All Data Big and Small: Legal Issues Surrounding Agricultural Data

Shannon L. Ferrell, Esq., J.D.
Professor, Agricultural Law
Oklahoma State University Department of Agricultural Economics
532 Agricultural Hall
Stillwater, OK 74078
shannon.l.ferrell@okstate.edu

CONTENTS

TABLE OF AUTHORITIES

All Data, Big and Small
Authors' Vitae
Shannon L. Ferrell, Esq., M.S., J.D.
Professor, Agricultural Law
Oklahoma State University Department of Agricultural Economics
532 Agricultural Hall
Stillwater, OK 74078
shannon.l.ferrell@okstate.edu

Shannon Ferrell is currently a Professor in the Oklahoma State University Department of Agricultural Economics, where he specializes in Agricultural Law. He grew up on a cattle and wheat operation in Western Oklahoma, and obtained his Bachelors and Masters degrees in Agricultural Economics from OSU before obtaining his Juris Doctorate *summa cum laude* from the Oklahoma City University School of Law with endorsements in Estate Planning and Business and Financial Services Law. Shannon spent a number of years in private practice, focusing on agricultural, environmental, energy, and corporate law, before joining OSU in the summer of 2007.

Professor Ferrell has been a practicing attorney for 15 years and focuses on agricultural law with a particular emphasis on energy, environmental, and estate planning issues. As a member of the Department of Agricultural Economics, Shannon holds an extension and teaching appointment. Since joining Oklahoma State University, he has provided over 400 extension seminars and workshops throughout North America with a cumulative audience in excess of nearly 25,000 while authoring over fifty extension publications. His extension activities encompass all areas of agricultural law, and he also teaches the agricultural law courses at both Oklahoma State University and the University of Oklahoma College of Law.

I.   INTRODUCTION

A.   Abstract

Drones and advanced sensing equipment on agricultural machinery can provide farmers and ranchers unprecedented insights to their own operations. Uploading, aggregating, and analyzing data across multiple operations (a process often referred to as "Big Data") also holds the potential to generate knowledge beneficial not only to producers but numerous other segments of the agricultural industry. However, many producers have numerous concerns about their rights with respect to the data generated by them or, in some cases, about them. This article addresses some of the legal concerns involved both with data acquisition and with data rights. Regardless of how data about their operations is acquired, though, producers should work with their attorneys to craft data use agreements to protect their interests, as few existing laws deal with these issues.

B.   The Brave New World of Farm Data

"Big Data" is one of the biggest buzzwords in the arena of agricultural technology right now and may receive almost as much discussion in agriculture as the weather and commodity prices. But what is Big Data anyway, and why should farmers care? This article aims to define both "Small" and "Big" Data, and to reveal its advantages and disadvantages for farmers. The discussion then turns to the concerns farmers express about disclosing farm data, and provides concrete solutions for what they can do individually and collectively to address those concerns.

1.   Drones and Other Data Acquisition Tools

As many in Generation X learned from School House Rock, "knowledge is power!" Increasingly, agricultural producers rely on advanced analytics for their operations to optimize their operations and stay "in the black" in an era of increased volatility for input prices and production conditions. These analytics are only as good as the data that drives them, though, and producers have more tools than ever to acquire that data.

One important potential source of this data is the Unmanned Aerial Vehicle (UAV), more commonly called a "drone." Though there are numerous definitions of "UAV" or "drone," the FAA Modernization and Reform Act of 2012 defines the term "unmanned aircraft system" (sufficiently synonymous with UAV for the purposes of this discussion) as "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system." P. Law 112-95 (H.R. 658-62), § 331(9).

The opportunity for producers to fly over their operations for relatively little cost and virtually no risk to life (at least their own) opens a number of doors for them to gain much better data of crop and pasture conditions through both visual and non-visual spectrum (such as infrared) data that can look at entire parcels at once. Imagery from drones can even be orthorectified through relatively inexpensive software to provide detailed measurements of land. Additionally, drones can be used to check on livestock, proving particularly useful on large operations and/or those with rugged, inaccessible terrain. Indeed, the potential uses of drone technology are almost innumerable.

At the same time, though, any new technology comes with risks and fears of misuse. Privacy and safety concerns are perhaps two of the largest issues swirling around agricultural drone use. When flying at any appreciable altitude, a camera-equipped drone can see not only the property over which it flies, but adjoining parcels. Naturally, this raises concerns of privacy, with those concerns drastically exacerbated by public proclamations of groups critical of standard agricultural practices that they will deploy drones to overfly agricultural operations in circumvention of "ag-gag" laws and to surveil livestock operations for potential environmental and animal well-being violations. *See* Lowe, P., "Drone to Fly Over Livestock Operations and 'Ag-Gag' Laws," Nebraska Educational Telecommunications Commission / Harvest Public Media, August 25, 2014. *Available at* http://www.netnebraska.org/article/news/933744/drone-fly-over-livestock-operations-and-ag-gag-laws. Pilots flying at low altitudes are also concerned about potential mid-air collisions with drones, as noted by a number of near-misses. *See* "Drone Sightings," Wall Street Journal, November 26, 2014, *available at* http://graphics.wsj.com/faa-drones/ .

2.   "Small" and Big Data" on the Farm

The evolution and revolution in agricultural Big Data comes from the expansion of "Small Data" in agriculture. Recent years have seen remarkable growth in producers' ability to collect data pertaining to their own operation through the growth of techniques and technologies such as grid soil sampling, telematics systems for farm equipment, Global Navigation Satellite Systems (GNSS), farm aerial imagery acquired via small unmanned aerial systems (sUAS), and the like. In simplest terms, "Small Data" consists of data isolated to the fields or farms where the data originated. Farmers who use information technology to conduct their own

on-farm experiments, document yield penalties from poor drainage, or negotiate crop share agreements are using data that is considered "small." Coble, Keith *et al*, 2017. *Big Data in Agriculture: A Challenge for the Future*, Appplied Economic Perspectives and Policy, 40(1):79-96.

Drones represent only one of a myriad of tools now available to help producers accumulate data about their agricultural operations. Machinery-based and even hand-held sensors provide mountains of information about the operation of farm equipment as well as the inputs they apply, the crops they harvest, and even the ground over which they run. This data can be wirelessly uploaded to consultants and cloud-based data storage warehouses, sometimes even without any intervention on the part of the operator. The ability to aggregate data over hundreds or even thousands of farms creates the power to conduct analyses more powerful than ever-before imagined.

These capabilities give rise to the issue of "Big Data." While the term Big Data is relatively new, it refers to a concept that is not. There are many definitions for the term, but a straight-forward one might be "a collection of data from traditional and digital sources inside and outside your company that represents a source for ongoing discovery and analysis." Arthur, Lisa. 2013. What is Big Data? Forbes, CMO Network blog entry, *available at* http://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/. While this definition sounds much like traditional data analysis (and it is), recent advances in both data collection and transmission increase the analytical power of datasets by orders of magnitude. Not only do companies now have access to data from every link in their supply and marketing chain from sensors on the factory equipment to GPS on delivery trucks and bar code scanners in the store; they can now track search engine inquiries for their product and listen directly to conversations about their products in social media. This profusion of data creates an enormous dataset, the analysis of which can do everything from predict the hot toy for Christmas this year to tell the Centers for Disease Control ground zero in the next influenza outbreak. Google.org. 2011. "Google Flu Trends: How Does it Work?" *available at* http://www.google.org/flutrends/intl/en_gb/about/how.html).

Given these considerations, a more complete definition of "Big Data" requires data considered truly "big" possess the following traits (Coble, Keith *et al*, 2016." Advancing U.S. Agricultural Competitiveness with Big Data and Agricultural Economic Market Information. Council on Food, Agricultural, and Resource Economics report):

Volume: The amount of data is so large it cannot be stored on one physical volume such as a hard drive; put

another way, the analytical software must "go to" the data rather than the data being "brought to" it.

Velocity: The data comes at higher rates than can be handled by a single computer.

Variety: The data comes from a broad array of sources including data automatically gathered by sensors and software as well as data manually entered by users. This also means the data may come in a variety of formats with a lack of structure or design to it.

Veracity: The data analytics are required to consider the accuracy and credibility of the data, especially considering the "variety" considerations mentioned above and the potential for mis-calibration of automated data collection systems or user error (and bias) coming from manually-entered data.

The agricultural industry stands on the front line with other industries in the Big Data revolution. In agriculture, tremendous leaps in data acquisition equipment on everything from tractors to granaries coupled with instantaneous and continuous transmission of that data through cellular modems creates a dataset soon to rival that of any industry. In a farm context, Big Data means farmers can not only analyze their own production data in ways never before possible; they can also aggregate their data with other producers to drastically increase their ability to detect trends in everything from seed variety performance to the comparative economics of cultivation practices. As anyone who has taken a statistics class knows, the predictive power of a dataset grows with its size. The exponential growth of farm data means farmers will soon have analytic tools to rival those of any industry.

3. The Promise and Peril of Big Data on the Farm

If Big Data posed nothing but advantages, its discussion would not have the fevered pitch currently seen across virtually every agricultural media source. As with any tool, Big Data is neither inherently good nor evil – it is simply a tool. As with any tool, its benefits and dangers lie in how one uses it. Following is a discussion of these potential advantages and disadvantages.

Many a farm management teacher has proclaimed "you can't manage what you can't measure," and today's farmer lives in an era where almost everything on the farm can be measured, giving him or her the power to manage elements of agricultural production heretofore unimaginable. Improvements in farm equipment diagnostic and data acquisition systems alone provide the potential to diagnose equipment issues before they manifest themselves in downtime and to monitor a crop at literally every step of the production process from planting through cultivation and to harvest. One need only watch John Deere's "Farm

Forward" video to see a host of innovations made possible by these technologies and to realize that these possibilities are not as far away as one might think. John Deere, Inc. "Farm Forward (video) *available at* https://www.youtube.com/watch?v=jEh5-zZ9jUg.

Looking one step up the data ladder from the farm, cellular modem technology means producers can instantly and continuously share data with crop advisors and other consultants. These consultants can analyze this data (using their own Big Data tools), prepare recommendations, and even create prescriptions that can be uploaded to the producer's equipment to make on-the-fly adjustments to seeding, fertilizer, pesticide, and cultivation practices.

While these advantages alone make the prospects of Big Data tantalizing, the power of Big Data only comes to full force when it is truly big. What if equipment companies, consultants, and input suppliers combined the data from thousands of farmers into one massive dataset? Seed trials could be conducted in a fraction of the time as varieties could be compared across hundreds or even thousands of farms representing dozens of soil types, microclimates, and production systems simultaneously. The costs and benefits of various production systems and cultivation practices could be analyzed with similar speed. Plant disorders could be isolated and eradicated before costing producers their entire crops.

Lest one think any of these prospects to be far-fetched, many of them are (or soon will be) a reality. John Deere already uses real-time telematics data to analyze potential equipment failures to dispatch service technicians, and has partnered with Pioneer to provide near-real-time crop recommendations that can be uploaded to the farmer's equipment (Eckelkamp, 2013). Eckelkamp, Margy. 2013. John Deere Partners with Open Platform. Agweb.com*, available at* http://www.agweb.com/article/john_deere_partners_with_open_platform_NAA_Margy_Eckelkamp/. Monsanto's work through The Climate Corporation looks to create massive datasets to analyze a host of issues from plant variety protection to the impacts of climate change on crop production systems (Upbin, 2013). Just as the constantly increasing speed and decreasing size of processors continues to yield evermore-powerful computers, so too may one expect new applications of Big Data to farm issues.

Any new technology carries potential harms, whether real or imagined. In the realm of Big Data, recent history suggests many of the real threats come from insufficient controls to prevent the disclosure of personally identifiable information ("PII") to outside parties and inadequate agreements on the uses of data by parties to whom it is disclosed.

One need not look far into the past to find numerous examples of the disclosure of PII, whether merely inadvertent or the result of targeted hacker attacks. Attacks on companies' payment systems have resulted in the credit card information of hundreds of millions of customers from Adobe Systems (150 million customers), Heartland Payment Systems (130 million customers), TJX (parent company of TJ Maxx and Marshalls, 94 million customers), TRW Information Systems (credit reporting company, 90 million customers), Sony (70 million customers) all of which dwarf breaches attracting more media attention such as Home Depot (56 million customers) and Target (40 million customers). Pepitone, Julianne. 2013. "5 of the Biggest-ever Credit Card Hacks." CNN Money. *available   at* http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/. Credit card theft may be the most direct form of PII theft, but theft of other individual pieces of information such as Social Security Numbers, addresses, and birthdays may allow a criminal to fabricate an identity as well. Farmers are understandably concerned that PII may be stolen if that information is disclosed to an outside party such as a financial consultant. However, most data disclosed to a crop production consultant will be in the form of raw data regarding crop production, GIS information about the farm, and the like. This significantly reduces the risk of identity theft by someone obtaining the data by illicit means. Nevertheless, farmers should still be aware of the data they are disclosing to providers as discussed later in this paper.

The theft of PII by criminals is one threat posed by data transfers, but so too is the inadvertent, or perhaps intentional but misinformed, disclosure of data by the party receiving that data. Take, for example, the disclosure of thousands of "farmers' and ranchers' names, home addresses, GPS coordinates and personal contact information" by EPA in response to a Freedom of Information Act (FOIA) request regarding concentrated animal feeding operations (CAFOs) which prompted a lawsuit from the American Farm Bureau Federation and National Pork Producers Council alleging that the agency overstepped its authority in doing so (Wyant, 2013). Wyant, Sara. 2013. "Farm Groups File Lawsuit to Stop EPA Release of Farmers' Personal Data." Agri-Pulse, available at http://www.agri-pulse.com/Farm-groups-file-lawsuit-to-stop-EPA-release-of-farmers-personal-data-07082013.asp. While this event represents the disclosure of information by an enforcement agency, many farmers fear the converse - that an enforcement agency could compel a data-receiving party to disclose information even if such disclosure were not legally required. Another concern is whether an adverse party in litigation (or even a party contemplating litigation) could persuade a party holding a farmer's data to disclose the data as an aid to their case, again even if such disclosure was not legally required.

Still another issue of concern for farmers, but clearly not limited to farmers, is how data – some willingly disclosed via social media platforms such as Facebook, Twitter, Instagram, and others – can be used for purposes well beyond those conceived when the user agrees to participate in such platforms. The myriad uses of data to psycometrically analyze and potentially manipulate users were highlighted in the Cambridge Analytica controversy. *See* Granville, Kevin, 2018. "Facebook and Cambridge Analytica: What you Need to Know as Fallout Widens," New York Times, March 19, 2018.

Indeed, a number of potential data uses lie within a gray area of conduct. These uses may seem wrong or at least uncomfortable at an intuitive level, but are not illegal at this point in time. The first such use – highly targeted or "laser" marketing – is encountered almost every day as one sees online ads through Google search results or Facebook selected based on a user's online profile. In some cases, this marketing can become uncomfortably precise and predictive, as was recently publicized by a recent story showing now Target's retail analytics could predict shoppers were pregnant (Duhigg, 2012). Duhigg, Charles. 2012. "How Companies Learn Your Secrets." The New York Times Magazine, available at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp&. In the agricultural realm, many of the consulting service providers to whom farmers are disclosing data are the same companies (or affiliates of companies) providing a number of other inputs such as seed, fertilizer, pesticide, and equipment. At a minimum, one could see a potential conflict of interest in such companies recommending products their affiliate provide, and at a maximum a customer could be barraged by solicitations for products based on their production patterns. Taken one step further, could such companies manipulate commodity markets themselves? If one thinks about it, equipment companies already have fleets of combines and other harvesters continuously uploading harvest data to their servers – what better market intelligence could one have? Although such behavior could arguably fit into some legally-prohibited practices, it is also arguably outside the reach of those prohibitions in that "really good intelligence" might not be regarded by courts as price manipulation. 17 C.F.R. § 180.1 (2015).

Salon.com summarized many of these fears in its article "Monsanto's Scary New Scheme: Why Does it Really Want All This Data?" Khan, Lina. 2013. "Monsanto's Scary New Scheme: Why Does It Really Want All This Data?" Salon.com, *available a*t http://www.salon.com/2013/12/29/monsantos_scary_new_scheme_why_does_it_really_want_all_this_data/. Although the story may be speculative in some of the prospective problems it outlines, the old adage "perception is reality" bears some weight in the Big Data discussion. Although many argue that the potential advantages of Big Data on the farm will significantly outweigh the potential disadvantages (pointing out that any firms abusing the data relationship with producers will soon find themselves out of business), the perceptions of those concerns prevent many producers from exploring Big Data applications.

II. PROTECTING FARM DATA

A. Where does farm data fit in the current intellectual property framework?

The United States of America has one of the most robust systems of property rights in the world, empowered by a legal system making it (relatively) easy to enforce those rights. Thus, the first place many look for a means of protecting one's data from misappropriation and/or misuse is the property rights system. This requires one to examine who "owns" farm data. The answer to the question is not easy, though, as traditional notions of property ownership find challenge in their application to pure information.

The notion of property ownership typically involves some form of six interests, including the right to possess (occupy or hold), use (interact with, alter, or manipulate), enjoy (in this context, profit from), exclude others from, transfer, and consume or destroy. Some of these interests do not fit, or at least do not fit well, with data ownership. Excluding others from data, for example, is difficult, particularly when it is possible for many people to "possess" the property without diminishing its value to the others, just as the value of a book to one person may not be diminished by the fact other people own the same book. Smith, Lars. 2006. "RFID and other embedded technologies: who owns the data?" SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL 22:4, 695. Thus, the better question may be "what are the rights and responsibilities of the parties in a data disclosure relationship with respect to that data?" (Petersen, 2013). Peterson, Rodney. 2013. "Can Data Governance Address the Conundrum of Who Owns Data?" Educause blog, http://www.educause.edu/blogs/rodney/can-data-governance-address-conundrum-who-owns-data.

Data is difficult to define under traditional notions of tangible property, but the intellectual property framework serves as a useful starting point to define what rights a farmer might have to their farm data. Intellectual property can be divided into four categories: (1) trademark, (2) patent, (3) copyright, and (4) trade secret. The first three areas compose the realm of federal intellectual property law as they are defined by the Constitution as areas in which Congress has legislative authority. U.S. Constitution, Article I, §8,

clause 8. For the purposes of the following discussion, "farm data" will include the types of data typically uploaded automatically by the farmer's equipment, such as diagnostic and use data, input application data, harvest data, and global positioning system (GPS) and geographic information system (GIS) data.

1. Trademark

One of the easiest intellectual property models to discard as a viable farm data protection tool is trademark. The Federal Trademark Act (sometimes called the Lanham Act) defines trademark as "any word, name, symbol, or device, or any combination thereof...to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown." 15 U.S.C. § 1127. Examples of trademark include product names, such as Coca-Cola® or the design of its contoured bottle. One quickly realizes trademark fits poorly as a model for defining farm data ownership, as trademark addresses intellectual property used for branding purposes rather than information.

2. Patent

The U.S. Patent Act states "whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor." 35 U.S.C. § 101. Generally, for an invention to be patentable, it must be useful (capable of performing its intended purpose), novel (different from existing knowledge in the field), and non-obvious (somewhat difficult to define, but as set forth in the Patent Act, "a patent may not be obtained… if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains"). 35 U.S.C. §§ 102, 103. Patent serves as a poor fit for a model of farm data ownership since it protects "inventions." Raw data, such as farm data, would not satisfy the definition of invention.

It should be noted patentable inventions could be derived from the analysis of farm data. While this does not mean the data itself is patentable, it does suggest that the agreement governing the disclosure of farm data by the farmer should address who holds the rights to inventions so derived (as discussed below).

3. Copyright

The federal Copyright Act states the following:

> Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or

later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories:
> literary works;
> musical works, including any accompanying words;
> dramatic works, including any accompanying music;
> pantomimes and choreographic works;
> pictorial, graphic, and sculptural works;
> motion pictures and other audiovisual works;
> sound recordings; and
> architectural works.

17 U.S.C. § 102(a). More so than trademark and patent, the copyright model at least resembles a model applicable to farm data. At the same time, however, the model also has numerous problems in addressing agricultural data. First, the list of "works of authorship" provided in the statue strongly suggests a creative component is important to the copyrightable material. Second, the term "original works of authorship" also has been interpreted to require some element of creative input by the author of the copyrighted material. This requirement was highlighted in the case of *Fiest Publications Inc. v. Rural Telephone Service Company*, 499 U.S. 340 (1991), where the U.S. Supreme Court held that the Copyright Act does not protect individual facts.

In *Fiest Publications*, the question was whether a pure telephone directory (consisting solely of a list of telephone numbers, organized alphabetically by the holder's last name) was copyrightable. Since the directory consisted solely of pure data and was organized in the only practical way to organize such data, the Supreme Court held the work did not satisfy the creative requirements of the Copyright Act. This ruling affirmed the principle that raw facts and data, in and of themselves, are not copyrightable. However, an author can add creative components to facts and data such as illustrations, commentary, or alternative organization systems and can copyright the creative components even if they cannot copyright the underlying facts and data. Put another way, the facts that hydrogen has an atomic number of 1 or that the number of ABC Plumbing is 555-1234 are not copyrightable, but an article about hydrogen in an encyclopedia or a Yellow Pages® ad with ABC Plumbing's number along with a graphic and description of their services are.

As with patent, farm data can lead to copyrightable works even if the underlying data is not protected itself. For example, farm data may not be copyrightable, but a

report summarizing the data and adding recommendations for action might be. Again, then, it is incumbent upon those disclosing farm data to include language in their agreements with the receiving party to define the rights to such works derived from the data.

4. Why trade secret might work as a farm data framework

While trademark, patent, and copyright do not appear to fit as models for farm data ownership, trade secret has the potential to fit the bill. Importantly, trade secret is a function of state law (unlike trademark, patent, and copyright, which are all creatures of federal law). As of this writing, all but three states have adopted the Uniform Trade Secrets Act, providing a significant degree of consistency in trade secret law across most states.

Under the Uniform Trade Secrets Act, a "trade secret" is defined as:

> …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.

Uniform Trade Secret Act, § 1. Importantly, this definition makes clear that "information… pattern[s], [and] compilation[s]" can be protected as trade secret. This, at last, affords hope of a protective model for farm data. This is not to say that trade secret is a "slam dunk" for protecting farm data, however. Note the two additional requirements of trade secret: first, that the information has actual or potential economic value from not being known to other parties, and second, that it is the subject of reasonable efforts to maintain the secret.

The first provision requires that to be protected as a trade secret, farm data such as planting rates, harvest yields, or outlines of fields and machinery paths must have economic value because such information is not generally known. While a farmer may (or may not) have a privacy interest in this information, the question remains as to whether the economic value of that information derives, at least in part, from being a secret. The counterargument to that point is that the economic value of the information comes from the farmer's analysis of that information and the application of that analysis to his or her own operation – a value completely independent of what anyone else does with that information – and that the information for that farm, standing alone, has no economic value to anyone else since that information is useless to anyone not farming that particular farm. One can see then this first element

poses problems for the trade secret model. It should be noted here that there is a clear economic benefit to the collection of farm data; otherwise Monsanto would not spend nearly $1 billion in acquiring a company to aggregate such data. This represents a question yet to be answered clearly by the body of trade secret law: whether one can have trade secret protection in information that standing alone has no economic value to other parties, but does have such value when aggregated with similar data from other parties.

The second provision – that the data be subject to reasonable efforts to maintain its secrecy – also finds problems in an environment where the data is continuously uploaded to another party without the intervention of the disclosing party. The fact that data is disclosed to another party does not mean it cannot be protected as a trade secret; if that were the case, there would be little need for much of trade secret law. Rather, the question is how and to whom the information is disclosed. As noted in the Restatement (Third) of Unfair Competition's comments on the Uniform Trade Secret Act, "…the owner 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." (Smith, 2006, *citing* Restatement, 1995). The question becomes what constitutes "reasonable steps" to keep continuously uploaded data protected. Almost certainly this means there must be some form of agreement in place between the disclosing party and the receiving party regarding how the receiving party must treat the received information, including to whom (if anyone) the receiving party may disclose that information.

While an explicit written agreement is not necessary to claim trade secret protection, such an agreement is almost certainly a good idea. Not only can such an agreement clarify a number of issues unique to the relationship between the disclosing and receiving parties; it can also address numerous novel issues in the current information environment that trade secret law has not yet reached.

B. The Importance of Non-Disclosure Agreements

As the reader can see from the preceding discussion, there is not an intellectual property model presenting a spot-on fit for the protection of agricultural data. Trade secret comes closest, and if indeed a farmer can prove their data is protectable information (with the burden of such proof resting on the farmer), no agreement is needed to provide such protection. However, this scenario poses a tremendous amount of uncertainty and requires costly, time-consuming litigation.

Conversely, farmers disclosing their data, and service providers receiving it, proactively could enter a non-disclosure agreement (NDA) in which both parties

agree in advance to hold the information confidential and agree to what uses can and cannot be made of the data. Such an agreement may be entered even if the information would not be regarded as a trade secret, since the parties covenant to treat the information as secret independently; the obligations of the party derive from the contract itself and not another legal doctrine. The following discussion addresses attempts to address some NDA issues by corporate policies, and the provisions that should be considered by farmers when negotiating an NDA with a party to whom they will be disclosing farm data.

Many companies offering consulting or data analysis services have company policies addressing various concerns such as confidentiality of the information, specifying to whom the data may be disclosed, and uses that may be made of the data. Examples of such policies can be found in the Climate Corporation (2014) and John Deere (2014) data privacy statements. As an example of these policies, below is an excerpt from the John Deere Privacy and Data Statement:

John Deere understands that you may not want us to provide Personal Information and Machine Data to third parties for their own marketing purposes. We limit our sharing of Personal Information and Machine Data as follows:

We may share Personal Information and Machine Data with our affiliated companies, suppliers, authorized John Deere dealers and distributors, and business partners, which may use it for the Purposes listed above.

We may also share Personal Information and Machine Data with our service providers to fulfill the Purposes on our behalf. Our service providers are bound by law or contract to protect the information and data, and to only use it in accordance with our instructions.

We may disclose Personal Information and Machine Data where needed to affect the sale or transfer of business assets, to enforce our rights, protect our property, or protect the rights, property or safety of others, or as needed to support external auditing, compliance and corporate governance functions.

We will also disclose Personal Information and Machine Data when required to do so by law, such as in response to a subpoena, including to law enforcement agencies and courts in the United States and other countries where we operate.

John Deere, Inc. 2014. Privacy and Data, *available at* https://www.deere.com/privacy_and_data/privacy_and_data_us.page. Policy statements can have value, but they are only legally enforceable if their text is incorporated by reference into a binding agreement between the farmer and the service provider. This underscores the need for some form of NDA. However,

the relative bargaining power between the farmer and the service provider will obviously vary. Negotiating the terms of "boilerplate" agreements large corporations will provide to their customers will likely require high-level collective discussions between industry groups and corporate service providers (see the Epilogue). This discussion presumes at least some parity in bargaining power between the farmer and the service provider receiving the farm data.

The following is a list of items the farmer and his or her attorney should consider in drafting an NDA for the disclosure of farm data to a service provider. These considerations are compiled from the works of Bowden (1995) and Fishman and Stim (2001). Bowden, Brian. 1995. Drafting and Negotiating Effective Confidentiality Agreements (with forms). The Practical Lawyer, 41:7, pp. 39-56.. Fishman, Stephen and Richard Stim (2001). Nondisclosure Agreements: Protecting Your Trade Secrets and More. Nolo Press.

1) Execute the agreement prior to data disclosure: Trade secret law will not protect information voluntarily disclosed or publicly available (see Uniform Trade Secret Act, § 1 above). Thus, it is critical the NDA be executed before the disclosure of any data.

2) Define who is disclosing and receiving the information: In most cases, the farmer will be the disclosing party, and the service provider will be the receiving party, though this is not necessarily always the case. In many cases, the obligations of the agreement will be defined the role of the party, so defining when those roles are triggered is important.

3) Define what information will be regarded as confidential: Blanket statements that all information disclosed by the farmer to the service provider may be ineffective as the protection of all information may be impractical or counterproductive to the services provided. As a result, the agreement should define what information is, and is not, to be kept confidential, whether by category of information or the channel by which such information is transmitted.

4) Exclude information that will not be regarded as confidential: By the same token, it may be useful to define what categories of information are not to be treated as confidential and may be disclosed without further consent from the parties. Other information may be discloseable, but only with the express written consent of the party providing the information.

5) Establish a duty to keep the information secret: Perhaps the most important portion of the agreement, an affirmative contractual duty should be established that the party receiving the information must keep it secret. On the

other side of the same coin, this portion of the agreement should also explicitly prohibit the disclosure of the information, and should also define the measures the receiving party must take to maintain the secrecy of the information. This portion of the agreement may also be accompanied by a time limit on its enforceability, which is usually defined by an event (such as execution of a release by the party providing the information, or the public disclosure of the information by that party) rather than a period of time.

6) Specifically allowed/prohibited uses of information: This section of the agreement can spell out what uses of the information are specifically allowed, and which are specifically prohibited. The farmer and his or her attorney will wish to use care in making sure that the beneficial uses of the data motivating the farmer to seek the service provider's services are not blocked by these terms.

7) Data destruction requirements: The farmer may wish to require the destruction of all data transmitted to the service provider in the event of a breach of the agreement by the service provider or some other event terminating the agreement. While there may be merit in such provisions, it should also be noted that data destruction in today's highly-interconnected computing environment may be a practical impossibility. The most one may be able to achieve is the destruction of any hardcopies of the information and the complete erasure of physical drives where the data is stored.

8) Provision for injunctive relief: Without boring the reader with a discussion of civil procedure rules, suffice it to say that proving the case for "injunctive relief" (that is, an order from a court commanding an offending party to immediately cease a harmful activity such as releasing data, as opposed to the much more common remedy of ordering the offending party to pay monetary damages to the injured party) can be both costly and time-consuming, permitting the farmer to suffer continuing damages from data disclosure until it is stopped. A provision stating that the parties both agree that injunctive relief is appropriate in the specified circumstances can drastically shorten this process and limit the expenses in securing such relief.

9) Indemnity clause: The farmer may desire a clause stating the service provider will indemnify the farmer for any of his or her expenses (or the expenses of third parties asserting a claim against the farmer) caused by the wrongful disclosure of data.

10) Integration clause: An integration clause will state the entire agreement between the parties has been reduced to writing through the NDA. The effect of the integration clause is to exclude evidence of the parties' discussions in the negotiation of the agreement and to limit the resolution of any disputes to the language in the agreement itself. If the parties agree to an integration clause, it is critical all of their concerns be addressed in the text of the agreement.

11) Attorney's fees: The "American Rule" in most civil litigation is the parties pay for their own attorney's fees, unless a statute or other legal rule overrides this presumption. Frequently, contracts override this rule and require the losing party pay the prevailing party's costs; this is usually an attempt to minimize the chance of frivolous claims by one party. Farmers should use care in the inclusion of such language since it may result in the payment of significant legal fees if they should initiate what is eventually proven to be an unsuccessful claim against the service provider.

12) Alternative Dispute Resolution (ADR) and venue provisions: The parties may want to require any dispute among them be first submitted to ADR (arbitration or mediation) before the claim may be litigated. Large corporations often prefer arbitration as it may be faster and less expensive than litigation, but a growing body of research suggests arbitration may favor the corporation over other plaintiffs. The farmer may wish to specify mediation as a first line of ADR. At the same time, many large corporations fear they will be treated unfairly at the hands of local juries, where the opponent will have "home field advantage." This may or may not be true; by the same token, if there is to be such an advantage, does the farmer wish to relinquish it?

13) Disclosure under legal process: One situation in which the receiving party may have little choice in disclosing information is when they are legally compelled to do so. However, there may be disagreement about when a party is "legally compelled" to disclose information. To provide the best possible opportunity for both parties to determine is such disclosure is indeed legally required, many attorneys recommend a fourfold approach: (a) disclosure of the information is prohibited unless the receiving party is subpoenaed or otherwise compelled by some form of legal process; (b) the disclosing party must be given as much notice as possible, allowing them to contest the legal process; (c) the receiving party must use best efforts to

cooperate with the disclosing party; and (d) the receiving party may disclose only information which, in the written opinion of its legal counsel, it is required to disclose.

14) Liquidated damages: It may be difficult (or even impossible) to determine the amount of damages that the farmer has sustained from the disclosure of protected information. As a result, the farmer may wish to define an amount of liquidated damages in advance. Liquidated damages are simply an amount, agreed to in advance of a contractual breach, to be paid if a breach is proven to have occurred. The counterpoint to liquidated damages is that they serve as both a floor and ceiling to claimed damages; even if a farmer sustained greater damages than those negotiated in the liquidated damages provision, he or she will likely be deemed to have waived any claim to a greater damage amount.

III. CONCLUSIONS

Acquiring farm data via the use of drones currently poses a number of regulatory challenges, although continued pressure on the FAA to open up more avenues for drone use may eventually ease those restrictions.

Regardless of how farm data is acquired, though, Big Data on the farm holds the promise for tools heretofore undreamt of – tools necessary for the American farmer to meet the challenges of feeding a world population of 9 billion by the end of the 21st Century. At the same time, there are many concerns about the potential misuses of Big Data. Some of these concerns may prove to be more imagination than fact, but recent history is replete with reasons for those disclosing data to have legitimate reasons for seeking the assurance of data security. At the individual level, thoughtful consideration of the advantages and disadvantages of data use and the negotiation of thorough and balanced NDAs can do much to protect farmers' data interests. At the industry level, continued discussion of these issues can lead to proactive, negotiated solutions between large service providers and the agriculture industry.

All Data, Big and Small