mediation first rather than court

These considerations are not an exhaustive list in contracting farm data protections. It may be worth time and money to have a qualified attorney look over the details of the contract. Until the legal framework catches up to agricultural technology, ensuring protection of farm data in a well-crafted contract is the best management practice to follow.

Bargaining Power within Contracts Can Help You Decide Where Your Data Are Housed

Simple economics of supply and demand may inevitably solve the issue of the ATP's out-leveraging farms in bargaining power at least in the short run. Although initially many companies may compete to become the most successful farm data company, few ATPs in the farm data sector can be expected to last. As the number of startup companies and cooperatives offering these services increase and the larger manufacturers (e.g. Monsanto, John Deere, etc.) begin to step back, these smaller ATP's must attract farmers such that their networks can continue to exist and grow.

What does this mean? The relative advantage of farmers compared to the aggregator changes over time as the number of farmers join the system. In the infancy of agricultural big data systems there are numerous ATPs all striving to attract farmers who have the ability to pick and choose which ATP to house their farm data. Since many ATPs are attempting to attract farm data, these companies will have to appear as being farmer-friendly, which means alleviating farmers' fears with respect to data ownership, privacy, and security. Perceptions of ATPs are important to their success such that if the ATP manufactures or sells products in the agricultural sector, the ATP is unlikely to be successful in the farm data sector due to unfavorable perceptions (Mayer-Schönberger and Cukier, 2014). Ultimately, any company with unfavorable perceptions or *not* allowing farmers to retain ownership of farm data, or does not leave the data decision-making up to the farmer, will likely be excluded from being a viable farm data ATP.

Does the Data Stay with the Land or the Landowner?

Another issue in the discussion of farm data are the ownership of the data when the land is leased and farmed by another individual. There are three critical clauses to include in a farm lease to address ownership of farm data:

1. Define what the data are;
2. Define early in the lease relationship who owns this data; and
3. Specify how data are shared or not shared between landlord and tenant and whether the farm data are transferred to the landlord at the end of the lease (Janzen, 2015).

Clauses for land leases should be considered for the potential impacts on farm management (Goeringer, 2015). These clauses can be customized to fit the landlord and tenant's specific and unique needs. The landlord may want data defined broadly to include all forms of data collected on the farm. Whether the landlord wants to own the data collected or the tenant wants to own the data, negotiations should be initiated before the lease begins. No matter if the landlord or tenant will own the data, the third and final clause listed here is important to ensure the data ultimately stays with whoever is the current landowner. This leads to opportunities for negotiation with the landowner having 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 at any point in time, but that opportunity for negotiation exists regarding transferring data between parties. However, economic theory suggests that, in the long run, the value of farm data will be built into farmland values. For the same reasons, farm data are also expected to stay with the land.

Summary

No existing laws cover farm data ownership or implications of misappropriation of that data. Trade secrets are examined and the subsequent damages discussed as it may impact farm data. Case law, and/or legislation, are likely to be the deciding factor in determining the rights and protections associated with farm data.

References

Fishman, Stephan; and, Richard Stim. Nondisclosure Agreements: Protecting Your Trade Secrets and More. 2001. NOLO. 300 pp

Goeringer, Paul. "Farm Leases and Big Data: Issues That Cannot Be Settled by a Handshake Deal" Last visited December 21, 2015. http://www.aglaw.umd.edu/blog/farm-leases-and-big-data-issues-that-cannot-be-settled-by-a-handshake-deal?rq=data

Goeringer, Paul; Ashley Newhall; and John Molye. "Privacy Issues and the Use of sUAS/Drones in Maryland," University of Maryland Extension Fact Sheet, Nov. 2015.

Grant, R. M. The resource-based theory of competitive advantage: implications for strategy formulation. *Knowledge and Strategy*, 33(3), 3–23. 1991.

Griffin, T.W.; T.B. Mark,; S.L. Ferrell; T. Janzen; G. Ibendahl; J.D. Bennett; J.L. Maurer; and A. Shanoyan. "Big Data Considerations for Rural Property Professionals," *Journal of American Society of Farm Managers and Rural Appraisers,* pp 167-180. 2016.

Inside Counsel. Last visited December 20, 2015. http://www.insidecounsel.com/2015/04/24/the-3-types-of-trade-secret-misappropriation-damag

Janzen, Todd. "Does Your Lease Address Farm Data" Last visited May 26, 2016. http://www.aglaw.us/janzenaglaw/2015/10/2/does-your-lease-address-farm-data

"Legislative Fact Sheet - Trade Secrets Act." Retrieved December 18, 2015. http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act

Mayer-Schönberger, Viktor and Cukier Kenneth. Big Data: A Revolution That Will Transform How We Live, Work, and Think Kindle Edition. Houghton Mifflin Harcourt Publishing Company, New York, NY. 257 pp. 2014.

Uniform Law Commission Website. Last visited December 18, 2015. http://www.uniformlaws.org/ActSummary.aspx?title=Trade%20Secrets%20Act

USAChem, Inc. v. Goldstein, 512 F.2d 163 (2d Cir. 1975)