Committee on Agriculture
U.S. House of Representatives
Big Data and Agriculture: Innovations and Implications

Testimony by Shannon L. Ferrell, J.D., M.S.
Associate Professor and Faculty Teaching Fellow
Oklahoma State University Department of Agricultural Economics

Executive Summary

Today's technology affords farmers the ability to instantaneously collect data about almost every facet of their cropping operations from planting through harvest. Many agricultural producers have concerns about their rights in this data and their privacy if they choose to share their information to take advantage of the numerous tools afforded by the Big Data revolution as they struggle with 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 agricultural data in the realms of trademark, patent, or copyright law. Agricultural data may fit within the realm of trade secret, but that fit is, at best, arguable. To the extent Congress wishes to enhance the intellectual property rights held by agricultural producers in agricultural data, adaptation of the Uniform Trade Secret Act to accommodate the unique characteristics of agricultural data may be a viable approach.

The greater concern may be in the privacy issues surrounding the sharing of agricultural data through Big Data applications. Current federal privacy laws do not directly address one's privacy rights with respect to information like agricultural data. Ways in which Congress can directly address privacy issues in this field is (1) to enact legislation clearly and narrowly defining the circumstances under which production of agricultural data can be compelled by federal agencies and the circumstances under which agricultural data held by federal agencies can be disclosed, and (2) strengthening the safeguards preventing the inadvertent disclosure of agricultural data held by federal agencies or the unauthorized access of that data by outside parties.

Significant steps are already underway to facilitate consensus among industry stakeholders regarding these issues. This Committee and Congress as a whole may best be able to facilitate the realization of Big Data's potential advantages to U.S. agriculture through support of this consensus effort, support of educational efforts to help agricultural producers make informed decisions about how to engage with Big Data systems, continued development of more robust protections for agricultural data shared with the government, and continued support of improved broadband access in rural areas.

Acknowledgements

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, Ms. Maureen Kelly Moseman, Adjunct Professor of Law at the University of Nebraska College of Law, Mr. Todd Janzen of the Plews Shadley Racher & Braun LLP firm 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 contributed greatly to the development of this testimony.

Perhaps the greatest contribution to this testimony and my 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 we examine here today, Dr. Stone was a mentor to myself and hundreds of other students at Oklahoma State University. He and his wife were both killed in the tragic accident last Saturday at the University's homecoming parade. I hope this testimony honors his memory, the contributions he made to this field, to the U.S. agriculture industry, and to all of his students.

Issue Analysis

1. Introduction

I would like to thank Chairman Conaway, Ranking Member Peterson, and the Members of the Committee for the opportunity to present my observations on the legal issues surrounding the concept of Big Data and its application to data collected by U.S. farmers and ranchers. This new frontier in agriculture presents a fascinating and sometimes paradoxical mix of cutting edge technology, recent legal changes, and centuries-old doctrines of common law. In my testimony today, I will lay a framework for discussing the legal issues surrounding Big Data in agriculture, discuss how the current U.S. legal environment addresses ownership and privacy rights in agricultural data, and suggest some potential avenues for policy responses that may facilitate the economic advantages to be gained from the application of Big Data principles to agricultural data while dealing with the concerns associated with such applications.

2. Framework for legal issues surrounding big data in agriculture

The concept of Big Data has exploded in a relatively short period of time. As a result, the national dialogue continues to develop both common definitions for the core terms in the discussion and the central issues of the discussion. Since these definitions and issues continue to evolve, my testimony today will provide some framing for both.

2.1 Defining core terms in the Big Data discussion

Two terms immediately rise to the top in an examination of the agricultural data discussion: Big Data and agricultural data itself.

While the term **Big Data** is relatively new, it refers to a concept that is not. There are many definitions for the term, but a straight-forward one might be "a collection of data from traditional and digital sources inside and outside your company that represents a source for ongoing discovery and analysis."[1] While this definition sounds much like traditional data analysis (and it is), recent advances in both data collection and transmission increase the analytical power of data analysis procedures by orders of magnitude. The "big" in Big Data comes from the fact data sets continue to grow exponentially both in breadth (with more and more firms collecting data) and depth (with data from more and more firms being aggregated by service providers). Big Data can be defined in the agricultural context to mean the analysis of large numbers of data points both from a producer's own operation and from other operations to discover actionable information at the farm level and to identify trends at the regional or industrial level.

Another term vital to the discussion is **agricultural data**. The concept of agricultural data is almost too broad to define, but looking at research in the field and conversations surrounding agricultural data as part of the Big Data debate indicates the term centers around two more specific concepts: telematics data and agronomic data. **Telematics data** (sometimes called "**machine data**") refers to the information an agricultural implement (such as a planter) or self-propelled vehicle (such as a tractor or combine) collects about itself. Almost by definition, telematics data comes from agricultural equipment owned, operated, or hired under contract by the agricultural producer. **Agronomic data** refers to information about a crop or its environment, such as "as-planted" information from a seed planter, "as-applied" information from a fertilizer sprayer, yield data from a grain combine, and so on. While agronomic data resembles telematics data in that much of it is gleaned directly from agricultural implements, agronomic data can also be obtained from many other sources such as hand-held sensors, aerial platforms such as manned survey flights or flights by unmanned aerial systems (UAS, commonly called "drones"), and even satellite imagery.

Although not as prominent to the discussion as Big Data and agricultural data, another important term to define is service provider. **Service provider** (sometimes called an "**Agricultural Technology Provider**" or "**ATP**") is the term frequently used to describe a party external to the farm providing some service in regard to either crop production or management of the crop enterprise. Crop production services could include fertilizer or chemical applicators, custom cultivators, or harvest contractors whose equipment

---

[1] Arthur, Lisa. 2013. What is big data? Forbes, CMO Network blog entry. Available at http://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/, last accessed November 15, 2014.

generate agricultural data regarding the farm. Management services include traditional services such as crop consulting and scouting, but increasingly include services targeted specifically at data collection and analysis.

2.2 Framing the legal issues surrounding Big Data in agriculture

The issues involved in the discussion of Big Data in Agriculture is almost innumerable, but many can be captured under the umbrella of two over-arching concepts: ownership of agricultural data, and protections against the unauthorized disclosure of agricultural data. Although each of these issues is discussed in greater detail later in this testimony, a brief framing of each issue is provided here.

It is important to note this discussion would not occur were it not for the tremendous potential the nascent farm data revolution promises. Existing technologies such as real-time kinematics (RTK) and auto-steer have already provided substantial economic returns to farmers.[2] Improved sensing of soil conditions, crop health, and yields has led to significantly improved management information for agricultural producers.

To date, much of the gains from improved sensing technologies and their sharing with service providers have come from eliminating inefficiencies in the utilization of agronomic and machinery inputs. Put another way, we have seen significant increases in the use of "data." Perhaps the most dramatic gains lie ahead, though, as agriculture puts the "Big" in Big Data by compiling datasets of sufficient size to enable much more robust statistical analyses of multiple factors influencing commodity production. Examples of how the aggregation of farm data across large datasets can significantly increase value to farmers are illustrated in Table 1 below.[3]

Table 1: Comparison of Primary and Secondary Agricultural Data Uses

Data	Primary Use	Secondary Use
Yield monitor data	Documenting yields; on-farm seed trials	Genetic, environmental, management effect (G x E x M) analyses
Soil sample data	Fertilizer decisions	Regional environmental compliance
Scouting	Spray decisions	Regional analytics

Yield monitor data on one farm can help document the farm's productivity on a field-by-field basis and can illustrate how a seed hybrid performed on said farm in one year, given the environment of that farm for that year and the management practices employed during that year. Big Data aggregation of similar data across hundreds or even thousands of farms allows for the evaluation of that seed hybrid across tens of thousands of

---

2 *See, e.g.* Matthew Darr, "Big Data and Big Opportunities," paper presented at PrecisionAg Big Data Conference, August 21, 2014 (Ames, Iowa).

3 Table and scenarios taken from Terry Griffin, "Big Data Considerations for Agricultural Attorneys," paper presented at American Agricultural Law Association Annual Symposium, October 23, 2015 (Charleston, South Carolina).

permutations of these factors, enabling both seed companies and agricultural producers to learn in one or two years what would take decades of collections by use of traditional seed trials. Soil sample data coupled with yield data can inform an agricultural producer about the nutrient uptake of the crop on his or her farm, but Big Data could allow all the agricultural producers in a region to effectively tackle nutrient loading to impaired water bodies through voluntary management of non-point pollution. Crop scouting can help an individual agricultural producer make decisions about the application of a particular pesticide, but Big Data could allow a crop industry to spot trends in plant pathogens that could be used to head off the spread of potentially devastating plant health threats.

Bringing about the full economic benefits of Big Data in agriculture require a robust system by which large numbers of agricultural producers can share their data since the predictive power of statistical analysis increases with the number of observations available for each variable examined[4]. The agricultural data industry is working tirelessly to create those systems. Perhaps the issue of greater concern to this hearing is not whether we will have systems that *can* accept and analyze that data; it is perhaps how Congress can facilitate the development of an environment in which farmers *will* share their data. Metcalfe's Law states that the value of a network is proportionate to the number of its members. Put another way, Facebook has little value if you are its only member, but it has tremendous value when populated by millions of members. Thus, agricultural producers can only harness the value of Big Data if we can foster an environment in which they are comfortable sharing their data. Doing so requires answers to questions of what rights they can retain in their shared data. Do they retain ownership of their information? Is there any hope of retaining their privacy in that information once it is shared?

2.2.1 Ownership of agricultural data

As agricultural producers began to realize the information they were generating (and, in some cases, sharing with service providers) had potential economic value, questions began to arise regarding who had the superior "ownership" right to that information, given that multiple parties had a hand in its creation. Thus, this issue might be framed as "*Who owns data generated about an agricultural producer's operation?"*

2.2.2. Privacy rights for agricultural data

As discussed in more detail below, it is possible – and even likely –the greatest economic value of agricultural data to the farm owner comes not from his or her own analysis of the data but from its aggregation with data from hundreds or even thousands of other farms (in a true Big Data model) to provide management information and trend identification that could not be derived from any smaller dataset. While aggregation may in some ways actually reduce the disclosure or discovery of information about any one farm, it naturally also raises fears about the release of that information (whether the result of intentional

---

4 *See generally* GEORGE G. JUDGE, ET AL, INTRODUCTION TO THE THEORY AND PRACTICE OF ECONOMETRICS (2nd ed, 1988), 96.

activity such as database hacking or an accidental disclosure). This leads to the second question: "*What protections prevent the disclosure of agricultural data to outside parties?"*

3. Current Legal Framework for Ownership of Agricultural Data

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

The notion of property ownership typically involves some form of six interests, including the right to possess (occupy or hold), use (interact with, alter, or manipulate), enjoy (in this context, profit from), exclude others from, transfer, and consume or destroy. Some of these interests do not fit, or at least do not fit well, with data ownership. Excluding others from data, for example, is difficult, particularly when it is possible for many people to "possess" the property without diminishing its value to the others, just as the value of a book to one person may not be diminished by the fact other people own the same book.[5] 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*?"[6]

Data is difficult to define as a form of property, but it most closely resembles intellectual property. As a result, the intellectual property framework serves as a useful starting point to define what rights a farmer might have to their agricultural data. Intellectual property can be divided into four categories: (1) trademark, (2) patent, (3) copyright, and (4) trade secret. The first three areas compose the realm of federal intellectual property law as they are defined by the Constitution as areas in which Congress has legislative authority.[7] Since trademark is not relevant to a discussion about data,[8] the analysis will focus on patent, copyright, and trade secret.

---

5 Smith, Lars. 2006. "RFID and other embedded technologies: who owns the data?" SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL

6 Peterson, Rodney. 2013. "Can data governance address the conundrum of who owns data?" Educause blog, http://www.educause.edu/blogs/rodney/can-data-governance-address-conundrum-who-owns-data, last accessed November 15, 2014.

7 U.S. Constitution, Article I, § 8, clause 8.

8 The Federal Trademark Act (sometimes called the Lanham Act) defines trademark as "any word, name, symbol, or device, or any combination thereof...to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown." 15 U.S.C. § 1127.

3.1 Application of patent law to agricultural data

The U.S. Patent Act states "whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor" (35 U.S.C. § 101). Generally, for an invention to be patentable, it must be useful (capable of performing its intended purpose), novel (different from existing knowledge in the field), and non-obvious (somewhat difficult to define, but as set forth in the Patent Act, "a patent may not be obtained… if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains").[9] Patent serves as a poor fit for a model of agricultural data ownership since it protects "inventions." Raw data, such as agricultural data, would not satisfy the definition of invention.

It should be noted patentable inventions could be derived from the analysis of agricultural data. While this does not mean the data itself is patentable, it does suggest that any agreement governing the disclosure of agricultural data by the agricultural producer should address who holds the rights to inventions so derived.

3.2 Application of copyright law to agricultural data

The federal Copyright Act states the following:

Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories:

> literary works;
> musical works, including any accompanying words;
> dramatic works, including any accompanying music;
> pantomimes and choreographic works;
> pictorial, graphic, and sculptural works;
> motion pictures and other audiovisual works;
> sound recordings; and
> architectural works. [10]

More so than trademark and patent, the copyright model at least resembles a model applicable to agricultural 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 statute strongly suggests a creative component is important to the copyrightable

---

[9] 35 U.S.C. §§ 102, 103.
[10] 17 U.S.C. § 102(a).

material. Second, the term "original works of authorship" also has been interpreted to require some element of creative input by the author of the copyrighted material. This requirement was highlighted in the case of *Fiest Publications Inc. v. Rural Telephone Service Company,*[11] where the U.S. Supreme Court held the Copyright Act does not protect individual facts. In *Fiest*, the question was whether a pure telephone directory (consisting solely of a list of telephone numbers, organized alphabetically by the holder's last name) was copyrightable. Since the directory consisted solely of pure data and was organized in the only practical way to organize such data, the Supreme Court held the work did not satisfy the creative requirements of the Copyright Act.[12] This ruling affirmed the principle that raw facts and data, in and of themselves, are not copyrightable. Put another way, the fact that ABC Plumbing's telephone number is 555-1234 is 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. Continuing the analogy, ABC's phone number alone is not copyrightable, but a Yellow Pages® ad with ABC Plumbing's number accompanied by a logo and a description of the company's services *would* be copyrightable.

Agricultural data in and of itself may not be copyrightable, but it can lead to copyrightable works. For example, agricultural data may not be copyrightable, but a report summarizing the data and adding recommendations for action might be. Again, then, it is incumbent upon those disclosing agricultural data to include language in their agreements with the receiving party to define the rights to such works derived from the data.

A separate issue regarding copyrights deriving from agricultural data also continues to emerge. Increasingly, the original agricultural data is never even disclosed to the agricultural producer; rather, the data has been processed into a report or a new form through use of a computer algorithm. Quite simply, agricultural producers may often receive a completely computer-generated report with no human author. This requires moving into the realm of copyrights in computer generated works – an area that is far from settled.[13] The evolution of understanding who holds the rights to computer-generated works with regard to agricultural data played out recently in the discussions surrounding comments by Deere & Company on proposed exemptions to the Digital Millennium Copyright Act[14] regarding copyright protection systems in vehicle software.[15]

---

11 499 U.S. 340 (1991).

12 *See id.*

13 *See generally* MARSHALL A. LEAFFER, UNDERSTANDING COPYRIGHT LAW, 109-110 (5th ed. 2011).

14 17 U.S.C. §§ 512, 1201–1205, 1301–1332; 28 U.S.C. § 4001

15 *See* Deere & Company, "Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201" (2015). Available at http://copyright.gov/1201/2015/comments-032715/class%2022/John_Deere_Class22_1201_2014.pdf (last visited October 25, 2015). *Compare* Kyle Weins, WIRED (Business Blog Section, online edition)

3.3 Application of trade secret law to agricultural data

While trademark, patent, and copyright do not appear to fit as models for farm data ownership, trade secret has the potential to appropriately serve the agriculture industry's concerns regarding rights in data shared with Big Data service providers. Importantly, trade secret is a function of state law (unlike trademark, patent, and copyright, which are all creatures of federal law). At the time of this testimony, all but three states have adopted the Uniform Trade Secrets Act, providing a degree of consistency in trade secret law across most states.

Under the Uniform Trade Secrets Act ("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.

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

The first provision requires that to be protected as a trade secret, farm data such as planting rates, harvest yields, or outlines of fields and machinery paths must have economic value because such information is not generally known. While a farmer may (or may not) have a privacy interest in this information, the question remains as to whether the economic value of that information derives, at least in part, from being a secret. The counterargument to that point is the economic value of the information comes from the farmer's analysis of that information and the application of that analysis to his or her own operation – a value completely independent of what anyone else does with the information – and that the information for that farm, standing alone, has no economic value to anyone else since that information is useless to anyone not farming that particular farm.[16] One can see this first element poses problems for the trade secret

---

(editorial) "We Can't Let John Deere Destroy the Very Idea of Ownership," April 21, 2015. http://www.wired.com/2015/04/dmca-ownership-john-deere/ (last visited October 25, 2015).

[16] An agricultural producer could, hypothetically, use such data to bid rented agricultural land away from another tenant if they could somehow demonstrate they could provide the landowner with evidence they could increase the landowner's

model. It should be noted here there is a clear economic benefit to the collection of farm data; otherwise companies would not be investing billions of dollars to position themselves in the agricultural data industry.[17] This represents a question yet to be answered clearly by the body of trade secret law: whether one can have trade secret protection in information that standing alone has no economic value to other parties, but does have such value when aggregated with similar data from other parties.

The second provision – the data be subject to reasonable efforts to maintain its secrecy – also finds problems in an environment where the data is continuously uploaded to another party without the intervention of the disclosing party. The fact data is disclosed to another party does not mean it cannot be protected as a trade secret; if that were the case, there would be little need for much of trade secret law. Rather, the question is how and to whom the information is disclosed. As noted in the Restatement (Third) of Unfair Competition's comments on the Uniform Trade Secret Act, "…the owner is not required to go to extraordinary lengths to maintain secrecy; all that is needed is that he or she takes reasonable steps to ensure that the information does not become generally known."[18] The question becomes what constitutes "reasonable steps" to keep continuously uploaded data protected. Almost certainly this means there must be some form of agreement in place between the disclosing party and the receiving party regarding how the receiving party must treat the received information, including to whom (if anyone) the receiving party may disclose that information.

While an explicit written "non-disclosure agreement" (or "NDA") is not necessary to claim trade secret protection, such an agreement is almost certainly a good idea if an agricultural producer wishes to retain a protectable ownership interest in their data if such an interest exists. Not only can such an agreement clarify a number of issues unique to the relationship between the disclosing and receiving parties, but also can address numerous novel issues in the current information environment that trade secret law have not yet reached.

While the concept of NDAs as separate agreements may be practicable for one-on-one relationships, such as those between agricultural producers and smaller consulting firms, negotiating separate agreements with multiple entities poses significant transaction costs. This problem is particularly magnified when one considers larger corporate service providers who would face the issue of negotiating tens of thousands of NDAs. Unsurprisingly, such entities choose to create standard agreements in their form contracts. While certainly understandable, this in turn creates the "opt-out problem" wherein a farmer who believes the form contract does not adequately protect his or her

---

returns. However, this seems a tenuous argument for the economic value element of the UTSA test and has no application at all in a scenario with owned agricultural land.

[17] *See* Bruce Upbin, FORBES (Tech business blog), "Monsanto Buys Climate Corp for $930 Million," October 2, 2013. http://www.forbes.com/sites/bruceupbin/2013/10/02/monsanto-buys-climate-corp-for-930-million/.

[18] Smith, *supra* note 5, *citing* Restatement of Unfair Competition (Third) §757 (1995).

interests is forced to either agree to the form or do without the product or service – which may be the only product or service compatible with a significant portion of the very expensive equipment he or she already owns or uses. This then provokes the discussion of whether such contracts are enforceable or are, instead, adhesion contracts. There is yet to be found consistency among federal courts as to the enforceability of such software use agreements.[19]

To conclude the trade secret analysis, colorable arguments exist both for and against the proposition farm data poses an "ownable" and protectable trade secret. That said, this option 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. Even so, use of trade secret doctrine as a protective measure for agricultural data has drawbacks in the lack of consistency among states in trade secret law (although the UTSA has done much to add consistency to the field) and the fact it is often a "backward looking" and costly solution since trade secret must frequently be used to seek damages (which are often difficult to both prove and quantify) through litigation after a disclosure has already been made.

4. Current Legal Framework for Privacy Rights in Agricultural Data

Those concerned about the disclosure of personal data can certainly cite a number of damaging data breach examples. 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.

To the extent producers regard agricultural data as proprietary, their concerns about its disclosure naturally invite a review of the release or theft of proprietary information in other sectors. 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 hacks. 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

---

[19] The asymmetry of EULA's has led to allegations they represent "adhesion contracts" and should not be enforceable as a matter of policy. However, some courts have found insufficient evidence of adhesion and held such agreements enforceable. *Compare* cases finding EULAs enforceable: *Ariz. Cartridge Remanufacturers Ass'n v. Lexmark Int'l, Inc.*, 421 F.3d 981 (9th Cir., 2005); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996); *Microsoft v. Harmony Computers,* 846 F. Supp 208 (E.D.N.Y. 1994); *Novell v. Network Trade Center,* 25 F. Supp. 2d. 1218 (D. Utah, 1997) *with* cases finding EULAs unenforceable: *Step-Saver Data Systems Inc. v. Wyse Technology*, 939 F.2d 91 (3rd Cir. 1991); *Vault Corp. v. Quaid Software Ltd.* 847 F.2d 255 (5th Cir. 1988); *Klocek v. Gateway, Inc.*, 104 F. Supp. 2d 1332 (D. Kan. 2000).

million customers), TRW Information Systems (credit reporting company, 90 million customers), Sony (70 million customers) each of which dwarf breaches attracting more media attention such as Home Depot (56 million customers) and Target (40 million customers).[20]

Theoretically, a hacker could tap into the tractor/implement network (also called the tractor/implement bus) using a number of commercially-available technologies allow farmers to plug into the network and access Controller Area Network ("CAN") messages directly; for example, one could purchase a CAN message reader to read machine diagnostic codes for repairs.[21] Someone wishing to "steal" data would likely not want to be present to retrieve the data from the device, 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.[22]

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.[23] Note, that several companies now provide means for re-engineering proprietary CAN messages (such as those related to crop yield) so farmers can automatically transfer yield data to the cloud. Such technology could also be used to decode other proprietary information.[24] Perhaps ironically, the growth of proprietary data network protocols that lead to complaints about the lack of interoperability of farm equipment systems could also provide greater protection against data breaches.

Additionally, the Global Positioning System "GPS" receiver in most systems connects directly to the implement's task controller. As a result, a "bug" might receive information about the commands sent to the implement but without the associated location data, rendering it meaningless. The bug would require its own GPS receiver along with implement data (the configuration and dimensions of the implement), which today could

---

20 Julianne Pepitone, "5 of the Biggest-ever Credit Card Hacks," (2013) CNN Money, a*vailable at* http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/ (last accessed May 21, 2015).

21 Interview with Dr. John Fulton, Ohio State University Department of Food, Agricultural, and Biological Engineering, July 6, 2015.

22 *See* Progressive Corporation, "Snapshot® Terms and Conditions," https://www.progressive.com/auto/snapshot-terms-conditions/ (last visited July 6, 2015).

23 *See* interview with Dr. Marvin Stone (June 10, 2015).

24 Interview with Dr. John Fulton, Ohio State University Department of Food, Agricultural, and Biological Engineering, July 6, 2015.

be done for a modest equipment cost.[25] Obtaining agronomic data via a physical connection to an implement poses a task manageable for someone knowledgeable in SAE J1939 and ISO 11783[26] technology.[27] 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.

As illustrated from this discussion, a number of factors in the configuration and operation of farm data networks limit the opportunities for hackers to take agricultural data directly from the agricultural producer. Admittedly, most producers 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;[28] without the decryption key, interpreting any data transmitted would be difficult (although not impossible for a sophisticated hacker; recent news has highlighted the ability of some groups to do so[29]). The use of data encryption through a secure sockets layer ("SSL") protocol by the farmer and his or her service provider in data transfers adds another difficult-to-break security barrier to interception of the data.[30]

---

[25] A relatively quick search of Google will yield many GPS receiver units for less than $50.

[26] SAE International, "The SAE J1939 Communications Network: An Overview of the J 1939 Family of Standards and How they are Used," 5 (white paper), *available at* http://www.sae.org/misc/pdfs/J1939.pdf (last visited October 25, 2015). *See also* INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO DRAFT INTERNATIONAL STANDARD ISO/DIS 11783: TRACTORS AND MACHINERY FOR AGRICULTURE AND FORESTRY – SERIAL CONTROL AND COMMUNICATIONS DATA NETWORK (2012). The ISO 11783 standard is often referred to as the "ISOBUS standard" and defines how the on-board computer networks on most agricultural equipment works and how their individual components work together. Combined, SAE J1939 and ISO 11783 govern much of how the data-collection network on any agricultural equipment works.

[27] Mikko Miettien, "Implementation of ISO 11783 Compatible Task Controller," XVI CIGR (International Commission of Agricultural and Biosystems Engineering)World Congress, Bonn, Germany (2006), available at http://users.aalto.fi/~ttoksane/pub/2006_CIGR20062.pdf (last visited July 11, 2015).

[28] For a primer on the process of encoding and decoding cellular signals, *see* How Stuff Works, "How Cell Phones Work," http://electronics.howstuffworks.com/cell-phone.htm (last visited October 8, 2015).

[29] *See* Craig Timberg & Ashkan Soltani, *By Cracking Cellphone Code, NSA Has Ability to Decode Private Conversations*, THE WASHINGTON POST, December 13, 2013. Online edition, *available at* 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 (last visited July 1, 2015).

[30] *See* Clemens Heinrich, *Secure Socket Layer (SSL)*, in ENCYLOPEDIA OF CRYPTOGRAPHY AND SECURITY 1135 (Henck C.A. van Tilborg, Sushil Jajodia, eds., 2011)

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 other similar types. Conversely, hackers frequently go after large concentrations of data with easily-converted financial value, such as credit card information. Thus, it may be difficult for hackers to make a "quick buck" from agricultural data making it a less-appealing target of attack. Nevertheless, an adage in computer security is "where there is value, there will be a hacker."[31] 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 more appealing target. Depending on the type of computer at issue and its common use, the federal Computer Fraud and Abuse Act ("CFAA")[32] may provide a means of prosecuting unauthorized access of the computer in the event agricultural data linked to PII is compromised. Discussed below, the federal Electronic Communications Privacy Act (ECPA) [33] could also be used as a potential prosecutorial tool for those attempting to intercept agricultural data during the data transmission process.

The theft of PII by criminals is one threat posed by data transfers, but so too is the inadvertent, or perhaps intentional but misinformed, disclosure of data by the party receiving that data. Take, for example, the disclosure of thousands of farmers' and ranchers' names, home addresses, GPS coordinates and personal contact information" by EPA in response to a Freedom of Information Act (FOIA) request regarding concentrated animal feeding operations (CAFOs) which prompted a lawsuit from the American Farm Bureau Federation and National Pork Producers Council alleging the agency overstepped its authority in doing so.[34] While this event represents the disclosure of information by an enforcement agency, many farmers fear the converse – that an enforcement agency could compel a data-receiving party to disclose information even if such disclosure were not legally required. Another concern is whether an adverse party in litigation (or even a party contemplating litigation) could persuade a party holding a farmer's data to disclose the data as an aid to their case, again even if such disclosure was not legally required.

Much work remains to be done on defining governmental safeguards against disclosures, and even more work remains to be done in defining how the government can obtain electronic data. Although laws such as the ECPA (heavily modified by the USA Patriot Act) govern the acquisition of information through intercepted communications, there is

---

31 Sam Sammataro, "Cybersecurity for Small or Regional Law Firms," paper presented at American Agricultural Law Association Annual Symposium, Charleston, South Carolina (October 23, 2015).

32 18 U.S.C. §§ 1030 *et seq.*

33 18 U.S.C. §§ 2510 *et seq.*

34 Sara Wyant, "Farm Groups File Lawsuit to Stop EPA Release of Farmers' Personal Data." Agri-Pulse (2013), *available at* http://www.agri-pulse.com/Farm-groups-file-lawsuit-to-stop-EPA-release-of-farmers-personal-data-07082013.asp (last visited May 21, 2015).

little law to prevent a government agency from simply requesting data from a service provider. Anecdotal evidence suggests service providers and their legal counsel continue to struggle in defining parameters for how to respond to non-subpoenaed requests for data by government agencies.

All these issues surround restrictions on the taking of information by some unauthorized (or at least questionable) means. While there are at least some laws potentially applicable in these circumstances, there are no laws defining an inherent privacy right in agricultural data.[35] For example, the federal Health Insurance Portability and Accountability Act ("HIPAA")[36] provides privacy rights and restrictions against disclosure of health information; the Gramm-Leach Bliley Act (also known as the Financial Modernization Act of 1999)[37] and Fair Credit Reporting Act[38] protect financial information from disclosure; the Privacy Act of 1974[39] restricts disclosures of personal information by held by the federal government. As of now, though, there are large categories of agricultural data that may fall between the cracks of these laws with no federal (and in most cases, no state) protections against its disclosure.

5. Potential Policy Responses to Address Big Data in Agriculture

Having reviewed the current legal environment surrounding the ownership rights and privacy protections relevant to agricultural data, what can this Committee and Congress do to enable U.S. farmers and ranchers to take maximum economic advantage of Big Data tools? As referenced above, Big Data cannot be Big Data without "buy-in" to the system from large numbers of agricultural producers, and, at a fundamental level, that buy-in requires trust in the system from those producers. That trust, in turn, likely requires answers to the questions of ownership and privacy in agricultural data.

None of the federal intellectual property laws directly address who holds a protectable intellectual property right in agricultural data. Arguably, the most appropriate fit may be found in state law under the UTSA, although the applicability of that law is questionable as well. The UTSA may provide a useful map to any Congressional efforts to help define ownership rights in agricultural data. Passage of statutory law defining ownership of "agricultural data" may be a daunting task given the complexity of the current federal and state intellectual property framework (which also draws from centuries of common law). Thus, it may be advisable instead to use a consensus-driven approach among agricultural producers and service providers to define agricultural data rights. The coalition led by the American Farm Bureau Federation and its "Privacy and Security Principles for Farm

---

35 Todd Janzen, "Legal Issues Surrounding Farm Data Ownership, Transfer, and Control," paper presented at American Agricultural Law Association Annual Symposium, Charleston, South Carolina (October 23, 2015).

36 42 US.C. §300gg, 29 U.S.C. §§ 1181 *et seq.* and 42 U.S.C. §§ 1320d *et seq.*

37 15 U.S.C § 6803.

38 15 U.S.C. §§ 1681 *et seq.*

39 5 U.S.C. § 552a.

Data"[40] represents a tremendous step forward on this issue. Other groups, such as the Open Ag Data Alliance, continue to build coalitions on the technical side of the Big Data issue to develop systems and standards embodying the principles of interoperability, security and privacy.[41] The next step is to see continued cooperation among groups such as these in integrating their principles in legally-binding service agreements.

Modern agricultural producers are expected to be proficient in a broad array of the disciplines of science and business, but few have a background in intellectual property law. Support of educational programs to help these producers understand the legal issues at play in Big Data service agreements could do much to help increase trust, advance the consensus process, and empower producers to make informed decisions about the cost-benefit analysis of sharing their data under those service agreements. The consensus process may also provide a vehicle for developing an understanding among all stakeholders as to the privacy protections necessary and appropriate to protect agricultural data, which occupies a unique space between purely personal and business information. Such information does not readily fit into the existing framework of federal privacy laws, and as business information, may not belong in such a framework.

One matter in which Congressional action may be directly applied is the development of clearer guidelines regarding the production of agricultural data held by private data aggregators, more robust safeguards against inadvertent disclosure or intentional hacking by outside parties, and clear guidance on when disclosure of government-held data is, and is not, required under the Freedom of Information Act[42] or other circumstances.

Finally, although outside the direct scope of a discussion of legal issues in agricultural use of Big Data tools, rural access to wireless broadband services is crucial to fully utilizing the potential of agricultural data systems. Congress should be encouraged to continue its efforts to expand access to this vital utility.

Concluding Remarks

The application of Big Data to agricultural production holds the potential to improve the profitability of U.S. agriculture and to better prepare its farmers and ranchers to handle the inherent risks of the industry. Additionally, Big Data could play a vital role in the further development of tools and techniques necessary to feed an ever-growing, hungry world. I commend this Committee for its foresight in addressing these issues, and sincerely thank the Committee, Chairman Conaway, and Ranking Member Peterson for the opportunity to address you today.

---

40 American Farm Bureau Federation, "Privacy and Security Principles for Farm Data," November 13, 2014 (revised May 5, 2015). Available at http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf (last visited October 25, 2015).

41 Open Ag Data Alliance, "Principals and Use Cases," http://openag.io/about-us/principals-use-cases/ (last visited October 25, 2015).

42 5 U.S.C. § 552.