LEGAL ASPECTS RELATED TO AGRICULTURAL DATA COLLECTION, STORAGE AND USE

Author:
Todd J. Janzen
Janzen Agricultural Law LLC
8425 Keystone Crossing
Indianapolis, IN 46240
www.aglaw.us / janzen@aglaw.us

I. KEY TERMS FOR UNDERSTANDING AG DATA

A. Agricultural Data

To date, there are no published cases in the United States interpreting or defining "ag data." The term is a legal question mark. Understanding ag data requires one to first define what it is. *Merriam-Webster's* online dictionary defines data as:

> facts or information used usually to calculate, analyze, or plan something, information that is produced or stored by a computer.

Http://www.merriam-webster.com/dictionary/data. At its most basic level, data is an arrangement of 1s and 0s in a certain order. This pattern, when created, can be transferred from computer to computer and then translated into something else.

Although the term could encompass a variety of data collected on the farm, today there are at least six different types of important data that make up the more general common phrase "ag data." These categories are:

- **Agronomic Data** – information related to plants, such as soil nutrient levels, crop selection, herbicide and pesticide application, and yield.
- **Land Data** – information related to topography, slope, soil type, etc.
- **Machine Data** – information related to the performance measurement of machines, such as fuel usage, hour operated, RPMs, ground speed, oil usage, etc.
- **Weather Data** – information related to climate, such as temperature and precipitation.
- **Production Data** – information related to financial and contractual arrangements made by the farm.
- **Livestock Data** – information related to livestock genetics, production, feed consumption, medicine usage, etc.

Many of these categories of data can be tied to geospatial information. Even livestock data

is connected to geospatial information, as grazing cattle may perform very differently in different pastures. That is what makes ag data unique. A farmer can record not just his entire yield on an 80-acre field, but the exact yield in every point in the field.

B. ***Aggregation and Anonymization.***

Many ag data platforms will describe the concepts of "aggregation" and "anonymization," often together. "Aggregation" refers to the collecting and combining of multiple datasets together. For example, if you aggregated the yield data for each acre in an 80 acre field, one could determine the average yield by looking at the aggregated number (and dividing by 80).

Anonymization refers to the process by which the identifying characteristics of data are removed so that persons can no longer determine the data's origin. For example, if you removed a field's owner and location from yield data, that data would be anonymized.

C. ***Cloud.***

The "cloud" is the remote server (or multiple servers) where data is stored.

D. ***Integration.***

When an ag data platform creates a digital connection to another data platform, that connection is described as an "integration."

II. WHO OWNS AG DATA GENERATED ON MY FARM?

"Ownership" as a legal concept is complicated. You can only own something if the law recognizes that an ownership right. "Ag Data" is not a traditionally recognized type of property, subject to ownership. In the US, our laws recognize ownership of real property (land), improvements (buildings), personal property (goods), and even animals. Ag data is none of these.

US laws also recognize ownership of "intellectual property" or "IP" in a few instances. You can own a patent on a new invention. You can own a trademark or service mark. You can own a copyright in an original literary, musical, theatrical or other creative work. Ag data doesn't fit into these traditional IP classifications.

That leaves the law of trade secrets as the only real path for protection of ag data. Trade secrets are governed by the Uniform Trade Secrets Act, which has been adopted in similar forms in most states. A typical definition of a trade secret is:

> Information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value,

> actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

E.g. Ind. Code. § 24-2-3-2. The classic example is the formula for Coca-Cola. Coke guards this formula like a hawk, making sure that no one else can reproduce the exact flavor without knowing the exact formula. Of course, Coca-Cola has been reverse engineered many times, but never exactly replicated. Coke's formula is not readily ascertainable by others.

If a court attempted to determine whether ag data was a "trade secret," the court would do a multi-part examination of the elements. Here is an example of how that analysis might unfold, using the example of an entire year of agronomic data generated on an 80-acre cornfield:

Trade Secret Element	**Application to Agronomic Data**
A formula, pattern, method, technique or process	The manner in which a field was planted, tilled (or no-tilled), sprayed, and harvested. This likely satisfies the first element of the definition.
That creates economic value	There is generally value in knowing how to raise a field of corn over the course of a year. This element is likely satisfied.
It is not generally known or	This depends. If the farmer is not doing anything unique or unusual in how he or she farms the land, it may not be a trade secret. However, certain aspects like yield are unique to each field.
Readily ascertainable to other persons	Some aspects of agronomic data a person could ascertain without access to the raw data. For example, plant population could be determined by county the number of plants in a certain row distance.
Its secrecy is maintained.	This depends on how the farmer treats agronomic data in his or her possession.

Although the definition of trade secret is not a perfect fit for agronomic data, a farmer who

keeps the agronomic data for years and understands a particular field better than anyone else probably has a strong argument that his or her ag data could be a trade secret—provided reasonable steps are taken to maintain its secrecy.

Machine data could also be protected, although the ability to readily ascertain a modern machine's data makes protection less likely than agronomic data. However, manufacturers that collect machine data remotely and prevent others from doing so may have a strong argument that such data is the manufacturer's trade secret.

Weather data is likely not a trade secret unless it is generated by a farmer's personally owned weather station. Even then, it is hard to argue that particular weather data is not ascertainable from other sources and therefore not protected.

Financial and production data has very strong case for being a farmer's trade secret. It is generally not known, easily ascertainable, and farmers take reasonable steps to maintain its secrecy.

Livestock data could be a trade secret, depending on the type of information collected. For example, a dairy farmer may have a vested interest in maintaining the secrecy of the genetics of his herd. This information is not easily determined without the raw data in hand.

III. ISSUES CONCERNING TRANSFER AND CONTROL OF AG DATA.

With the general understanding that ag data likely contains trade secrets—assuming certain conditions are met—issues surrounding transfer and control of ag data should be addressed using the law of trade secrets. That means that owners of ag data should take steps to protect and maintain ag data secrecy. There are many areas where farmers routinely are asked to share data, but for purposes of example, this article addresses two: (1) in farm leases and (2) in arrangements with other persons who perform farming activities for the farmer.

A. Landowner/tenant relationship

In a farmland lease, a landowner and farmer have three basic ways they can address the ownership of data generated on farmland: (a) the person farming the land, normally the tenant, can own all data generated on the land; (b) the landowner can own all data generated on the land; or (c) the landowner and tenant can share, or co-own any ag data generated.

Regardless of who the landowner and tenant determine will own the data, a lease should address at least three data issues. First, a lease should define what "Ag Data" is since there is no widely recognized legal definition that fills in this blank. Second, the lease should establish who is the default owner of the defined "Ag Data." Finally, the lease should spell out what happens to "Ag Data" generated during the lease when the lease expires or is

terminated.

Depending on the landowner's interest in the farming activities on his or her land, a landowner may also want to require periodic uploads from the tenant of the current ag data. Today's online cloud-based data sharing tools would facilitate this transition as a landowner could be granted permission to access their tenant's files remotely.

In the long run, the data will certainly be an asset of the landowner as it will assist with establishing the proper rental rate, productivity, and nutrient content of the farmland.

B. "Custom" farming arrangements.

Likewise, farmers often utilize local cooperatives, seed consultants, nutritionists, agronomists, and other persons to engage in farming activities on their farms. A local co-op that provides spraying of pesticide is a perfect example. The raises questions about who owns the data generated by the co-op's sprayer?

Applying the trade secret definition onto the data generated by the sprayer, suggests that the person who creates the "pattern," "method" or "technique"—the co-op—would be the owner of the trade secret. But that is oversimplifying the analysis, because intellectual property law also recognizes that intellectual property can be created as a "work for hire." The employer is the owner of the "work" in those situations. Perhaps a court would view a co-op's data as a "work for hire" belonging to the farmer. We are still likely years away from an appellate court giving us an opinion on this question.

Assuming the co-op owns the data, which is the safe assumption, I suggest that the time has come to address ag data ownership in custom applicator agreements. Here are few provisions I think should be included:

> **Ownership:** Co-ops should explain which party owns the data generated by custom farming activities. Either the farmer or the co-op could be considered the data owner, depending on contractual preferences. The important thing is that the contract removes any uncertainty as to who owns the data after the work is done.
>
> **Transfer:** A custom applicator contract should require that ag data be transferred or made accessible to the farmer after the work is complete.
>
> **Accuracy:** A good, farmer-friendly contract will require the co-op to warrant that their equipment has been properly calibrated before each use, and that data generated by their operations is accurate. Without assurances that the data is accurate, sorting out ownership is pointless.
>
> **Privacy Protection:** A co-op should promise to take reasonable steps to safeguard information gathered during custom farming operations.

Retention: A contract should spell out exactly how long the co-op will maintain the ag data before it is deleted. There is no magic formula here, but I suggest the time-frame be at least one growing season to allow farmers plenty of time to remove data before it is deleted.

Similar provisions should be incorporated into contracts with agronomists, nutritionists, seed consultants, and custom harvesters if farmers want to protect the data generated on their fields and farms.

IV. QUESTIONS TO ASK BEFORE CLICKING "I ACCEPT"

The first time you sign into an ag data product you will be asked to accept certain terms of service, a privacy policy, or user agreement. Before signing on, here are some questions you can ask ag data product representatives:

A. What categories of data does the product collect from me?
B. Is my data portable after it is uploaded? Can I move my data from this platform to another platform?
C. Will you ask for my consent before providing my data to third parties?
D. Can I delete my ag data if I cease using your product?
E. What happens to my data if the tech provider is sold?
F. Does the provider recognize my ownership of ag data?
G. Does the product convert my data into a proprietary format? (Meaning I cannot use my data elsewhere once uploaded)
H. Is my ag data aggregated and anonymized?
I. Will the ag tech provider notify me if there is a data breach?
J. Is the ag tech provider "Ag Data Transparent" certified?

V. INDUSTRY EFFORTS TO BRING TRANSPARENCY TO AG DATA

A. Ag Data's "Core Principles"

In 2014, American Farm Bureau Federation (AFBF) observed that many of its farmer-members were concerned about the variety of new ag data products that were arriving on the market. What would happen to ag data once provided to these platforms? Would the tech providers use this data for their own purposes? Could the farmer ever get this data back? Should they trust these providers, which included legacy companies like John Deere that were developing new cloud-based products, as well as new startups from Silicon Valley and the Midwest?

To address these concerns, AFBF hosted a series of meetings with representatives of other interested farm groups, such as American Soybean Association, National Corn Growers,

National Association of Wheat Growers, National Farmers Union, and National Sorghum Producers. These organizations had similar concerns.

Ag tech providers were also invited. Representatives from the big equipment manufacturers were there: Deere, CNH, AGCO, as well as large seed and chemical companies, Dow, DuPont, and Monsanto. Smaller and start-up ag tech companies were there too.

After a series of these meetings, the group drafted *The Privacy and Security Principles for Farm Data*, or what today we call ag data's "***Core Principles***." These Core Principles represented basic guidelines that ag tech providers should following when collecting, using, storing, and transferring farmers' ag data. After publishing, 37 different companies signed onto the Core Principles, pledging to incorporate them into their contracts with farmers.

B. The Ag Data Transparent Seal of Approval

Of course, a pledge to follow non-binding guidelines is good, but incorporating the Core Principles into actual data contracts is much better.

To verify compliance with the Core Principles, AFBF and the other interested organizations and companies formed the Ag Data Transparency Evaluator, Inc., a non-profit organization (ADT) to audit companies' ag data contracts. This organization developed the Ag Data Transparent seal of approval. Much like the Good Housekeeping seal of approval verifies compliance with Good Housekeeping's standards, the Ag Data Transparent seal recognizes compliance with ag data's Core Principles.

Companies that want to be recognized as Ag Data Transparent must submit their contracts with farmers for certification to the ADT. In addition, companies must answer 10 questions about how they collect, store, use, and share farmers' ag data. The contracts and answers to the 10 questions are then reviewed by a third-party administrator* for accuracy. If the answers match what the company's contracts say, the Ag Data Transparent seal is awarded. If there is a discrepancy, the company is required to make a change before the seal is awarded.

Each of the 10 questions is based upon one or more of the Core Principles. For example, one principle is *portability*--farmers should be able to move ag data from one platform and use it in another. Accordingly, question 4 asks: *After I upload data to the Ag Tech Provider, will it be possible to retrieve my original complete dataset in an original or equivalent format?*

Participating companies must answer yes or no and provide an explanation. The final results are posted only at the Ag Data Transparent website

(www.AgDataTransparent.com) so that farmers, agronomists, and other ag professionals can review. The results also include hyperlinks to the companies' ag data contracts, in case someone wants to more closely examine a particular answer.

When a participating company changes or updates its ag data contracts, the company's answers must be updated as well if they want to continue to use the Ag Data Transparent seal.

C. The European Union's Code of Conduct for Sharing Agricultural Data

The European Union's (EU) General Data Protection Regulation (GDPR) encourages industry segments to develop guidelines for data processing and sharing. A number of farm organizations have come together to develop a set of guidelines for sharing agricultural data. The result is the EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement (EU Ag Data Code). Here are some of the key concepts identified by the EU Ag Data Code.

Data Originator Concept. Much ink has been spent writing about data "ownership." The EU Ag Data Code favors the concept of a data "originator" instead. The Code states that, as a basic principle, data produced by the farm operator, or commissioned by the operator, is considered property of the data originator. The data originator should decide how that data is used or shared downstream.

Rights of the Data Originator. The Code recognizes the data originator as the person with the initial rights in the data. This includes the right to benefit or be compensated for use of data they originated. The Code also states that, unless otherwise agreed in contract, only the data originator may authorize transfer of data. Transfer must occur only after the data originator grants their "explicit, express and informed consent."

The Need for Simple and Understandable Contracts. The Code states that contracts for ag data should clearly specify: (1) important terms and definitions; (2) the purpose of collecting, sharing, and processing data; (3) rights and obligations of parties related to data; (4) information related to storage and use of ag data; (5) verification mechanisms for the data originator; and (6) transparent mechanisms for adding new uses.

Encouraging Pseudonymization. The EU Ag Data Code contains the concept of "pseudonymization," which is a procedure for replacing certain fields in data with artificial identifiers, or pseudonyms. The purpose of pseudonymization is to render data less identifiable and therefore lower the risks that it inadvertently shares personal information. This is different than anonymization, which irreversibly strips information so that it can no longer be identified with the originator. The Code

states that data processor should use pseudonymization unless the parties agree on the terms by which the data originator can be identified.

Reducing Unfair Amendments to Contracts. Tech companies are constantly changing their online agreements and then simply informing their users, "by continuing to use this program, you agree to our new terms." Most people would shocked if this happened in other types of contracts. Imagine a car lease that changes terms if you continue to use your car. But the tech industry has managed to get away with one-sided amendments for years. The Code tries to limit this behavior by stating, "contracts must not be amended without the prior consent of the data originator."

Protecting a Natural Person's Privacy. If companies use ag data "to make decisions about the data originator 'as a natural person,'" then the GDPR protections for personal privacy rights apply. This is another way of saying, if you use my data to try to sell me stuff from third parties, the GDPR will apply.

Many of these concepts are similar to the widely adopted United States' Ag Data Core Principles, but some are new. Like the Core Principles, the EU Ag Data Code is non-binding.

VI. LEGAL ISSUES ASSOCIATED WITH AI

The proliferation of ag data platforms, Internet of Things type sensors, and cloud-based computing has led agriculture into another frontier—artificial intelligence (AI) and machine learning.

A. What is AI?

At its most basic level, AI is the process of learning from experiences in order to perform certain tasks. There are typically understood to be two types of AI: (1) Applied AI and (2) General AI. Applied AI occurs when a computer makes a unique decision based upon defined situation. A computer program that makes a stock trade when certain market conditions are present would be an example of Applied AI. In contrast, General AI is the concept of using artificial intelligence to perform many different tasks. The Siri program used on iPhones is an example of General AI, as Siri will perform many different tasks depending on the command and information "her" database.

AI works on probability. Programs must first be "trained" by being fed data that teaches the program what decision is right and what decision is wrong. Based upon the trained database, the program (or machine) is able to calculate the highest probability that decision will be right or wrong and then act accordingly. Over time, as the program obtains more examples of right or wrong decisions, the program gets more "intelligent."

B. What are the legal issues arising from AI?

AI requires a lot of data to operate correctly. Therefore, all of the concerns surrounding data collection, use, ownership and control are also present with AI applications. Privacy concerns are especially relevant, as many AI uses require day-to-day interaction with humans. For example, AI programs that use "natural language" speech recognition must listen for and to human voices in order to make decisions. This constant-listening makes users wonder what happens to all the information that is gathered by the AI device.

AI can also raise liability concerns. Our tort system is designed to apportion blame among the humans (or legal entities) that made decisions leading to the tort. What happens when a *machine* makes a decision that causes damage or injury? Who is liable under that scenario: (1) the owner of the machine; (2) the programmer of the AI software; (3) the person who trained the machine; or (4) someone else? Our courts will be in unchartered territory when these issues first arise.

For more information, please contact:

Todd J. Janzen
Janzen Agricultural Law LLC
8425 Keystone Crossing Suite 111
Indianapolis, IN 46240
janzen@aglaw.us
www.aglaw.us