LEGAL ISSUES ON THE FARM DATA FRONTIER, PART I: MANAGING FIRST-DEGREE RELATIONSHIPS IN FARM DATA TRANSFERS

Shannon L. Ferrell, J.D.†

† Associate Professor and Faculty Teaching Fellow, Agricultural Law. The Author would like to acknowledge Dr. Terry Griffin of Kansas State University's Department of Agricultural Economics, Dr. John Fulton of Ohio State University's Department of Food, Agricultural, and Biological Engineering, Mr. Todd Janzen of Janzen Agricultural Law LLC in Indianapolis, Mr. Ryan Jenlink of the Conley Rose, PC firm in Plano, Texas, and Mr. Matthew Steinert of Steinert Farms, LLC in Covington, Oklahoma, who each contributed greatly to the development of this article. Perhaps the greatest contribution to this article and the Author's understanding of agricultural data systems, though, was made by Dr. Marvin Stone. Dr. Stone was a giant in the agricultural data field, contributing tremendously to the development of the Green Seeker technology that significantly advanced machine-sensing of plant health. He was also instrumental in the development of the SAE J1939 standard that forms the foundation for many of the machine data technologies at the heart of this discussion. Beyond being a giant in the field examined in this article, Dr. Stone was a mentor to myself and hundreds of other students at Oklahoma State University. He and his wife Bonnie were both killed in the tragic accident at Oklahoma State University's homecoming parade on October 24, 2016. This article is dedicated to the memory of Marvin and Bonnie Stone and to their influence on American agriculture.

I. INTRODUCTION

A. Abstract

Today's technology affords farmers the ability to instantaneously collect data about almost every facet of their cropping operations from planting through harvest. Many farmers have concerns about their rights in this data and how to balance the advantages of automatic and continuous uploading of that data to other parties such as equipment dealers, input vendors, and consultants with the potential loss of confidentiality in such transfers. The current intellectual property framework fails to provide a clear niche for farm data in the realms of trademark, patent, or copyright law. Farm data may fit within the realm of trade secret, but the fit is at best arguable. To whatever extent farm data comprises legally-protectable intellectual property owned by the farmer, producers wanting to maximize their claim of rights in farm data should carefully manage their data disclosures through agreements with three categories of those with data access: employees, vendors/consultants, and those in the landlord/tenant relationship.

B. An Introduction to the Brave New World of Farm Data

As many in Generation X learned from School House Rock, "knowledge is

power!"[1] 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 and commodity prices as well as production conditions.[2] These analytics are only as good as the data that drives them. Producers have more tools than ever to acquire data in the form of sensors and data collection systems that will continuously monitor thousands of parameters about both the farm equipment on which they reside, the environment around the equipment, and the crops over which they pass or the produce passing through them.[3] Beyond the farm gate, uploading, aggregating, and analyzing data across multiple operations, a process often referred to as "Big Data," holds the potential to generate knowledge beneficial not only to producers but numerous other segments of the agricultural industry.[4]

However, many farmers have numerous concerns about their rights with respect to the data generated by them or, in some cases, about them. This article is the first in a series of three that will addresses some of the legal concerns involved with the collection and analysis of farm data agricultural producers, equipment manufacturers, input suppliers, agricultural production consultants, and a number of third parties who house, store, or collect data either from farmers or about them. This first article, Part I in the series, deals with managing the rights to farm data in data exchanges directly between the farmer and another party providing a service directly to the farmer. Examples of this "first-degree" relationship include an equipment dealer monitoring telematics data in the context of a service agreement for a tractor or combine, or a crop consultant uploading input field prescriptions. Part II of the series will examine what happens to farm data as it is processed by proprietary software beyond its mere collection by the farmer, as well as the legal issues in "second-degree" farm data relationships; that is, what dynamics are involved when data provided by a farmer is shared by an equipment provider or consultant with a data processing services provider or a cloud storage service? In these relationships, concerns about "Big Data" begin to emerge. Part III will examine the increasing array of issues involved in "third-

1. SCHOOL HOUSE ROCK LYRICS, http://www.schoolhouserock.tv/ (last visited April 26, 2016).

2. *See* Christopher Doering, *Big Data Means Big Profits, Risks for Farmers*, USA TODAY (May 11, 2014, 1:40 PM), http://www.usatoday.com/story/money/business/2014/05/11/gannett-big-data-means-big-profits-for-farmers-but-trust-concerns-loom/8970299/.

3. *See id.*; Jenna Broughton, *How Farmers Are Harvesting Big Data*, Inc.com (July 6, 2015), http://www.inc.com/jenna-broughton/how-farmers-are-harvesting-big-data.html.

4. *See generally* Marcos Fava Neves, *The Unlimited Potential of Big Data for Agriculture*, FRUITWORLD (July 28, 2015), http://fruitworldmedia.com/index.php/production/the-unlimited-potential-of-big-data-for-agriculture/ (listing numerous ways that agricultural data can be used and collected across the industry).

degree" relationships when there may be no direct relationship between the farmer and the holder of the data because the holder of the data has not collected data from the farmer but rather about his or her operation – or about him or her personally – in the form of metadata or information gained from publically accessible points (such as aerial or satellite imagery).

In this article, the focus turns to "first-degree" farm data relationships. First, the mechanics of the data collection and sharing process will be examined along with the concerns expressed by some groups about the process and its products. Next, the rights of agricultural producers to this data will be examined under the current framework of intellectual property law. Finally, suggestions will be made for both how individual producers can use this framework to protect their rights with respect to farm data and how they can engage in the national policy discussion regarding farm data rights.

1. Data acquisition and transmission technology in agriculture

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.[5] This farm data – collectively, machine (telematics) and crop (agronomic) data – can be wirelessly uploaded to a number of parties.[6] To examine the advantages and potential challenges of this capability requires a discussion of how the data collection and transmission process works.

To explore the legal issues surrounding the rights to agricultural data, one must first explore the systems through which that data is generated, collected, and shared. In starting this exploration, one must first separate agricultural data into two distinct but related domains.

(i) Telematics Data

The first domain of agricultural data is that of "telematics" data. Although formally defined as "the branch of information technology which deals with the long-distance transmission of computerized information,"[7] for the purposes of this discussion, telematics will refer to data a machine such as a tractor, combine, or other self-propelled implement collects about itself. In other words, one could consider telematics data as "machine health" data such as engine temperature, oil

5. Broughton, *supra* note 3; Dan Bobkoff, *Seed by Seed, Acre by Acre, Big Data is Taking Over the Farm*, BUSINESS INSIDER (Sept. 15, 2015, 10:57 AM), http://www.businessinsider.com/big-data-and-farming-2015-8.

6. Bobkoff, *supra* note 5.

7. *Telematics Definition*, OXFORD DICTIONARY OF ENGLISH 1828 (3d ed. 2010).

pressure, transmission RPMs, and so on.[8]

SAE International Standard J1939 governs the configuration of most telematics systems on tractors, combines, and other self-propelled agricultural equipment.[9] J1939 was originally conceived as a standard for the configuration of Controller Area Networks (CAN) used in on-road diesel trucks' powertrains to meet Environmental Protection Agency and California Air Resources Board (CARB) emissions requirements, but has since extended to on-road and off-road diesel engines, agricultural equipment, marine diesel engines, and even stationary generator engines.[10] The J1939 standard describes how Electronic Control Units (ECUs) – embedded electronic devices that receive information from sensors embedded in the vehicle and issue control commands to a system such as the engine or transmission – exchange information with other ECUs throughout the vehicle via a physically-connected network typically referred to as a "bus."[11] A vehicle's bus relays both information (such as "current engine RPMs are X") and commands ("increase throttle to setting Y") in real time by allowing simultaneous use of the bus by multiple ECUs through a process called "multiplexing."[12] A Controller Area Network (CAN) manages the use of the bus and defines a syntax for its messages.[13] Many of the commands transmitted through the bus and the CAN use proprietary formats, meaning a third-party device cannot issue commands to the system.[14] This provides an important layer of security and safety for the vehicle. The communications procedures of J1939 enable ECUs to au-

8. *See* Rich Mattern, *Telematics Giving Farmers Increasing Equipment, Internet Options*, W. FARM PRESS (Dec. 10, 2010, 3:10 PM), http://westernfarmpress.com/equipment/telematics-giving-farmers-increasing-equipment-internet-options.

9. SAE INT'L, THE SAE J1939 COMMUNICATIONS NETWORK: AN OVERVIEW OF THE J1939 FAMILY OF STANDARDS AND HOW THEY ARE USED 1 (2011), http://www.sae.org/misc/pdfs/J1939.pdf.

10. MARK R. STEPPER, STEVEN R. BUTLER & GEORGE G. ZHU, SAE INT'L, ON-BOARD DIAGNOSTICS, A HEAVY DUTY PERSPECTIVE 1 (SAE Technical Paper Series No. 951947, 1995), http://papers.sae.org/951947/; *See also* SAE WHITE PAPER, *supra* note 10, at 5; Interview with Dr. Marvin Stone (June 10, 2015) (on file with author). *See generally* MARK R. STEPPER, SAE INT'L, J1939 SERIAL VEHICLE NETWORK EXPLANATION AND TUTORIAL 1 (SAE Technical Paper Series No. 972757, 1997), http://papers.sae.org/972757/.

11. NAT'L INSTRUMENTS, ECU DESIGNING AND TESTING USING NATIONAL INSTRUMENTS PRODUCTS 1 (Nov. 7, 2009), http://www.ni.com/white-paper/3312/en/.

12. *See id.*

13. MARCO DI NATALE ET AL., UNDERSTANDING AND USING THE CONTROLLER AREA NETWORK COMMUNICATION PROTOCOL: THEORY AND PRACTICE 1 (2012).

14. A. Munack & H. Speckmann, *Communication Technology is the Backbone of Precision Agriculture*, AGRIC. INT'L: CIGR J. OF SCI. RES. & DEV., May 2001, at 6, https://ecommons.cornell.edu/bitstream/handle/1813/10257/Munack%20Invited%20Paper.pdf?sequence=1&isAllowed=y.

tomate many functions of the equipment, improving performance and reliability) while also making more information available to the operator through dashboard displays that connect to the network.[15]

Historically, telematics systems looked inward to the machine itself, but that perspective continues to undergo radical change. First, telematics systems continue to evaluate a growing number of parameters external to the vehicle that could impact its performance through machine-vision tools such as radar and image processing,[16] as well as tools to sense the ambient climate around the equipment.[17] Second, and more important to this discussion, the telematics systems can now automatically share the information they collect via wireless communications. A growing number of tractors, combines, and other self-propelled machines roll off the assembly line with cellular modems attached to their tractor bus.[18] These modems continuously provide data to designated recipients such as the equipment owner and/or a dealer, enabling them to quickly diagnose machine health along with equipment failures or even prevent them.[19] Generally, telematics systems do not accept outside commands via these cellular modems, but other industries have modified that functionality for a number of management purposes.[20] For example, trucking companies (for whom the J1939 standard was initially created) have the ability to remotely limit horsepower to accommodate engine warranty specifications, to increase trucks' horsepower output in mountainous regions, or reduce maximum speed when the vehicle is in a state with a lower speed limit.[21]Agricultural operations could use the same equipment management procedures, although no major agricultural equipment manufacturers currently offer such remote management systems.[22]

(ii) Agronomic Data

The second domain of agricultural data is that of "agronomic data." If

15. *See generally* SAE WHITE PAPER, *supra* note 9; STEPPER, *supra* note 10.

16. *See* J.D. Turner & L. Austin, *Sensors for Automotive Telematics*, 11 MEAS. SCI. TECHNOL. R58 (2000).

17. *Weather Telematics Transforms Truck Fleets into National Sentinels*, MOBILE DEVICES, http://www.mobile-devices.com/case-studies/weather-telematics-transforms-truck-fleets-into-national-sentinels/ (last visited Apr. 26, 2016).

18. *See, e.g.*, Quentin Hardy, *Working the Land and the Data*, N.Y. TIMES, Nov. 30, 2014, http://www.nytimes.com/2014/12/01/business/working-the-land-and-the-data.html?_r=0.

19. Mattern, *supra* note 9.

20. *See* Interview with Dr. Marvin Stone, *supra* note 10.

21. *See id.*

22. Interview with Kevin Thedford, Precision Agriculture Specialist, P&K Equipment (June 30, 2015) (on file with author).

telematics data describes machine health, one could consider agronomic data as describing crop health or field conditions.[23] Collected by sensors targeting the crop and soil rather than the machine, agronomic data could include information from moisture and temperature sensors and yield monitors.[24] Most would also consider "as applied" information from sprayers and planters as agronomic data, such as geo-referenced information about the type and rate of application (be it by seed variety, spacing, and population or by chemical applied and rate).[25] Put another way, the domain of telematics data generally looks inward to the implement (though that is likely to change in the future), while agronomic data looks outward to the crop and its environment.[26]

Although distinct from telematics data, farmers frequently generate agronomic data from implements pulled by their tractors or input from other sources (including user inputs for parameters such as seed variety and targeted seed population rate or fertilizer and application rate), thus creating a need for implements' sensor systems to communicate with those of the tractor, thus bridging the domains of telematics and agronomic data.[27] To this end, the International Organization for Standardization (ISO) created ISO Standard 11783, sometimes called the "ISOBUS" standard.[28] ISO 11783 applies to self-propelled equipment (such as combines) and tractors, and defines two buses for its networks: a tractor bus and a "tractor/implement" bus.[29] The tractor bus reflects the J1939 bus discussed above (indeed, the ISO 11783 standard builds upon the J1939 standard; in essence an ISO 11783 tractor bus is typically a J1939 bus on an agricultural vehicle), connecting the systems operating the tractor or the powertrain of the machine.[30] The tractor/implement bus extends from front of the tractor or self-propelled implement back through the hitch via a standard connector and through

23. Todd Janzen, *What Makes Agronomic Farm Data Different from Other Forms of Intellectual Property?*, JANZEN AG LAW BLOG (May 10, 2015), http://www.janzenaglaw.com/2015/05/what-makes-agronomic-data-unique.html.

24. *Id.*

25. *Id.*

26. *Id.*

27. *See generally* Dr. Marvin Stone, *ISO 11783 Part 10 Task Controller and Management Information System Data Interchange: A Brief Overview*, AM. SOCIETY OF AGRIC. & BIOLOGICAL ENGINEERS (Jan. 5, 2011), http://www.shieldedpair.net/downloads/ISO%2011783%20Part%2010.pdf.

28. *See generally* INT'L ORG. FOR STANDARDIZATION, ISO DRAFT INTERNATIONAL STANDARD ISO/DIS 11783: TRACTORS AND MACHINERY FOR AGRICULTURE AND FORESTRY – SERIAL CONTROL AND COMMUNICATIONS DATA NETWORK (hereinafter referred to as ISO 11783) (2012).

29. *Id.* §§ 6.3 – 6.4 (discussing connection of network architectures.)

30. *See* SAE WHITE PAPER, *supra* note 9, at 5; *see also* Stone, *supra* note 27.

the implements.[31] Thus, the agronomic sensors installed on an implement (such as flow meters on a sprayer, plant population sensors on a seeder, or yield monitors on a combine) connect to the tractor/implement bus.[32]

Operating the vehicle and implement combination as an integrated unit requires a connection between the tractor bus and tractor/implement bus, which is provided by a translator/gatekeeper called the "tractor ECU."[33] The tractor ECU might share information from the tractor with the implement such as PTO speed, ground speed, or engine RPM if the information is relevant to the implement's operation.[34] However, ISO 11783 also provides for a proprietary security mechanism within the tractor ECU to prevent the implement from giving the tractor commands unless it is authorized to do so.[35]

(iii) Telematics and Agronomic Data in Precision Agriculture

How do the domains of telematics and agronomics data converge in precision agriculture applications? Consider the example of a variable-rate application of fertilizer. A crop consultant may examine soil and yield maps (both of which represent agronomic data) and devise an application map called a "Work Order" specifying the rates of fertilizer application for the various areas of a particular field.[36] The consultant likely creates this Work Order then sends the data file providing instructions to the variable-rate sprayer the farmer or custom applicator will use for the application. The data file contains the information needed for the machine to execute a "Task."[37] Frequently, task data files use a Georeferenced Tagged Image File Format (GeoTIFF) to provide these instructions.[38] The

31. Marvin Stone, Presentation, *National Engineering Research Center for Information Technology in Agriculture: Introduction to ISO 11783* (November 16, 2012) (presentation on file with author).

32. *Id.*

33. *See* Stone, *supra* note 27 (diagram of the integrated tractor-implement bus network).

34. *See* ASS'N OF EQUIP. MFRS., ISOBUS COMPLIANCE TEST PROTOCOL 89 – 91 (Oct. 2005), https://www.aem.org/Documents/NAIITF/Documents/ISOBUS%20Compliance%20Test%20Protocol_1_0.pdf (tractor ECU protocol sheet and application layers showing the information that can be shared).

35. *See* AGRIC. INDUS. ELEC. FOUND., AEF DRAFT INTERNATIONAL GUIDELINE: ISOBUS IMPLEMENTATION SPECIFICATION FUNCTIONALITY TIM 16 (June 18, 2015).

36. *Work Order Definition*, AG GATEWAY, http://agglossary.org/wiki/index.php?title=Work_order (last visited Apr. 26, 2016).

37. *Task Definition*, AG GATEWAY, http://agglossary.org/wiki/index.php?title=Task (last visited Apr. 26, 2016).

38. *Georeference System Definition*, AG GATEWAY, http://agglossary.org/wiki/index.php?title=Georeference_system (last visited Apr. 26, 2016). *See generally GeoTIFF Specifications*, GEOTIFF,

GeoTIFF comprises three sub-files: a SHP file containing a vector description of the graphical objects in the file (the shape of the field and the polygons that define the pieces into which the field is broken, for example), a DBF file containing a small database of instructions ("while the implement is in polygon 1, apply fertilizer at a rate of 50 pounds per acre, while the implement is in polygon 2, apply fertilizer at a rate of 45 pounds per acre, etc.) and an index file allowing fast lookup of objects in the SHP file.[39] The consultant or the farmer may load the Task data file to the sprayer's task controller.[40]

As the farmer moves through the field, the task controller receives information from the Global Navigation Satellite System (GNSS) receiver telling it the location, orientation, and velocity of the implement and enabling the task controller to implement the instructions contained in the task data file.[41] Note that this information likely involves pieces of information from the tractor's telematics system.[42] With all of this information, the task controller positions each controllable element of the implement on the SHP map and reads the map data, sending a message to the implement to operate the element in a defined manner.[43] The implement sensor feedback provides the actual rate it applied, and the task controller creates an "as-applied map" from that data.[44] This record can be exported back to the farmer and/or consultant desktop as a task data file.

(iv) Transmission of Farm Data

A farmer or consultant could upload a task data file or download an as-applied map by physically connecting a storage device (such as a USB drive) to the task controller through a connection on the tractor/implement bus.[45] However, that same data transfer could be accomplished by adding a cellular modem to

(http://www.remotesensing.org/geotiff/spec/geotiffhome.html (last modified Dec. 28, 2000).

39. Sk. Sazid Mahammad & R. Ramakrishnan, *GeoTIFF – A Standard Image File Format for GIS Applications*, GISDEVELOPMENT, http://www.gisdevelopment.net/technology/ip/mi03117pf.htm (last visited Apr. 26, 2016) (description of this structure in terms of a header/directory (Image File Directory)/data framework).

40. *See* Andy Beck & Hans Nissen, *ISOBUS Task Controller Workshop*, ASS'N OF EQUIP. MFRS., 7 - 11 (June 4, 2008), http://aem.org/Documents/NAIITF/Documents/NAIITF-ISOBUSWorkshop-TaskController.pdf (outlining the task controller process).

41. *See generally id.* at 10.

42. Interview with Dr. Marvin Stone, *supra* note 10.

43. *See generally* Beck & Nissen, *supra* note 40 (detailed outline of the task controller process).

44. *Id.*

45. *See generally id.* at 8.

the tractor/implement bus or to the tractor ECU.[46] With such a connection, not only could data be shared throughout the tractor-implement combination in real time; it could also be shared with a dashboard at the farm's headquarters and/or with a consultant, who could make "on-the-fly" adjustments and upload prescription adjustments in real time as well.[47] The system could also transmit the data to a cloud storage service for future use and analysis.[48]

Many farmers select specific systems and service packages specifically to share their telematics and agronomic data with a third party, but others worry about how other parties could take such data without their consent. What pathways exist for such a taking? First, could someone "hack" the tractor/implement bus by physically connecting to the system? The answer is, 'theoretically, yes."[49] A number of commercially-available technologies allow farmers to plug into the network and access CAN messages directly. For example, one could purchase a CAN message reader to read machine diagnostic codes for repairs.[50] Someone wishing to "steal" data would likely not want to be present to read the data, though, and would likely prefer to use a CAN data logger coupled with a device to wirelessly transmit the data. Many data loggers are available to the public as well; for example, the "Snapshot®" device used by Progressive Insurance for some insurance programs is simply a CAN data logger plugged into a vehicle's On-Board Diagnostic (OBD-II) port.[51] While such an approach would work for standard messages transmitted over the bus, it would not work for proprietary messages. To decode such messages, the prospective hacker would have to develop a system for decoding the information being provided from the task controller for the implement, and that task would take almost as much work (if not more) than the work in developing the task controller system in the first place.[52] Note, though, that several companies now provide means for re-engineering proprietary CAN messages (such as those related to crop yield) so farmers can au-

46. *See generally* Mattern, *supra* note 8.

47. *Id.*

48. *See, e.g.*, *Ag Management Solutions*, *Advanced Farming Systems*, CASE IH AGRIC., http://www.caseih.com/northamerica/en-us/products/advanced-farming-systems (last visited Apr. 26, 2016); *AgFiniti Product Group*, AG LEADER, http://www.agleader.com/products/agfiniti/ (last visited Apr. 26, 2016) (examples of potential applications of wireless farm data transmission and management); JOHN DEERE, https://www.deere.com/en_US/products/equipment/ag_management_solutions/ag_management_solutions.page (last visited Apr. 26, 2016).

49. Interview with Dr. Marvin Stone, *supra* note 10.

50. Interview with Dr. John Fulton, Ohio State Univ. Dep. of Food, Agric., and Biological Eng., (July 6, 2015) (on file with author).

51. *See Snapshot® Terms and Conditions*, PROGRESSIVE CORP., https://www.progressive.com/auto/snapshot-terms-conditions/ (last visited Apr. 26, 2016).

52. Interview with Dr. Marvin Stone, *supra* note 10.

tomatically transfer yield data to the cloud; such technology could also be used to decode other proprietary information.[53] Additionally, as discussed above, the GNSS receiver in most systems connects directly to the task controller. As a result, a "bug" might receive information about the commands sent to the implement, but without the associated location data, the command information is rendered meaningless.[54] The bug would require its own GNSS receiver along with implement data (the configuration and dimensions of the implement), which today could be done for relatively modest equipment cost. Suffice it to say that obtaining agronomic data via a physical connection to an implement poses a task manageable for someone knowledgeable in ISO 11783 technology.[55] However, building and deploying such a device poses a significant amount of effort (to say nothing of the potentially-criminal trespass involved in deploying it) in relation to the prospect of collecting data on only one farm.

Admittedly, most producers rightly put little thought into their systems being physically hacked but worry instead about their data being accessed through an intercepted cellular signal. First, virtually all cellular signals are encrypted when transmitted and decrypted at the cellular tower; without the decryption key, interpreting any data transmitted would be quite difficult (although not impossible for a sophisticated hacker; recent news has highlighted the ability of some governmental agencies to do so).[56] The use of data encryption through a secure socket layer ("SSL") protocol by the farmer and his or her service provider adds another difficult-to-break security barrier to interception of the data.[57]

Some producers also worry that another party could be feeding harmful commands to their equipment through a similar signal. Beyond the encryption issues discussed in the preceding paragraph, a number of built-in safety features make this difficult.[58] First, as mentioned previously, the ISO 11783 standard provides a safety mechanism to prevent harmful commands being issued from

53. Interview with Dr. John Fulton, *supra* note 50.

54. Interview with Dr. Marvin Stone, supra note 10.

55. *See generally* Mikko Miettien et al., IMPLEMENTATION OF ISO 11783 COMPATIBLE TASK Controller (XVI CIGR World Congress, 2006), http://users.aalto.fi/~ttoksane/pub/2006_CIGR20062.pdf.

56. *See, e.g.*, Craig Timberg & Ashkan Soltani, *By Cracking Cellphone Code, NSA Has Ability to Decode Private Conversations*, WASH. POST, Dec. 13, 2013, http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html.

57. *See Secure Socket Layer (SSL)*, ENCYLOPEDIA OF CRYPTOGRAPHY & SECURITY 1135 (Henk C.A. van Tilborg, Sushil Jajodia, eds., 2d ed. 2011).

58. Interview with Dr. Marvin Stone, *supra* note 10; Interview with Dr. John Fulton, *supra* note 50.

the implement to the tractor.[59] Second, the cellular modems connected to the tractor bus for sharing machine health information either cannot send commands to the ECUs in the system (because of the physical configuration of the system) or the ECUs are programmed not to accept commands from the modem.[60] As mentioned above, though, systems can be configured to accept commands in the J1939 standard, such as truck powertrain management systems.[61] Again, though, most agricultural systems are not configured to accept such commands, although this may change in the near future.

2. The Promise and Perceived Peril of Farm Data

The agricultural industry stands on the front line with other industries in the 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.[62] Improvements in farm equipment data acquisition systems 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.[63] 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.[64]

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 a power to manage elements of agricultural production heretofore unimaginable.[65] Cellular modem technology means producers can instantly and continuously share data with crop advisors and other consultants.[66] 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 seed-

59. Interview with Dr. Marvin Stone, *supra* note 10.

60. Interview with Dr. John Fulton, *supra* note 50.

61. STEPPER & BUTLER, *supra* note 10.

62. *See generally* Neves, *supra* note 4.

63. See Mattern, *supra* note 8 (troubleshooting of equipment problems remotely); Bobkoff, *supra* note 5 (describing data that can be collected and read from crop sensors).

64. John Deere, Inc., *Farm Forward*, YOUTUBE (Aug. 23, 2012), https://www.youtube.com/watch?v=jEh5-zZ9jUg.

65. *See generally* Neves, *supra* note 4 (discussing all the data that can be measured from agriculture).

66. Mattern, *supra* note 8.

ing, fertilizer, pesticide, and cultivation practices.[67] Lest one think any of these prospects to be far-fetched, many of them are (or soon will be) a reality.[68] 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.[69]

Any new technology carries potential harms, whether real or imagined. If farm data posed nothing but advantages, its discussion would not have the fevered pitch currently seen across virtually every agricultural media source.[70] As with any tool, farm data is neither inherently good nor evil – it is simply a tool – and as with any tool, its benefits and dangers lie in how one uses it.[71]

Recent history suggests many of the real threats in data transfers 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.[72] As discussed above, the nature of agricultural data means PII itself would rarely, if ever, be transmitted to a service provider.[73] Nevertheless, to the extent producers regard agricultural data as proprietary, their concerns about its disclosure naturally invites a review of the release or theft of proprietary information in other sectors.[74] 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.[75] 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 com-

67. *Id.*

68. *See generally id.*

69. Margy Eckelkamp, *John Deere Partners with Open Platform*, AGWEB.COM (Dec. 6, 2013, 6:35 PM), http://www.agweb.com/article/john_deere_partners_with_open_platform_NAA_Margy_Eckelkamp/.

70. *See, e.g.*, Mattern, *supra* note 8; Neves, *supra* note 4 (examples of media sources covering farm data).

71. *See generally* JOHN STRINGER, SOPHOS, PROTECTING PERSONALLY IDENTIFIABLE INFORMATION: WHAT DATA IS AT RISK AND WHAT YOU CAN DO ABOUT IT 1 – 2 (2011).

72. *See generally id.*

73. *Id.*

74. *See* Doering, *supra* note 2; Bobkoff, *supra* note 5 (discussing the data security concerns of farmers).

75. *See, e.g.*, Julianne Pepitone, *5 of the Biggest-ever Credit Card Hacks*, CNN MONEY (Jan. 12, 2014, 7:11 PM), http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/.

pany, 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).[76] 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.[77] Most agricultural data disclosed to a service provider is likely in the form of telematics data, raw data regarding crop production, GIS information about the farm, and the like. Additionally, financial systems such as credit card payment mechanisms are ripe targets for active attacks since it is relatively easy to get the value out of credit card information. Conversely, it would be difficult for a hacker to make a quick buck from agricultural data. As a result, systems storing agricultural data are less likely to be directly attacked, but farmers are understandably concerned that PII may be stolen if, for example, their vendor account information is somehow linked to their agricultural data or if their account information is stored with a third party that is a "juicier" target.[78] This significantly reduces the risk of identity theft by someone obtaining the agricultural data by illicit means. Nevertheless, farmers should still be aware of the data they are disclosing to providers as discussed later in this article.

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.[79] 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.[80] 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 hold-

76. *Id.*

77. *See generally* Phil McKenna, *My Identity Was Stolen. Here's How They Did It*, NOVA NEXT (Nov. 20, 2013), http//www.pbs.org/wgbh/nova/next/tech/science-of-identity-theft/.

78. *See, e.g.*, Michael Doyle, *Stolen USDA Computers May Have Left Farmers at Risk*, INFOSEC NEWS (Mar. 12, 2007), http://seclists.org/isn/2007/Mar/60.

79. See STRINGER, *supra* note 71.

80. Sara Wyant, *Farm Groups File Lawsuit to Stop EPA Release of Farmers' Personal Data*, AGRI-PULSE (July 8, 2013), http://www.agri-pulse.com/Farm-groups-file-lawsuit-to-stop-EPA-release-of-farmers-personal-data-07082013.asp.

ing a farmer's data to disclose the data as an aid to their case, again even if such disclosure was not legally required.

Regardless of their respective probabilities, these scenarios pose concerns weighing on a number of farmers as they make management decisions about their production systems and their integration of the new farm data tools. From a legal perspective, what can be done to protect farm data as it is shared with parties in a first-degree relationship with the farmer?

II. THE LEGAL FRAMEWORK FOR FARM DATA PROTECTION

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.[81] Thus, the first place many look for a means of protecting one's data from misappropriation and/or misuse is the property right system.[82] This requires one to examine who holds property rights; that is, who "owns" farm data.[83] Although a seemingly simple question, finding an answer creates quite a challenge as traditional notions of property ownership do not fit neatly 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.[84] Some of these interests do not fit, or at least do not fit well, with data ownership.[85] 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 other possessors, just as the value of a book to one person may not be diminished by the fact other people own the same book.[86] 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?[87]

Since data belongs to the realm of intellectual property, the intellectual

81. *See* Ashley Newhall, *Big Data: What's the Big Deal?*, MD. RISK MGMT. EDUC. BLOG (Feb. 4, 2015), http://www.aglaw.umd.edu/blog/big-data-whats-the-big-deal.

82. *See id.*

83. *Id.*

84. *Id.*

85. *Id.*

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

87. Rodney J. Petersen, *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 (last visited Apr. 27, 2016).

property framework serves as a useful starting point to define what rights a farmer might have to their farm data.[88] In discussing the legal protections available under the American legal system, intellectual property can be divided into four categories: (1) trademark, (2) patent, (3) copyright, and (4) trade secret.[89] The first three areas compose the realm of federal intellectual property law defined by the grant of legislative authority to Congress under the Constitution.[90] 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

Trademark fails to provide a viable farm data protection tool. The Federal Trademark Act[91] (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."[92] Examples of trademark include product names, such as Coca-Cola® or the design of its contoured bottle.[93] 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[94] (Patent Act) states "[w]hoever 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 thereforFalse"[95] Generally, for an invention to be patentable, it must be useful (capable of performing its intended purpose), novel (different from existing knowledge in the

88. Tiffany Dowell, *Big Data on the Farm (Part II): What Laws Might Protect it?*, TEX. AGRIC. LAW BLOG (Sept. 8, 2015), http://agrilife.org/texasaglaw/2015/09/08/big-data-on-the-farm-part-ii-what-laws-might-protect-it/.

89. *Id.*

90. U.S. CONST. art. I, § 8, cl. 8.

91. The Federal Trademark Act, 15 U.S.C. §§ 1051–1141n (2012).

92. *Id.* § 1127.

93. *See generally* THE COCA-COLA COMPANY, http://www.coca-colacompany.com/history (last visited May 22, 2016) (information regarding the Coca-Cola name and the bottle design as trademarks).

94. The Patent Act, 35 U.S.C. §§ 1–376 (2012).

95. *Id.* § 101.

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).[96] Patent serves as a poor fit for a model of farm data ownership since it protects inventions.[97] Raw data, such as farm data, fails to satisfy the definition of invention under the Patent Act as discussed in Digitech Image Technologies, LLC v. Electronics for Imaging, Inc., "Data in its ethereal, nonphysical form is simply information that does not fall under any of the categories of eligible subject matter under section 101 [of the Patent Act]."[98]

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.[99] Further, while data itself may not be patentable, one may question whether farm data evidences a potentially-patentable process, also discussed below.

3. Copyright

The federal Copyright Act[100] states the following:

> (a) 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:
> (1) literary works;
> (2) musical works, including any accompanying words;
> (3) dramatic works, including any accompanying music;
> (4) pantomimes and choreographic works;
> (5) pictorial, graphic, and sculptural works;
> (6) motion pictures and other audiovisual works;
> (7) sound recordings; and
> (8) architectural works.[101]

96. *See id.* §§ 102, 103.

97. *Id.* § 101.

98. *Digitech Image Technologies, LLC v. Electronics for Imaging, Inc.*, 758 F.3d 1344 (Fed. Cir. 2014).

99. SAE WHITE PAPER, *supra* note 9, at 5.

100. 17 U.S.C. §§ 10 – 1332 (2012).

101. *Id.* § 102(a)(1) – (8).

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.[102] Second, the term "original works of authorship" has been interpreted to require some element of creative input by the author of the copyrighted material.[103] This requirement was highlighted in the case of Fiest Publ'ns, Inc. v. Rural Tel. Serv. Co., where the U.S. Supreme Court held the Copyright Act does not protect individual facts.[104]

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.[105] 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.[106] 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.[107]

> It is this bedrock principle of copyright that mandates the law's seemingly disparate treatment of facts and factual compilations. "No one may claim originality as to facts." This is because facts do not owe their origin to an act of authorship. The distinction is one between creation and discovery: The first person to find and report a particular fact has not created the fact; he or she has merely discovered its existence. To borrow from Burrow-Giles, one who discovers a fact is not its "maker" or "originator." "The discoverer merely finds and records." Census takers, for example, do not "create" the population figures that emerge from their efforts; in a sense, they copy these figures from the world around them. Census data therefore do not trigger copyright because these data are not "original" in the constitutional sense. The same is true of all facts—scientific, historical, biographical, and news of the day. "They may not be copyrighted and are part of the public domain available to every person."
>
> Factual compilations, on the other hand, may possess the requisite originali-

102. *Id.* § 102(a).
103. *Id.*
104. Fiest Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 350 – 51 (1991).
105. *Id.* at 342.
106. *Id.* at 363 – 64.
107. *See id.* at 344 – 50.

> ty. The compilation author typically chooses which facts to include, in what order to place them, and how to arrange the collected data so that they may be used effectively by readers. These choices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws. Thus, even a directory that contains absolutely no protectible (sic) written expression, only facts, meets the constitutional minimum for copyright protection if it features an original selection or arrangement.[108]

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 with an original layout of the facts about the element, or a Yellow Pages® ad with ABC Plumbing's number along with a graphic and description of their services are.[109]

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.[110] Further, vigorous debate continues over the extent of copyright protection and ownership for "works" created by copyrighted works such as software embedded in agricultural equipment.[111] 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.

B. Farm data as a potential trade secret

While trademark, patent, and copyright do not appear to fit as models for farm data ownership and protection, trade secret has the potential to fit the bill. However, defining whether farm data (or any information, for that matter) constitutes a "trade secret" presents a challenge, as courts routinely make observations such as "[t]he determination of whether information constitutes a trade secret is a highly fact-specific inquiry"[112] and "[the] same information that qualifies as a

108. *Id.* at 347 – 48 (citation omitted).

109. *See generally id.* (facts and data that would not copyrightable per the holding of the case).

110. *See generally id.* at 340.

111. *Compare* JOHN DEERE, INC., LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. 1201 (2014), http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf, *with* Kyle Weins, *We Can't Let John Deere Destroy the Very Idea of Ownership*, WIRED (April 21, 2015), http://www.wired.com/2015/04/dmca-ownership-john-deere/.

112. AMY E. DAVIS ET AL., GUIDE TO PROTECTING AND LITIGATING TRADE SECRETS 15 (Sarah Forbes Orwig ed., 2012) (quoting Thermodyne Corp. v. 3M Co., 593 F. Supp. 2d 972,

trade secret under one set of facts may not be afforded protection under a different set of facts."[113] It is also worth noting with regard to the earlier discussion of whether farm data can even be "owned" that trade secrets have not always been regarded universally as "property" subject to ownership.[114]

For the vast majority of its existence as a distinct legal concept, trade secret was a creature of the common law.[115] The Restatement of Torts sought to collect much of that common law and provided "[a] trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[116] The Restatement of Torts ceased coverage of the topic of trade secret in 1979 "having concluded that it was no longer properly classified as a species of tort law."[117] Then, in 1995, the reporters of the Restatement (Third) of Unfair Competition began integrating coverage of trade secret into their publication.[118] The Restatement (Third) of Unfair Competition defined trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[119] Then, the National Conference of Commissioners on Uniform State Laws (observing a number of then-recent cases reflecting the need to clarify the doctrines of trade secret law relative to other bodies of intellectual property law and the inconsistencies among state laws) sought to codify and clarify much of the common law of trade secret and authored the Uniform Trade Secret Act in its first form in 1979, later amending the uniform law in 1985.[120] As of this writing, all but two states have adopted the Uniform Trade Secrets Act,[121] (hereinafter UTSA). The trend appears to be towards reliance on the UTSA, although courts continue to reference frequently both the Restatement of Torts and the Restatement (Third) of Unfair Competition in handling trade secret matters. To an extent, this stands to reason

986 (N.D. Ohio 2008)).

113. *Id.* (quoting N. Elec. Co. v. Torma, 819 N.E.2d 417, 425 (Ind. App. Ct. 2004)).

114. *See generally* 1 ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS §§ 1.01 – 1.09 (2013).

115. *See* JAMES POOLEY, TRADE SECRETS § 2.01[1] (1997).

116. RESTATEMENT OF TORTS § 757 cmt. b (1939).

117. POOLEY, *supra* note 115, at § 2.02[1].

118. *Id.*

119. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

120. *See generally* National Conference of Commissioners on Uniform State Laws, UNIFORM TRADE SECRETS ACT WITH 1985 Amendments §§ 2, 3 (1985) [hereinafter USTA]; POOLEY, *supra* note 115, at § 2.03[3].

121. *Legislative Fact Sheet – Trade Secrets Act*, UNIFORM LAW COMMISSION (2015), http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (Every state but Massachusetts and New York have adopted the UTSA in some form).

as the UTSA sought to codify the existing body of trade secret law, and as a result courts have continued to look to the Restatement of Torts in interpreting the UTSA.[122] Under the UTSA, 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.[123]

Attempting to harmonize the definitions of trade secret from the Restatement of Torts, the Restatement (Third) of Unfair Competition, and the UTSA, Pooley proposed the following:

> A trade secret has four aspects. First, it must consist of qualifying information; that is, one must be able (at least in general terms) to articulate what it is in such a way that it may be distinguished from general knowledge and skill. Second, it must be secret, in the sense that it is not well known or easy to compile. Third, the owner must have made reasonable efforts to preserve secrecy. Fourth, the secret must have value as reflected in some competitive advantage that it gives to the owner.[124]

Since Pooley's definition provides a framework for analyzing a prospective trade secret attempting to encompass the spectrum of trade secret definitions, the following discussion analyses farm data within it.

1. Qualifying information

First, does farm data consist of qualifying information? Certainly all of the above-referenced definitions include "information" and one might simply conclude since farm data is clearly information, this element is satisfied. However, all of the definitions at least imply a requirement of something more than raw information.[125] For example, courts demonstrate a strong predisposition to protection of "business information" such as business methods such as market surveys, business plans, and service models.[126] That line of reasoning seems more analogous to a farmer's marketing plans or business analyses than farm data itself,

122. POOLEY, *supra* note 115, at § 2.02[1], § 2.03[3].
123. UNIF. TRADE SECRETS ACT § 1(4)(i)-(ii) (UNIF. LAW COMM'N 1985).
124. POOLEY, *supra* note 115, at § 4.01[1].
125. *See* UTSA § 1(4)(i)-(ii); POOLEY, *supra* note 115, at § 4.01[1].
126. POOLEY, *supra* note 115, at § 4.02[1].

though. If one argues farm data collectively represents the embodiment of a process of growing a crop rather than simply comprising descriptive information about the crop, one might attempt to leverage the cases demonstrating what appears to be a predisposal of courts to grant trade protection to process information.[127] Perhaps the strongest analogy between farm data and information found to present a protectable trade secret comes from cases protecting research information demonstrating both what does and does not work in producing a product.[128] In any case, one may propound a colorable argument farm data satisfies the definition of "information." Further, whether farm data constitutes "information" may be the least important element of the analysis; its use and secrecy may carry far more weight, as discussed below.

2. Secret information

Second, does farm data comprise "secret" information, not generally known or readily compiled by another party? Information representing common knowledge in an industry or "trivial advances in known formulas or processes" fail to satisfy this element.[129] Neither can information readily obtained from a number of publically accessible sources be regarded as a trade secret. Conversely, information solely within the possession of its creator (or discoverer) and unavailable elsewhere resonates with the very essence of trade secret; "[a]s the difficulty of ascertainment increases, the information becomes qualified as a trade secret."[130] Absent some affirmative effort by the farmer or an equipment/input vendor to publish farm data, the data likely does not enter the public domain, at least at any level of granularity beyond the farm level as disclosed in reports made to agencies like USDA such as FSA disclosures or to EPA in the form of permit applications and compliance reports.[131] Further, any protectable trade secret in farm data likely lies in the telematics and agronomic data of an agricultural operation, and not the farm-level reports submitted to such agencies. Putting aside the growing number of ways third parties can acquire data about farm operations without any affirmative acts of disclosure by the farmer (such as aerial / satellite imagery or advanced terrestrially-based sensors – the topic of another article) farm data likely remains a secret as defined by this second element.[132] However, the continuous and automated transmission of that data calls into ques-

127. MILGRIM & BENSEN, *supra* note 114, at §§ 1.01 – 1.09.

128. POOLEY, *supra* note 115, at § 4.02[3] (citing Metallurgical Inds., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1203 (5th Cir. 1986)).

129. *See* MILGRIM & BENSEN, *supra* note 114, at §§ 1.01 – 1.09.

130. POOLEY, *supra* note 115, at § 4.04[3].

131. *Id.* at § 4.04[3][a].

132. *Id.* at § 4.04[3].

tion that secrecy and leads directly to the analysis of the third element.

3. Efforts to preserve secrecy

Thus, third, have farmers made reasonable efforts to preserve farm data's secrecy? Anyone in the legal profession naturally cringes at the word "reasonable" since it so often invokes fears of a vague balancing test far, far removed from bright-line rules. Trade secret protection under the UTSA requires "efforts that are reasonable under the circumstances to maintain [the trade secret's] secrecy,"[133] while the Restatement of Torts takes into account "the extent of measures taken. . . to guard the secrecy of the information."[134] The Restatement (Third) of Unfair Competition takes a similar approach although it appears to regard efforts taken to preserve secrecy as a proxy for the value of the secrets themselves:

> Precautions taken to maintain the secrecy of information are relevant in determining whether the information qualifies for protection as a trade secret. . . Whether viewed as an independent requirement or as an element to be considered with other factors relevant to the existence of a trade secret, the owner's precautions should be evaluated in light of the other available evidence relating to the information's value and secrecy of the information. Thus, if the value and secrecy of the information are clear, independent evidence of specific precautions taken by the trade secret owner may be unnecessary.[135]

Can one conceivably maintain secrecy with respect to information shared with another party via the automated and continuous transmittal of digital data? Traditional security measures such as physically sequestering the information in a locked container, labeling it "CONFIDENTIAL," and requiring employees to "check out" simply do not apply to data in this form.[136] Unfortunately, the rapid expansion of the digital frontier, both globally and within the agriculture industry, affords few guiding precedents as to what security measures will suffice as "reasonable" though one may draw analogies from tangible security measures deemed sufficient by courts to their digital equivalents.[137] Although a more detailed discussion of these measures appears later in this article, for now, these measures could include use of proprietary data formats (encoding data while onboard the implement), encrypted transmission (encoding data while transmitted), requiring the recipient of the data to enter into non-disclosure agreements, and

133. DAVIS ET AL., *supra* note 112, at 12 (quoting UTSA, § 1(4)).
134. *Id.* (quoting RESTATEMENT OF TORTS § 757 cmt. b (1939)).
135. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. g (1995).
136. *See* DAVIS, *supra* note 112, at 72 – 77.
137. *See id.*

requiring password access for anyone to access the data.[138] One may not have to provide the same level of protection for corn yield maps as nuclear launch codes, though. Courts have repeatedly held the level of security required be proportionate to the value of the secret.[139] The guiding principles seem to boil down to simple cost-benefit analysis. Within a very wide band of discretion, the trade secret owner is to consider the value of the secret, the nature of the threat to disclosure, and the cost of any particular security measure.[140]

4. Economic value / competitive advantage

Courts often link the "reasonable" efforts of a putative trade secret's owner to keep the information to the fourth element: does farm data have value in providing a competitive advantage to its owner? The Restatement of Torts (alluding to economic value in stating "a trade secret. . . gives him an opportunity to obtain an advantage over competitors. . ."),[141] Restatement (Third) of Unfair Competition (referring to information "sufficiently valuable and secret to afford an actual or potential economic advantage over others"),[142] and most explicitly the UTSA ("[a trade secret] derives independent economic value, actual or potential from not being generally known. . .") all refer to the economic value element in some form or fashion.[143] However, the economic value element frequently get short shrift, with some courts simply allowing this element to be satisfied "through circumstantial evidence such as the fact that others are willing to pay for access to the information or that plaintiff would not have gone to the expense and hassle of bringing a trade secret infringement claim unless the alleged trade secrets have value."[144] The blame for this treatment may rest with the foundations of the doctrine in the Restatement of Torts, which only required a generalized recognition of value often satisfied by the fact the holder of the putative trade secret expended money in the development of the information.[145] Courts frequently admit circumstantial evidence of value such as the expense incurred to acquire the information and the willingness of others to pay for the information.[146] However, as adoption of the UTSA spreads and the body of precedent

138. *See id.* (for a collection of data protection protocols built around preserving trade secret information).

139. POOLEY, *supra* note 115, at § 2.03[2][a] – [e].

140. *Id.* at § 2.03[2][a] – [e].

141. RESTATEMENT OF TORTS § 757 cmt. b (1939).

142. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

143. *See id.*; RESTATEMENT OF TORTS § 757 cmt. b (1939).

144. Sharon K. Sandeen, *A Contract by Any Other Name is Still a Contract: Examining the Effectiveness of Trade Secret Clauses to Protect Databases*, 45 IDEA 119, 141 (2005).

145. *Id.*

146. *See, e.g.*, POOLEY, *supra* note 115, at § 4.05[2]; Gates Rubber Co. v. Bando Chem.

interpreting it apart from the Restatement grows, greater emphasis may be placed on its economic value language.

In any case, though, the economic value element ties inextricably to the secrecy element – the value must come from the secrecy; "[i]n other words, the value derived from the secret must be 'independent' of the value that is intrinsic to the good or service, or that derives from other factors."[147]

Clearly, farm data has value to the farmer – otherwise, an industry focused on improved farm sensing and data analysis would not be exploding. Clearly, also, farm data has value to others, evidenced by the multibillion-dollar industry growing around collective analysis of it. But neither of these facts answer the question: does farm data have economic value to the farmer him or herself because it is not generally known? Answering that question requires asking a new one: what would someone else do with the farm data that would directly injure the economic interests of the farmer? Farm input vendors could use the data to create specifically-targeted marketing for the farmer (a la GoogleAds dynamically adapted to highlight products or services related to the user's searches[148]) or equipment vendors could suggest preventative maintenance services. It should be noted here that there is a clear economic benefit to the collection of farm data in the aggregate; otherwise Monsanto would not spend nearly $1 billion in acquiring a company to aggregate such data.[149] However, while this proves the farm data has economic value to others, it fails to prove the data has economic value "derive[d]. . . 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."[150] In other words, the economic value element requires the facts have value to the holder of the fact and that such value derives from the secrecy of the fact.[151] Additionally, although the above-mentioned circumstances might economically benefit the input and equipment vendors, they may also benefit the farmer in being able to purchase inputs and equipment enabling him or her to improve the profitability of the farm operation, and in any

Indus., 9 F.3d 823, 848 (10th Cir. 1993); Tan-Line Studios, Inc. v. Bradley, 1986 U.S. App. LEXIS 36785 (3d. Cir. 1986).

147. POOLEY, *supra* note 115, at § 4.05[1] (citing Abba Rubber Co. v. Seaquist, 235 Cal. App. 3d 1, 19 (1991)).

148. *See* Chuck Topinka, *How Exactly does Google AdWords Work?*, FORBES (Aug. 15, 2014, 12:04 PM), http://www.forbes.com/sites/quora/2014/08/15/how-exactly-does-google-adwords-work/.

149. Bruce Upbin, *Monstanto Buys Climate Corp for $930 Million*, FORBES (Oct. 2, 2013, 9:13 AM), http://www.forbes.com/sites/bruceupbin/2013/10/02/monsanto-buys-climate-corp-for-930-million/.

150. UNIF. TRADE SECRETS ACT § 1(4)(i)-(ii) (UNIF. LAW COMM'N 1985).

151. *See id.*

case are likely not directly injurious to their economic interests.

Clearly, a farmer's mere desire to keep his or her farm data secret does not suffice to give the data trade secret protection. Courts have noted just because secret information is of value to its owner does not mean it has value to others.[152] Instead, the economic value element requires the farmer's economic interest derives from others not knowing the information. When could farm data have such traits? Say a Farmer B obtains data Farmer A compiled while farming leased land. Farmer B evaluates the data and determines he or she could produce the land more efficiently or profitably than Farmer A. Farmer B presents this information to the owner of the leased land, bidding the lease of such land away from Farmer A. The existence of such a scenario could, hypothetically, satisfy the economic value element as establishing that the alleged trade secret could cause economic harm to the holder if it were generally known. Put another way, the keeping of the secret increases the economic well-being of the holder. If a real-world Farmer B played out this scenario and acquired the data by improper means (and not from permissible means such as examining publicly-available records or observing Farmer A's practices from a publically-accessible vantage point, all of which goes to the definitional element of a trade secret as "not readily ascertainable by proper means by other persons who can obtain value from its disclosure or use"),[153] a colorable case for proof of the economic value element may exist. Whether or not a real-world Farmer B exists may not matter, as at least some cases require "only that their be actual or potential value from the information being secret" although Farmer A might also have to prove Farmer B is indeed a competitor. However, courts could just as easily find that allowing trade secret protection in this scenario would promote anti-competitive behavior in the underutilization of assets and rule against allowing trade secret protection on policy grounds.[154]

5. Proving a claim of trade secret misappropriation

Assuming, arguendo, that a farmer can craft a satisfactory case his or her farm data constitutes a trade secret, the data's classification as such provides no proactive protection but instead only provides a basis for assertion of a trade secret misappropriation claim. In asserting such a claim, the farmer bears the burden of proof.[155] Further (and unsurprisingly), the confluence of sources of trade

152. *See* Sandeen, *supra* note 144, at 142; Lejune v. Coin Acceptors, Inc., 849 A.2d 451, 462 – 63 (Md. 2004)).

153. UNIF. TRADE SECRETS ACT § 1(4)(i)-(ii) (UNIF. LAW COMM'N 1985).

154. Religious Tech. Ctr. V. Netcom On-Line Comm. Servs., Inc., 923 F. Supp. 1231, 1253 (N.D. Cal. 1995) (emphasis in original); *see also* POOLEY, *supra* note 115, at § 4.05[1].

155. *See* SECTION OF LITIG., AM. BAR ASS'N, MODEL JURY INSTRUCTIONS: BUSINESS

secret law leads to some confusion about the requirements of a prima facie case of trade secret misappropriation. The UTSA defines misappropriation as:

> (i)acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
> (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
> (A)used improper means to acquire knowledge of the trade secret; or
> (B)at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was
> (I)derived from or through a person who had utilized improper means to acquire it;
> (II)acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> (III)derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
> (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.[156]

In some ways, the Restatement (Third) of Unfair Competition has come to reflect the themes of the UTSA. For example, where UTSA §1(2)(i) recognizes improper acquisition even without disclosure, so too does the Restatement allow improper acquisition alone to provide grounds for actionable misappropriation even without use or disclosure of the trade secret.[157] The trend of convergence in the elements of misappropriation elements continues to emerge.[158] At the moment, though, there appear to be four elements common among all jurisdictions in proving a claim for trade secret misappropriation:

1. that a trade secret existed in which plaintiff had ownership rights when the defendant committed the acts complained of by plaintiff;
2. that defendant acquired the trade secret (a) through improper means, (b) through plaintiff's disclosure of the trade secret to the defendant under a confidential relationship, or (c) under other circumstances giving rise to a duty;
3. if acquisition was not through improper means, that defendant used or

TORTS LITIGATION 388 (Ian H. Fisher & Bradley P Nelson eds., 4th ed. 2005) [hereinafter ABA].

156. UNIF. TRADE SECRETS ACT § 1 (2).

157. ABA, *supra* note 156, at 388 (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40).

158. *See id.* at 384 – 91.

disclosed the trade secret without plaintiff's permission; and

4. that (a) plaintiff suffered harm as a direct and proximate result of defendant's use or disclosure of plaintiff's trade secret, or (b) defendant gained from such use or disclosure."[159]

Discussion of whether farm data can constitute a protectable trade secret under the first element has already consumed much of the discussion to this point.

Satisfaction of the second and third elements depends largely on the parameters of the relationship between the farmer and the alleged misappropriating party.[160] Discussion of these parameters follows in a later section of the article. For now, though, note that a party who acquires data by physically planting a "bug" on a farm equipment system or hacks an encrypted data transmission would clearly satisfy the second element of inappropriate acquisition.[161] Note also that someone receiving information and uses or discloses it in direct contravention of an agreement between the parties would also satisfy the third element.[162]

The fourth element goes back to hornbook torts law – a tort requires the plaintiff to have suffered some form of damage directly linked to the defendant's behavior.[163] Thus, while both the UTSA and Restatement (Third) of Unfair Competition recognize improper acquisition of farm data may constitute misappropriation, a judge and jury may be inclined to reply "so what" unless the farmer sustained some form of economic damage as a result of that improper acquisition.[164] In the scenario referenced above wherein Farmer B used information about Farmer A's practices to bid land away from Farmer A, the damages may be fairly clear (ignoring for the moment the time and expense likely necessary to prove the misappropriation) and could open Farmer B to significant liability: "Section 45 of the new Restatement [(Third) of Unfair Competition] also permits a plaintiff to recover both the plaintiff's pecuniary loss and the defendant's pecuniary gain, so long as there is no double recovery."[165] However, proving economic damage from improper acquisition or misuse by someone other than a direct competitor – say a consultant who disclosed data in the context of an aggregated database or a vendor who used the information to target marketing efforts at the farmer – may prove prohibitively inexpensive, technically challenging, or empirically impossible.

159. *Id.*
160. *See generally id.* at 408 – 417.
161. *Id.* at 408 – 414.
162. *Id.* at 415.
163. *See* ABA, *supra* note 156, at 384, 419.
164. *Id.* at 384.
165. *Id.*

Note also that farm data as a trade secret may have a shelf life. Certainly, as time passes, information may come into public knowledge and thus lose trade secret protection, but data rendered obsolete through changes in the farming practices applied to the land from which it was derived or simply the passage of time may undermine a trade secret claim in the data.[166]

To conclude the trade secret analysis, suffice it to say colorable arguments exist both for and against the proposition that farm data poses an "ownable" and protectable trade secret. That said, it provides the best doctrinal fit among the traditional intellectual property forms, and farmers wishing to preserve whatever rights they do indeed have in that data seem best advised to use the trade secret model to inform the their protective measures.

III. HOW CAN FARMERS PROTECT THEIR DATA

A. Securing data and data transmissions

Historically, a program to secure trade secret information focused on a two-pronged approach of securing the data from disclosure by employees or others given access the data and physically securing the data against inappropriate or unauthorized access.[167] While the first prong still holds, "physical" security of data holds limited meaning in the 21st century.[168]

Certainly, to the extent one retains farm data in a hardcopy form, one should secure it to the extent practicable. Physical security measures can include a number of measures:[169]

1. Store confidential information in areas not frequently used by personnel unauthorized to access the information.
2. Keep confidential information in locked storage rooms and cabinets
3. Restrict access to such areas to only those with a "need to know" the information
4. Provide sign-out/sign-in registers for confidential information
5. Utilize camera/alarm systems to alert of unauthorized access.
6. When disposing of confidential information, physically destroy hard-copies by shredding.

To an extent, physical security measures can help secure digital data stored

166. *See, e.g.*, Davis, *supra* note 112, at 11 (citing Fox Sports Net N., LLC v. Minn. Twins P'ship, 319 F.3d 329, 336 (8th Cir. 2003) ("obsolete information cannot form the basis for a trade secret claim because the information has no economic value").

167. *See, e.g.*, James Pooley, TRADE SECRETS: HOW TO PROTECT YOUR IDEAS AND ASSETS 35 – 67 (1982) [hereinafter Trade Secrets].

168. *See id.*

169. *See id*; DAVIS ET AL., *supra* note 112, at 71.

on computers and portable memory devices such as "flash" memory drives and Secure Digital (SD) memory cards by physically restricting access to the devices. However, once one connects such a device to an internet-connected computer, physical security measures quickly give way to computer security measures.[170] Thus, digital information generally requires an entirely new layer of security protocols. The first consists of restricting access to the digitally-stored data and means of unauthorized transmission of the data.[171]

1. Require password access to any computers storing confidential information and restrict password access to "need to know" employees.
2. Immediately change passwords when an employee leaves or after any indication of a potential breach.
3. Use computer software that alerts of any copying or downloading of confidential information.
4. Monitor employees' use of email or the Internet to detect any unauthorized transmissions of confidential information.
5. Do not store confidential information on Internet-connected devices.
6. Ask equipment vendors for a detailed listing of the sensor and wireless transmission systems embedded in any equipment.
7. Do not select any undesired sensor or wireless transmission systems when making option selections on the purchase of new equipment.
8. Request the deactivation of any wireless transmission systems on the purchase of existing equipment (or new equipment where such systems are standard) and confirm the deactivation with a third party technician.[172]

While such procedures might provide some modicum of protection against the accidental or intentional disclosure of confidential information, they also pose a number of problems. Additional layers of security necessarily hamper the efficiency of employees who do need to access the data in utilizing it, and blocking Internet access or deactivating wireless transmission systems means eliminating the myriad advantages in quickly sharing data with the vendors and consultants providing profit-enhancing services to the farm.[173] Given this, the aforementioned practices may be of limited use in a highly-connected agricultural operation. Thus, the more economical application of security may lie in clearly establishing secure means of data transfers. To a large extent, determining the methods of data transmission used on a farm involves a significant amount of

170. *See* DAVIS ET AL., *supra* note 112, at 71.

171. *See id.*

172. *See generally id*. at 68 – 84.

173. *See id*. at 72 – 76 (discussing restricting interest access and additional layers of security an employer may put in place).

consumer research on the part of the farmer prior to purchasing equipment with embedded sensors and transmission equipment or separate sensing systems.[174] It also involves monitoring the ongoing use of such systems.[175] Additional discussion of how farmers can work with their service providers to establish a secure data sharing arrangement is discussed in more detail in section IV.C. below.

B. Handling confidential information with employees

1. The implied duty of confidentiality for employees

The Restatement (Third) of Unfair Competition states "[a]n employee or former employee who uses or discloses a trade secret owned by the employer or former employer in breach of a duty of confidence is subject to liability for appropriation of the trade secret . . . ."[176] The Restatement links an implied duty of confidentiality to the agency theory connecting employers and employees[177] and ties that duty to the more general duty "not to compete with the employer in the subject matter of the employment, including a duty to refrain from using confidential information acquired during the course of the employment in competition with the employer."[178] Not surprisingly, the scope of the duty of loyalty looms larger for current employees, who are bound by both doctrines of trade secret and principal/agent law, than former employees.[179]

The UTSA says little about the employer/employee relationship, though it does reference the importance of that relationship but does so not in the context of implied duties of confidentiality; rather, the UTSA notes the importance of regulation of employee conduct in the form of warnings and employer policies as part of the duty to maintain the secrecy of information.[180] However, courts have

174. *See, e.g.*, Bobkoff, *supra* note 5; Broughton, *supra* note 3; Doering, *supra* note 2; Matter, *supra* note 8, (examples of different equipment and technology capabilities between industry suppliers).

175. *Id.*

176. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 (1939).

177. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. a, (citing RESTATEMENT (SECOND) AGENCY §§ 2, 220).

178. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. b, (citing RESTATEMENT (SECOND) AGENCY §§ 387, 393, 395 (citations omitted)).

179. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §42 cmt. a, ("Current employees, however, are also subject to a general duty of loyalty that is broader than the specific obligations arising under the law of trade secrets").

180. *See, e.g.*, UNIF. TRADE SECRETS ACT § 1 (UNIF. LAW COMM'N 1985), cmt. ('. . .reasonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on "need to know basis," and controlling plant access. . . It follows that reasonable use of a trade secret including controlled disclosure to employees and licensees is consistent with the requirement of relative secrecy").

struggled with how to reconcile the common law duties of employees with what was intended to be a more precise treatment of trade secrets under the UTSA.[181]

2. Employee policies before, during, and after employment

Given the uncertainty of relying only on implied duties of confidentiality, the better course for farmers concerned about potential disclosure of their farm data lies in affirmative, proactive management of the employer and employee relationship. This course allows for the maximum productivity of the farm by permitting employees to make full use of the data systems that can provide important information to the farm manager in making production decisions.

Many human resources professionals hold investment in robust employee screening and interview processes as the best means of solving employee problems before they even start. With respect to issues of confidential information, consider the following in screening and interviewing potential employees:[182]

1. Avoid the targeted recruitment of employees of a competitor; doing so may increase the likelihood of a claim from the competitor that the hiring employer was attempting to gain access to confidential information or create an opportunity for espionage.[183]
2. Ask the prospective employee about their attitudes with respect to confidentiality or proprietary information (people "philosophically committed to universal freedom of information" may not be inclined to keep secrets well).[184]
3. Ask about the circumstances under which the prospective employee left previous employers who are potential competitors.[185]
4. Obtain copies of any documentation related to confidential information the prospective employee may have handled in prior employment, including any confidentiality agreements to which the prospective employee is still bound and any termination statements.[186]
5. Discuss any potential limitations on job duties related to confidential

181. *See* Julie Piper, *I Have a Secret?: Applying the Uniform Trade Secrets Act to Confidential Information that Does Not Rise to the Level of Trade Secret Status*, 12 Marq. Intell. Prop. L. Rev. 359, 360 – 61 (2008).

182. *See generally* POOLEY, *supra* note 115, at § 9.04.

183. *Id.* at § 9.04[1] (in areas with a highly limited amount of qualified agricultural labor, a growing problem particularly in finding employees with the technical knowledge needed to make full use of modern agricultural equipment, this policy can severely restrict the hiring prospects for an agricultural employer).

184. *Id.* at § 9.04[1].

185. *Id.* at § 9.04[1][a].

186. *Id.* at § 9.04[1][a].

information.[187]

Potential employers should be up-front about the potential to deal with any confidential information and should share their employee policies (discussed below) in advance to help "create a culture of confidentiality" even before hiring.[188]

Once an employee has been selected, a thoughtful and clear set of employee policies, fairly and consistently enforced, and codified in an easy-to-read employee handbook, can further this culture of confidentiality.[189] The handbook can provide an important reference for the employee if he or she has questions and cannot reach a supervisor for help, and can also be a reminder of the importance of specific issues ("the boss must think this is a big deal if there is a policy on it.").[190] Items to be included in an employee handbook regarding confidential information include:

1. Advise the employee that some information they will encounter is confidential.
2. Underscore the importance to the long-term profitability of the business in keeping such information secret.
3. Describe the procedures in place to keep confidential information secret.
4. Describe company policies regarding (or prohibiting) keeping any confidential information on the employee's personal computer, mobile phone, or other electronic devices.
5. Outline the disciplinary measures that may be implemented if an employee discloses confidential information or violates confidentiality procedures.
6. Clearly identify who the employee can contact if they have a question about how to handle a situation involving potentially confidential information or if they suspect confidential information has been released.[191]

A strong confidentiality agreement to be executed by the employee may be even more important than the policies embodied in the handbook. Such an agreement solidifies the obligation of the employee to maintain the confidentiality well beyond the implied duty of confidentiality and an employee handbook that may not rise to the level of an enforceable contract.[192] Fortunately, a number

187. POOLEY, *supra* note 115, at § 9.04[1][a].

188. DAVIS ET AL., *supra* note 112, at 59; *see also* POOLEY, *supra* note 115, at § 9.04[1].

189. DAVIS ET AL., supra note 112, at 59.

190. *Id.*

191. LISA GUERIN & AMY DELPO, CREATE YOUR OWN EMPLOYEE HANDBOOK: A LEGAL & PRACTICAL GUIDE FOR EMPLOYERS 326 – 27 (5th ed. 2011); *see also* POOLEY, *supra* note 115, at § 9.04[5].

192. *See* GUERIN & DELPO, *supra* note 192, at 327 (many employers go to significant

of exemplars exist for such employee confidentiality agreements.[193] Although valuable, confidentiality agreements should be carefully crafted to avoid potential legal claims arising out of anti-competitive behavior.[194] Similarly, the confidentiality agreement should not be over-broad; "a confidentiality agreement cannot make a trade secret out of something that is generally known and, for the most part, courts will not restrain competition for alleged, but unproven, trade secrets."[195] On a related note, non-compete agreements or other restrictive covenants may also be in order to prevent confidential information from being used against the employer, but such agreements are strictly construed and often found unenforceable if too broad.[196]

When an employee with access to confidential information leaves the enterprise, a number of precautions should be taken:

1. Interview the employee to determine the reasons for which he or she is leaving (is the departure on good terms?).
2. Secure all equipment containing confidential information including company-owned computers, mobile phones, or other electronic storage devices.
3. Delete all confidential information from employee's personally-owned computers, mobile phones, and other electronic storage devices.
4. Review the confidentiality agreement with the employee and emphasize the employee's continuing obligations of confidentiality.
5. Obtain contact information for the employee and his or her new employer.
6. Change all passwords for systems to which the employee had access; secure any physical keys held by the employee and consider re-keying particularly sensitive areas.[197]

Although many farmers spend most of their concern on external threats to their information security, the most serious threats to confidentiality may lie in their own employees. Even though their breaches may be completely unintentional, employees routinely have access to information that would take extraordinary efforts by an outside party to access.[198] Thus, perhaps nowhere is the adage

lengths to ensure the handbook does *not* constitute a contractual arrangement to preserve an "employment at will" arrangement. In such circumstances, a separately-enforceable confidentiality agreement becomes even more important).

193. *See, e.g.*, POOLEY, *supra* note 115, at § 9.04; GUERIN & DELPO, *supra* note 192, at 326; DAVIS ET AL., *supra* note 112, at 62 – 63.

194. *See generally* DAVIS ET AL., *supra* note 112, at 85 – 115.

195. *See* AMP Inc. v. Fleischhacker, 823 F. 2d 1199, 1206 (7th Cir. 1987).

196. DAVIS ET AL., *supra* note 112, at 64.

197. *See id.* at 66.

198. *See generally id.* at 47 – 80.

"an ounce of prevention is worth a pound of cure" more true than in one's handling of employee confidentiality issues.

C. Relationships with vendors, consultants

Speaking of external threats leads to the focus of much of the farm data discussion in public discourse, namely, what might happen if someone outside the farm gains access to farm data. Among these concerns are a third party hacking into a data-carrying system (whether physically or by "hijacking" a wireless data transmission), and also what happens if someone who was given access to the data uses it for an unauthorized, or at least undesired, purpose.[199]

1. Data and transmission encryption systems

Some farmers are not as concerned with misuse of farm data by the vendors and consultants to which they transmit data as they are concerned with potentially-nefarious third parties obtaining that data during the transmission process. As discussed in section I(B)(1) of this article, physically tapping into farm systems' data networks would pose a technically daunting task to someone not well-versed in the relevant engineering disciplines and would involve a criminal trespass onto the farm in most cases. Similarly, as discussed above, most cellular data networks use encryption methods that secure transmissions against all but the most sophisticated decryption technologies.

While these basic conditions of the farm data transmission environment protect against most casual threats to farm data security, farmers can still take measures to increase data security. When using services that involve cellular data transmissions, farmers should ask the service provider what encryption methods are used by the network.[200] Farmers should also ask what computer security measures are used by the receiving company. Data encryption occupies an ever-increasingly important role in securing information as computers become increasingly mobile and connected.[201] For example, the receiving company should at least be using Secure Socket Layer[202] protocols to ensure there are no "eavesdropping" systems obtaining data through the connection and/or that an "impostor" system is on the receiving end of the data transmission.

199. *Id.* at 73 – 75.

200. *Id.* at 74.

201. *See id.* at 73.

202. *See* Jeff Tyson, *How Encryption Works*, HOWSTUFFWORKS, http://computer.howstuffworks.com/encryption4.htm (last visited May 22, 2016).

2. Use of non-disclosure agreements

Although there may be an implied duty of confidentiality on the part of one receiving trade secret information such as a consultant,[203] the preceding discussion should already lead the reader to conclude an explicit agreement is likely the better course. 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.[204] 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.[205] 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.[206] 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.

203. *See* MILGRIM & BENSEN, *supra* note 114, at § 5.01 – .02.

204. DAVIS ET AL., *supra* note 112, at 61 – 63.

205. *See generally* STEPHEN FISHMAN & RICHARD STIM, NONDISCLOSURE AGREEMENTS: PROTECTING YOUR TRADE SECRETS & MORE (Mary Randolph ed., 2001).

206. *E.g.*, *Privacy and Data*, DEERE & CO. (2015), https://www.deere.com/privacy_and_data/privacy_and_data_us.page.

> 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.[207]

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).[208] 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:

1) Execute the agreement prior to data disclosure:[209] Trade secret law will not protect information voluntarily disclosed or publicly available. 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.[210]
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.[211]

207. *Privacy and Data: Enterprise Privacy Statement*, DEERE & CO. (2015), https://www.deere.com/privacy_and_data/privacy_and_data_us.page.

208. *See generally* DAVIS ET AL., *supra* note 112.

209. *Id.* at 59.

210. FISHMAN & STIM, *supra* note 206, at 3/5.

211. *See id.* at 3/3 – 3/6.

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 disclosable, but only with the express written consent of the party providing the information.[212]
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.[213]
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.[214]
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 hard-copies of the information and the complete erasure of physical

212. *Id.* at 3/7 – 3/8.

213. *Id.* at 3/8 – 3/9.

214. *See* Brian D. Bowden, *Drafting and Negotiating Effective Confidentiality Agreements (with forms)* 41 Prac. Law. 39, 39 – 43 (1995).

drives where the data is stored.[215]

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.[216]
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.[217]
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.[218]
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

215. *See* DAVIS ET AL., *supra* note 112, at 81.
216. FISHMAN & STIM, *supra* note 206, at 3/14.
217. *Id.* at 3/14 – 3/15.
218. *Id*. at 3/11.

the service provider.[219]

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?[220]
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.[221]
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

219. FISHMAN & STIM, *supra* note 206, at 3/15.
220. *Id.* at 3/16 – 3/19.
221. *See id.* at 3/5.

> 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.[222]

3. Landlord and tenant relationships

A tremendous amount of discussion in the farm data space has focused on "who owns farm data" with many farmers asserting "obviously the farmer!" and industry representatives assenting to that assertion (although vigorous discussion of how closely industry actions align with that ideal continues).[223] While the notion of the farmer owning data generated from his or her land seems intuitively and emotionally satisfying, it also fails to consider an arrangement affecting at least part of almost every American farm – who owns the data regarding leased agricultural land? The tenant operating the land could easily assert the data belongs to him or her, since he or she expended funds to operate the equipment collecting the data about the agricultural practices he or she implemented on the land.[224] However, the landowner might also assert the data describes attributes of his or her property and thus should belong to him or her.[225] A share-lease arrangement would further complicate the issue (or perhaps clarify it in creating ownership rights in both landlord and tenant).

Whatever the doctrinally-correct answer may be to whether the landlord or tenant owns agricultural data, the most prudent course appears to be crafting an explicit agreement about farm data rights as part of the farmland lease. To this end, Janzen proposes a number of considerations in such agreements.[226] In cases where the tenant is regarded as the owner of the data, such provisions might include:

1. Landlord and tenant recognize that tenant's farming of the leased farmland during the term of the lease will generate agronomic data, including information related to soil, water, seed variety, crop health, crop

222. DAVIS ET AL., *supra* note 112, at 115 – 16.

223. *See, e.g.*, Bobkoff, *supra* note 5 (an example of this discussion stems from the rights of farmers to access proprietary network messages as discussed in section I(B)(1) of this article; these issues will be discussed in more detail in Part II of this series); Broughton, *supra* note 3; Doering *supra* note 2.

224. *See generally* Todd Janzen, *Big Data in Farm Leases: When Landlord and Tenant Both Want the Data*, JANZEN AG LAW BLOG (Feb. 6, 2015), http://www.janzenaglaw.com/2015/02/big-data-in-leases-when-landlord-and.html.

225. *See id.*

226. *See* Todd Janzen, *Does Your Agricultural Lease Address Big Data*, JANZEN AG LAW BLOG (Jan. 31, 2015), http://www.janzenaglaw.com/2015/01/does-your-lease-address-big-data.html#more [hereinafter Janzen, *Address Big Data*].

maturity, disease, nutrients, fertilizer, herbicides, pesticides, yield etc., in various digital forms, including files, imagery, records, video, photos, etc. ("Farm Data").

2. Landlord assigns all rights and interest to Farm Data to tenant and relinquishes landlord's rights in the same. Tenant is the exclusive owner of all Farm Data generated on the leased farmland during the lease term. Tenant shall have all rights associated with Farm Data ownership, including deletion, transfer, sale, and disclosure rights.
3. At the conclusion of the lease, tenant shall assign and transfer all Farm Data from the prior crop year to landlord, or at landlord's election, the subsequent tenant.[227]

If the landlord is deemed to have ownership of the farm data generated, the alternative form would be as follows:[228]

1. Landlord and tenant recognize that tenant's farming of the leased farmland during the term of the lease will generate agronomic data, including information related to soil, water, seed variety, crop health, crop maturity, disease, nutrients, fertilizer, herbicides, pesticides, yield etc., in various digital forms, including files, imagery, records, video, photos, etc. ("Farm Data").
2. Tenant assigns all rights to Farm Data to landlord and relinquishes tenant's rights in the same. Tenant shall cause all Farm Data to be transferred to landlord on or before December 31st each year by a mutually acceptable method of data transfer. Landlord is the exclusive owner of all Farm Data generated on the leased farmland during the lease term. Landlord shall have all rights associated with Farm Data ownership, including deletion, transfer, sale, and disclosure rights.
3. At the conclusion of the lease, landlord shall retain ownership of all Farm Data. Tenant shall delete any copies of Farm Data under tenant's possession, custody, or control.[229]

IV. THE PUBLIC DEBATE OF FARM DATA OWNERSHIP

With any disruptive advance in technology comes a strong reaction from the public, typically comprised of excitement at its promise and fear of its misuse.[230] As discussed throughout this article, the emergence of farm data collection and transmission technologies is no different. What perhaps is different,

227. Janzen, *Address Big Data*, *supra* note 227.

228. *See id.* (switching terms so that landlord has the ownership rights in the lease).

229. *See id.* at 231.

230. *See generally* Broughton, *supra* note 3 (discussing the benefits and concerns of farm big data).

though, is the new social media environment in which these reactions can mix to fuel public debate. With enhanced abilities to share articles, documents, and opinion pieces, all stakeholders in public discussions such as that surrounding farm data issues can seek information and support for their positions. While some may decry the discussion as "much ado about nothing" others hail it as the promise of full democratic engagement in the 21st century.

Much of the conversation about farm data revolves around who "owns" it, and this article has dealt with the issue of farm data ownership at length. Since some consensus seems to be emerging that ownership of farm data – at least in its raw form– lies with the owner, the discussion may now turn to what rights that ownership carries. Many producers and agricultural groups were concerned that larger industrial players such as larger equipment and input manufacturers and suppliers would use their asymmetric bargaining power to impose severe restrictions on farmer's rights with respect to their data to take advantage of the farm data tools now available, in much the same way software users were compelled to enter end-user license agreements (EULAs) if they wanted the benefit of the software attached to them.[231]

Sensing a need arrive at a consensus about how farm data should be handled, an impressive consortium of agriculture industries began a discussion process to arrive at a set of farm data principles.[232] On November 13, 2014, the American Farm Bureau Federation announced an important advancement in this arena with the Privacy and Security Principles for Farm Data.[233] This policy statement was the result of a facilitated dialogue among 13 farm organizations consisting of the American Farm Bureau Federation, the American Soybean Association, Beck's Hybrids, Dow AgroSciences LLC, DuPont Pioneer, John Deere, the National Association of Wheat Growers, the National Corn Growers Association, National Farmers Union, Raven Industries, The Climate Corporation, and the USA Rice Federation.[234] Among the principles included in the

231. *Compare* Ariz. Cartridge Remanufacturers Ass'n v. Lexmark Int'l, Inc., 421 F.3d 981 (9th Cir., 2005), *and* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); Microsoft v. Harmony Computers, 846 F. Supp 208 (E.D.N.Y. 1994), *and* Novell v. Network Trade Ctr., 25 F. Supp. 2d. 1218 (D. Utah 1997), *with* Step-Saver Data Sys. Inc. v. Wyse Tech., 939 F.2d 91 (3d Cir. 1991), Vault Corp. v. Quaid Software Ltd. 847 F.2d 255 (5th Cir. 1988), *and* Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332 (D. Kan. 2000) (Comparing cases finding EULAs enforceable and cases finding EULAs unenforceable).

232. *See generally Farmers, Agriculture Technology Providers Reach Agreement on Big Data: Privacy and Security Principles Expected to Accelerate Technology Adoption*, AM. FARM BUREAU FED'N (Nov. 13, 2014) [hereinafter *Farmers*], http://www.fb.org/index.php?action=newsroom.news_article&id=188.

233. *Id.*

234. *Privacy and Security Principles for Farm Data*, AM. FARM BUREAU FED'N (May 5, 2015), http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf.

statement are:

> Ownership: We believe farmers own information generated on their farming operations. However, it is the responsibility of the farmer to agree upon data use and sharing with the other stakeholders with an economic interest, such as the tenant, landowner, cooperative, owner of the precision agriculture system hardware, and/or ATP etc. The farmer contracting with the ATP is responsible for ensuring that only the data they own or have permission to use is included in the account with the ATP.
> Portability: Within the context of the agreement and retention policy, farmers should be able to retrieve their data for storage or use in other systems, with the exception of the data that has been made anonymous or aggregated and is no longer specifically identifiable. Non-anonymized or non-aggregated data should be easy for farmers to receive their data back at their discretion.
> Data Retention and Availability: Each ATP should provide for the removal, secure destruction and return of original farm data from the farmer's account upon the request of the farmer or after a pre-agreed period of time. The ATP should include a requirement that farmers have access to the data that an ATP holds during that data retention period. ATPs should document personally identifiable data retention and availability policies and disposal procedures, and specify requirements of data under policies and procedures.
> Liability & Security Safeguards: The ATP should clearly define terms of liability. Farm data should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure. Polices for notification and response in the event of a breach should be established.[235]

These principles address a number of concerns raised earlier in this article. However, as previously noted, policy statements are not legally enforceable unless integrated in some way to a legally enforceable agreement. Time alone will tell how fully these principles are embodied in the actual service agreements equipment dealers, input providers, and consultants put in place for their customers. Nevertheless, the policy statement represents an important step forward in the collective understanding of farm data issues by all stakeholders.[236]

Other groups have initiated ambitious efforts to advance the interests of farmers in the farm data space. The AgGateway consortium, for example, assembles a significant number of businesses and agricultural producer groups to develop open-source standards with the objective of improving farm data "porta-

235. *Id.*

236. *Farmers*, *supra* note 233.

bility" and interoperability among a number of equipment systems.[237] In a somewhat-related effort, the Open Ag Data Alliance (OADA) also works to develop open-source tools for farm data management and to improve farm data access and security.[238] The efforts of the American Farm Bureau Federation, AgGateway, and the Open Ag Data Alliance represent a continuous commitment to the farm data policy dialogue that will be vital to advancing both the technology available to farmers and the ability of farmers to accept and integrate that technology.

V. CONCLUSIONS

Regardless of how farm data is acquired, it 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 farm 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. While the concept of the "ownership" of farm data remains unsettled, the most prudent course may be for farmers to treat data they hold confidential as if it were a trade secret, although there remain significant questions as to whether farm data could indeed be a protectable trade secret. At the farm level, carefully crafted agreements with employees, service providers, and landlords, coupled with practical security measures, can maximize the available protection of farm data. At the industry level, continued discussion of these issues can lead to proactive, negotiated solutions between large service providers and farmers as a whole.

237. *See generally Working to Promote, Enable and Expand eBusiness in Agriculture*, AGGATEWAY, http://www.aggateway.org/Portals/0/DOCUMENTS/AgGateway%20Executive%20Overview%20-%20FINAL%20%209-5-14.pdf (last visited Oct. 9, 2015).

238. *Principals and Use Cases*, OPEN AG DATA ALLIANCE, http://openag.io/about-us/principals-use-cases/ (last visited Oct. 9, 2015).