



SCHOOL OF LAW
TEXAS A&M UNIVERSITY

Texas A&M Law Review

Volume 8 | Issue 4

6-27-2021

Agriculture & Data Privacy: I Want A Hipaa(Potamus) For Christmas . . . Maybe

Jennifer Zwagerman

Drake University Law School, jennifer.zwagerman@drake.edu

Follow this and additional works at: <https://scholarship.law.tamu.edu/lawreview>



Part of the [Agriculture Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Jennifer Zwagerman, *Agriculture & Data Privacy: I Want A Hipaa(Potamus) For Christmas . . . Maybe*, 8 Tex. A&M L. Rev. 685 (2021).

Available at: <https://doi.org/10.37419/LR.V8.I4.3>

This Article is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Texas A&M Law Review by an authorized editor of Texas A&M Law Scholarship. For more information, please contact aretteen@law.tamu.edu.

AGRICULTURE & DATA PRIVACY: I WANT A HIPAA(POTAMUS) FOR CHRISTMAS . . . MAYBE

by: Jennifer Zwagerman

TABLE OF CONTENTS

I	INTRODUCTION.....	686
II.	AGRICULTURE & BIG DATA—WHAT ARE THEY AND HOW ARE THEY USED?	688
	A. <i>What Is Agricultural Data?</i>	688
	B. <i>Data Gathering and Use by Agricultural Producers</i> .	691
	1. Collecting Data	691
	2. How Data Is Used by Producers—Rise of Precision Agriculture	692
III.	WHY IS USE OF AG DATA BY THIRD PARTIES A CONCERN?	693
	A. <i>Power Dynamics</i>	694
	1. Misuse and Abuse	696
IV.	EXISTING DATA PRIVACY LAWS AND REGULATIONS ...	698
	A. <i>Federal Law—Industry Specific</i>	699
	1. Fair Credit Reporting Act (“FCRA”)	699
	2. Children’s Online Privacy Protection Act (“COPPA”)	700
	3. Gramm-Leach-Bliley (“GLB”) Act	701
	4. Health Insurance Portability and Accountability Act (“HIPAA”)	703
	B. <i>Trade Secrets on the Farm</i>	705
	C. <i>Contracts and Data Protection</i>	707
	D. <i>State Data Privacy Laws</i>	709
V.	INTERNATIONAL DATA PRIVACY REGULATIONS	711
VI.	PROPOSALS AND RECENT ACTIONS AT THE FEDERAL LEVEL	713
	A. <i>Considering a Federal Privacy Law</i>	713
	B. <i>Defend Trade Secrets Act of 2016 (“DTSA”)</i>	714
VII.	WEIGHING REGULATORY OPTIONS: PUBLIC VS. PRIVATE, VOLUNTARY VS. MANDATORY.....	715
	A. <i>Industry Example: Farm Bureau’s Privacy and Security Principles for Farm Data</i>	716
	B. <i>Industry Example: Ag Data Transparent Project</i>	719
	C. <i>Federal Proposal: Agriculture Data Act of 2018</i>	721

- D. *Identifying Priorities: Political, Environmental, Social, and Economic Debates* 722
- E. *Next Steps: Potential Options* 725
 - 1. Enact Legislation Similar to the Agriculture Data Act of 2018 725
 - 2. Expand Access to Open Data 726
 - 3. Address Agricultural and Food Industry Consolidation 727
 - 4. Reinforce Producer Education and Understanding of Responsibilities 728
 - 5. Expanding Trade Secret Law to Specifically Include Agricultural Data and Business Operations 729
 - 6. Public Support to Increase Technology Infrastructure and Access 730
 - 7. Enacting a Federal Agricultural Data Protection Law 731
- VIII. CONCLUSION 732

I. INTRODUCTION

Technology advancements make life, work, and play easier and more enjoyable in many ways. Technology issues are also the cause of many headaches and dreams of living out the copier destruction scene from the movie “Office Space.”¹ Whether it be user error or technological error, one key technology issue on many minds right now is how all the data produced every second of every day, in hundreds of different ways, is used by those that collect it.

How much data are we talking about here? In 2018, the tech company Domo estimated that by 2020 “1.7 MB of data will be created every second” for every single person on Earth.² In 2019, Domo’s annual report noted that “Americans use 4,416,720 GB of internet data including 188,000,000 emails, 18,100,000 texts and 4,497,420 Google searches every single minute.”³ And this was before the pandemic of 2020, which saw reliance on remote technology and the internet skyrocket.⁴ It is not just social media and working from home that generates data—the “Internet of Things” (“IoT”) is expanding

1. OFFICE SPACE (20th Century Fox 1999).

2. *Data Never Sleeps 6.0*, DOMO, https://www.domo.com/assets/downloads/18_domo_data_never_sleeps-6-verticals.pdf [<https://perma.cc/G626-2WQA>].

3. Nicole Martin, *How Much Data Is Collected Every Minute of the Day*, FORBES (Aug. 7, 2019, 3:34 PM), <https://www.forbes.com/sites/nicolemartin1/2019/08/07/how-much-data-is-collected-every-minute-of-the-day/?sh=5baf1d683d66> [<https://perma.cc/63ZS-T9TJ>].

4. See Ella Koeze & Nathaniel Popper, *The Virus Changed the Way We Internet*, N.Y. TIMES (April 7, 2020), <https://www.nytimes.com/interactive/2020/04/07/technology/corona-virus-internet-use.html> [<https://perma.cc/3NGK-GJTU>].

exponentially.⁵ From our homes (smart appliances and thermostats), to entertainment (smart speakers and tablets), to what we wear (smartwatches and fitness devices), we are producing data constantly. Over 30 billion devices currently make up the IoT, and that number will double by 2025.⁶ The IoT is roughly defined as “devices—from simple sensors to smartphones and wearables—connected together.” That connection allows the devices to “talk” to each other across networks that stretch across the world, sharing information that in turn can be analyzed (alone or combined with data from other users) in ways that may be beneficial to the user or the broader economy.⁷

The key word in that last sentence is “may.” When it comes to the data that individuals and businesses across the world produce every second of every day, some of it—perhaps most of it—could be used in ways that are not beneficial to the user or the entire economy. Some data types can be used to cause harm in obvious ways, such as personal identifying information in cases of identity theft. While some data types may seem innocuous or harmful when viewed on their own, when combined with other data from the same user or even other users, it can be used in a wide variety of ways. While I find it beneficial to know how many steps I take in a day or how much time I sleep at night, I am not the only individual or entity with access to that information. The company that owns the device I wear also takes that information and uses it in ways that are beyond my control.⁸ Why would a company do that? In many instances, “[t]he data generated by the Internet of Things provides businesses with a wealth of information that—when properly collected, stored, and processed—gives businesses a depth of insight into user behavior never before seen.”⁹

Data security and privacy in general are issues that all companies manage as they work to protect the data we provide. Some types of data receive heightened protections, as discussed below, because they are viewed as personal, as private, or as potentially dangerous since unauthorized access to them could cause harm to the user/owner.¹⁰ Some states and countries have taken a step further, focusing not on industry-related data that needs particular types of protection, but in-

5. Arkady Zaslavsky, Charith Perera & Dimitrios Georgakopoulos, *Sensing as a Service and Big Data*, PROC. INT’L CONF. ADVANCES CLOUD COMPUTING 21 (July 2012), https://www.researchgate.net/publication/234017925_Sensing_as_a_Service_and_Big_Data [https://perma.cc/PV29-W2LY].

6. *What Is the Internet of Things?*, TALEND, <https://www.talend.com/resources/internet-of-things/> [https://perma.cc/TYS7-NLTX].

7. Matt Burgess, *What Is the Internet of Things? WIRED Explains*, WIRED (Feb. 16, 2018), <https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot> [https://perma.cc/PE22-3MSD].

8. See TALEND, *supra* note 6.

9. *Id.*

10. See *infra* Part IV.A.

stead looking at an individual's overall right to privacy, particularly on the internet. Those protections are summarized below.¹¹

It makes sense, you might say, to worry about financial or health-care data remaining private and to not want every website you have ever visited to keep a file of information on you. But why might we care about the use of data in agricultural operations? Depending on who you ask, the answer may be that agricultural data needs no more care or concern than any other type of business data. Some argue that the use of "Big Data" in agriculture provides opportunities for smaller operations and shareholders. These opportunities include increased power in a market driven for many years by the mantra "bigger is better"¹² and increased production of food staples across the world—both in a more environmentally-friendly fashion.¹³ While the benefits of technology and Big Data in the agricultural sector unarguably exist, questions remain as to how to best manage data privacy concerns in an industry where there is little specific law or regulation tied to collection, use, and ownership of this valuable agricultural production data.

In the following pages, this Article discusses what types of data are currently being gathered in the agricultural sector and how some of that data can and is being used. In addition, it focuses on unique considerations tied to the use of agricultural data and why privacy concerns continue to increase for many producers. As the Article looks at potential solutions to privacy concerns, it summarizes privacy-related legislation that currently exists and ends by looking at whether any of the current privacy-related laws might be used or adapted within the agricultural sector to address potential misuse of agricultural data.

II. AGRICULTURE & BIG DATA—WHAT ARE THEY AND HOW ARE THEY USED?

A. *What Is Agricultural Data?*

Many categories of data could fall under the definition of agricultural ("ag") data. There is not an official legal definition, but generally there are six basic types of data categories that fall under this phrase: agronomic, land, machine, weather, production, and livestock data.¹⁴

11. See *infra* Parts IV.D, V.

12. See Foteini Zampati, *Does Data Mean Power for Smallholder Farmers?*, WORLD BANK BLOGS (Sept. 26, 2019), <https://blogs.worldbank.org/pendata/does-data-mean-power-smallholder-farmers> [<https://perma.cc/5G7W-5VRC>].

13. Nurhan Dunford, *Big Data and Opportunities for Agricultural and Food Industries*, OKLA. STATE UNIV.: EXTENSION (Dec. 2017), <https://extension.okstate.edu/fact-sheets/big-data-and-opportunities-for-agricultural-and-food-industries.html> [<https://perma.cc/W6T3-39GD>].

14. Todd J. Janzen, *Legal Aspects Related to Agricultural Data Collection, Storage and Use 2* (Feb. 28, 2018), <http://wdmc.org/wp-content/uploads/2019/05/Janzen-Todd.pdf> [<https://perma.cc/Z7F7-ARHW>].

As we consider why privacy of this type of data matters, it is important to understand these data categories that collectively comprise ag data and a few other related terms. Todd Janzen is an attorney and Administrator of Ag Data Transparent, a certification program focused on increasing transparency in how ag data is managed between producers and companies.¹⁵ He defines these terms as set forth below:

- Agronomic Data—information related to plants, such as soil nutrient levels, crop selection, herbicide and pesticide application, and yield.
- Land Data—information related to topography, slope, soil type, etc.
- Machine Data—information related to the performance measurement of machines, such as fuel usage, hours operated, RPMs, ground speed, oil usage, etc.
- Weather Data—information related to climate, such as temperature and precipitation.
- Production Data—information related to a farm’s financial and contractual arrangements.
- Livestock Data—information related to livestock genetics, production, feed consumption, medicine usage, etc.¹⁶

Janzen points out that geospatial information is a common thread between these data types.¹⁷ Geospatial data is data “associated with a particular location.”¹⁸ When thinking about agricultural production, you can see the location tie to all of the above data types. Not only can we consider production data per field, but now fields and pastures may be broken down into smaller, specific areas that can be managed with precise attention—a key aspect of “precision agriculture.”¹⁹ In addition, farm data may be collected by multiple sources: the farmer, either an individual or a company at the request of the farmer, or an outside party unrelated to the farmer and not upon his or her request.²⁰ Data collected by third parties (perhaps from public records or publicly available sources like Google Earth) and by outside parties at the farmer’s request are the focus of much of the data privacy de-

15. See *Ag Data Transparent: Information About the Project to Bring Transparency to Ag Data*, JANZEN SCHROEDER AGRIC. L., LLC, <https://www.aglaw.us/agdatatransparent> [<https://perma.cc/RKE2-F4MU>] [hereinafter *Ag Data Transparent*].

16. Janzen, *supra* note 14, at 2.

17. *Id.* at 2–3.

18. Matt Sheehan, *Why Geospatial Technology Is So Important*, LINKEDIN (Nov. 14, 2018), <https://www.linkedin.com/pulse/why-geospatial-technology-so-important-matt-sheehan#:~:text=%22Geospatial%20is%20data%20that%20is,ask%20'where'%20based%20questions> [<https://perma.cc/KER2-7M98>].

19. See Peter Rodericks Oisebe, *Geospatial Technologies in Precision Agriculture*, GIS LOUNGE (Oct. 9, 2012), <https://www.gislounge.com/geospatial-technologies-in-precision-agriculture/> [<https://perma.cc/98BU-APC2>].

20. Ashley Ellixson et al., *Legal and Economic Implications of Farm Data: Ownership and Possible Protections*, 24 DRAKE J. AGRIC. L. 49, 53–54 (2019).

bate, as concerns over how third parties may use data, particularly non-public data, abound.²¹

Another term often used in this discussion is “big data,” a generic term with multiple meanings, all of which generally refer to “the exponential increase and availability of data,” the size of which requires some sort of structure for use and analysis.²² In the early 2000s, the mainstream definition of big data was developed, focusing on the three “Vs”: volume (large amounts), velocity (generated at a fast pace), and variety (various forms of data, both structured and unstructured).²³ More recently, the definition has been expanded to include additional “Vs,” such as: veracity (quality of data), variability (changing meanings of data), visualization (how to make data understandable through graphs and information), and value (using data to improve operations through efficiency or other savings).²⁴ Typically, this means that to use the data in a meaningful way, particularly over time, a person must use some sort of program or other mechanism to parse through the data since there is too much data for one person to analyze. The rise of careers in areas like data analytics is a result of the massive increase in data and the need to develop expertise in how to use it most effectively and efficiently.²⁵

In agriculture, data for one field, or perhaps even one farm, might not be considered “big data.” But when you combine the information for that farm across multiple years, or you have thousands of acres of fields, tens of thousands of heads of cattle grazing over large expanses of territory, or data from hundreds of thousands of customers, the amount of data can be overwhelming to comprehend. This process of combining data is referred to as “aggregation.”²⁶ Often, aggregated data is “anonymized.” Anonymization is an attempt to remove any information that would identify the data’s origin.²⁷ That usually means removing field location and ownership information from field data.²⁸ However, as I will discuss, anonymizing data may not always make the data as unidentifiable as privacy interests might prefer.

21. *See id.* at 52–54.

22. *What Is Big Data?*, UNIV. WIS. DATA SCI., <https://datasciencedegree.wisc.edu/data-science/what-is-big-data/> [<https://perma.cc/SKU5-575D>] (emphasis omitted).

23. *Id.*

24. *Id.*

25. *See Rise of the Data Analyst—What’s Behind the Boom?*, PURDUE UNIV. GLOB., <https://www.purdueglobal.edu/blog/information-technology/rise-of-data-analyst/> (Jan. 15, 2021) [<https://perma.cc/A5NE-7SY4>].

26. Janzen, *supra* note 14, at 3.

27. *See id.*

28. *Id.*

B. *Data Gathering and Use by Agricultural Producers*

1. Collecting Data

Agricultural production data is gathered in many ways, often without a producer specifically submitting data to a particular entity. For example, pre-installed GPS systems track location and speed on new tractors, and other technologies embedded in tractors track hours of use and whether any implements or attachments are connected.²⁹ In addition to the tractor information, systems can track usage rates for attachments such as sprayers and applicators, noting how much product is applied to a field or the rate at which a field was seeded.³⁰ Combines not only track location and speed via GPS, but can identify a product's moisture level and a field's yield.³¹

In addition to sensors and location information gathered by farm equipment, soil data is collected through testing or embedded sensors.³² Weather data can be gathered from on-farm locations as well as other centralized aggregate providers.³³ Satellites and drones can capture images that provide information on soil quality, nutrients, and erosion.³⁴ A recent survey conducted by Purdue University indicated that some form of data collection is happening on a majority of farming operations.³⁵ The survey collected information from 800 farming operations, seeking information on "the demographics of farm operators, the type of agronomic data they collected, and how the information is used."³⁶ Of those surveyed, "82[%] collect[ed] yield data, 77[%] collect[ed] soil data, 73[%] create[d] GPS maps from their data, and 47[%] of respondents collect[ed] satellite or drone imagery."³⁷ Larger farms collected data more often than smaller farms, particularly regarding imagery data.³⁸ Younger farmers with post-secondary degrees were also more likely to collect farm data and use some type of software to help analyze and use the information.³⁹ For farmers who did not indicate that they gathered data, major factors included

29. Thomas J. Horton & Dylan Kirchmeier, *John Deere's Attempted Monopolization of Equipment Repair, and the Digital Agricultural Data Market – Who Will Stand Up for American Farmers?*, COMPETITION POL'Y INT'L: ANTITRUST CHRON., Jan. 2020, at 1, 5, <https://ssrn.com/abstract=3541149>.

30. *Id.*

31. *Id.* at 5–6.

32. *How We Collect Agricultural Data*, ONE SOIL/BLOG, <https://blog.onesoil.ai/en/how-onesoil-collects-data> [<https://perma.cc/3CDL-S4RP>].

33. *Id.*

34. *Id.*

35. Robin Booker, *Farm Data Collection and Farmer Use Analyzed*, THE W. PRODUCER (April 16, 2020), <https://www.producer.com/crops/farm-data-collection-and-farmer-use-analyzed/> [<https://perma.cc/C2KR-LGD6>].

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

cost and a lack of perceived benefit.⁴⁰ Of those that did not collect data, privacy was cited by about 10% as a reason for not collecting farm data, which the survey noted was “really . . . surprising in light of some current events.”⁴¹

2. How Data Is Used by Producers—Rise of Precision Agriculture

How producers use the data they gather is an important question. The Purdue survey referenced above found that the main ways producers used data was to influence nutrient management (typically fertilizer applications), seeding rates, and drainage decisions.⁴² The more data collected, the higher percentage of producers who indicated a positive impact on yield.⁴³ In short, farmers are using farm data to make planting decisions, manage soil quality and nutrient loss, and balance weather concerns through irrigation and drainage control.⁴⁴ In order to do so, most producers subscribe to one or more software services to help manage the data and turn it into actionable recommendations.⁴⁵ Many producers also share the data with an agronomist as part of the planning and crop-management process.⁴⁶

The massive increase in agricultural data collection has been a driving factor in the rise of precision agriculture.⁴⁷ Precision agriculture involves collecting and using large amounts of high-quality data. This data is analyzed and manipulated to prescribe location- and/or timing-specific applications of management practices.⁴⁸ Often, management practices are applied not only to an entire field but also at a more targeted and focused level, with opportunities to treat a field by area of specific need.⁴⁹ This targeted pesticide or nutrient application will ideally lead to a more effective, efficient, economical, and environmentally friendly treatment of fields and crops.⁵⁰ From a producer standpoint, the potential exists for a positive impact from the collection and use of this data, from lower input costs to higher yields. However, there are also obstacles that stand in the way of large-scale adoption and use of precision agriculture tied to data collection.

Cost is one of the biggest factors preventing widespread adoption of data gathering techniques. Not only is there a cost for equipment used

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. *See id.*

45. *Id.*

46. *Id.*

47. *See Precision, Geospatial & Sensor Technologies Programs*, U.S. DEP'T AGRIC.: NAT'L INST. FOOD & AGRIC., <https://nifa.usda.gov/program/precision-geospatial-sensor-technologies-programs> [<https://perma.cc/8KWG-LK93>].

48. *Id.*

49. *Id.*

50. *See id.*

to gather the information at the farm level (tractors, combines, planters, etc.), but the producer needs to ensure the farm has: (1) the equipment to store and manage this data over time; (2) software programs that aggregate and analyze the data; and (3) a variety of additional costs and expenses that come with trying to sift through massive amounts of data to find potential improvements in a targeted way.⁵¹ As farmers noted in the Purdue study, many have multiple software subscriptions to manage data. Yet many still feel the potential for more effectively using the data to improve the farming operation remains largely unrealized.⁵²

Precision agriculture is one of the great opportunities for increasing production to feed a growing world, adapting to climate change concerns, and producing more food on less land, all in a more environmentally friendly way by reducing chemical inputs wherever possible. As we see more demand for this type of production, barriers to adoption serve to drive smaller producers out of business. Unable to compete with larger operations that can better afford this type of technology, there is a significant risk that pressure put on farmers to use big data will only lead to further increases in industrialized production and farm size. As we consider how to manage concerns related to agricultural data use, collective data use may play a significant role in any proposal, such that smaller operations are not penalized for an inability to quickly adopt and invest in this technology.

III. WHY IS USE OF AG DATA BY THIRD PARTIES A CONCERN?

As noted above, precision agriculture and developing sustainable, resilient agricultural production systems to feed a growing world are key benefits of gathering and analyzing data in the agricultural sector. While there are many potential benefits, the agricultural system's current structure causes concern among some within the industry. In particular, producers' perceived lack of power relative to agribusinesses' strong power and control leads to uncertainty about how to manage ag data in a way that does more good and less harm to those that work the land.⁵³ While changes in the agricultural sector and power dynamics are influenced by a number of issues and reasons over time, the fact that significant changes occurred since the 1900s is clear. Between 1900 and 2005, "the number of farms [fell] by 63[%], while the aver-

51. See Booker, *supra* note 35.

52. *Id.*

53. See generally Leanne Wiseman et al., *Farmers and Their Data: An Examination of Farmers' Reluctance to Share Their Data Through the Lens of the Laws Impacting Smart Farming*, 90 WAGENINGEN J. LIFE SCIS. 1 (2019), <https://doi.org/10.1016/j.njas.2019.04.007> (explaining attitudes of Australian farmers regarding sharing agricultural data in light of perceived lower bargaining power in ownership and management of agricultural data).

age farm size [rose] 67[%].”⁵⁴ Specialization in farming operations also increased dramatically, as farms in 1900 produced an average of five commodities per farm before declining to just one per farm in 2000, largely as a result of efficiencies of scale and risk management programs.⁵⁵ While farming operations have become more efficient, farmers receive less of the food dollar than ever. “After accounting for input costs, farmers and ranchers receive only [eight] cents out of every dollar spent on food at home and away from home. The rest goes for costs beyond the farm gate: wages and materials for production, processing, marketing, transportation[,] and distribution.”⁵⁶ Small farms often struggle to survive, particularly in this era of low prices, market challenges and decreased independence in the market.⁵⁷

A. Power Dynamics

The agricultural industry is increasingly one of the most concentrated industries, with impact from top (food processors and manufacturers, meat packers, and grain processors) to bottom (seeds and crop input suppliers).⁵⁸ For example, recent mergers in the agricultural input sector reduced the number of major providers of these products from six to four, with those remaining companies controlling approximately 60% of the global seed and chemical supply.⁵⁹ While agribusiness companies argue that consolidation and mergers are necessary

54. Carolyn Dimitri, Anne Effland & Nielson Conklin, *The 20th Century Transformation of U.S. Agriculture and Farm Policy*, U.S. DEP’T AGRIC., ECON. RSCH. SERV. 1, 2 (2005) (citation omitted), https://www.ers.usda.gov/webdocs/publications/44197/13566_eib3_1_.pdf [<https://perma.cc/RSA3-CWMY>].

55. *Id.*

56. *Fast Facts about Agriculture & Food*, AM. FARM BUREAU FED’N, <https://www.fb.org/newsroom/fast-facts> [<https://perma.cc/L7TS-EEAM>] (emphasis omitted).

57. See Alana Semuels, ‘They’re Trying to Wipe Us Off the Map.’ *Small American Farmers Are Nearing Extinction*, TIME (Nov. 27, 2019, 1:16 PM), <https://time.com/5736789/small-american-farmers-debt-crisis-extinction/> [<https://perma.cc/LZ9P-27SW>]; Arohi Sharma, *Ag Policy Must Value Independent Farmers Over Corporate Ag*, NAT. RES. DEF. COUNCIL (Jan. 8, 2020), <https://www.nrdc.org/experts/arohi-sharma/valuing-independent-farmers-over-corporate-agribusinesses> [<https://perma.cc/ZM8H-3LTJ>].

58. See Zoe Willingham & Andy Green, *A Fair Deal for Farmers*, CTR. FOR AM. PROGRESS (May 7, 2019, 12:00 PM), <https://www.americanprogress.org/issues/economy/reports/2019/05/07/469385/fair-deal-farmers/> [<https://www.perma.cc/3FAH-3T9A>]; Kristina “Kiki” Hubbard, *The Sobering Details Behind the Latest Seed Monopoly Chart*, CIV. EATS (Jan. 11, 2019), <https://civileats.com/2019/01/11/the-sobering-details-behind-the-latest-seed-monopoly-chart/> [<https://perma.cc/8G7E-QN65>].

59. James M. MacDonald, *Mergers in Seeds and Agricultural Chemicals: What Happened?*, U.S. DEP’T AGRIC.: ECON. RSCH. SERV. (Feb. 15, 2019), <https://www.ers.usda.gov/amber-waves/2019/february/mergers-in-seeds-and-agricultural-chemicals-what-happened/> [<https://perma.cc/73MY-72UA>]; Naki B. Mendoza, *Will Big Agriculture Mergers Impact Smallholder Farmers?*, DEVEX (Sept. 29, 2016), <https://www.devex.com/news/will-big-agriculture-mergers-impact-smallholder-farmers-88820> [<https://perma.cc/N7F9-VSLP>]; Hubbard, *supra* note 58.

for competing and maintaining the investment level required to research and develop new crop technologies, significant concerns about access and cost arise as well. For smaller farmers who purchase fewer inputs, this means less room to negotiate price and access. Consolidation also encourages monoculture, where fewer crops are grown on more acres to increase the efficiency of scale and spread input costs over more acres.⁶⁰ Over time, consolidation has led to “less choice and higher prices for farmers.”⁶¹ It is also not clear that consolidation has led to an increase in research and development, as some “studies suggest increased market domination removes companies’ incentive to innovate,” and that research in the private sector has decreased in the post-merger period.⁶²

Agribusiness companies also exert power over producers through limits on technology use and access and through various agreements that producers sign to utilize services and products. For example, if a producer were to purchase a new tractor to track data more precisely, the tractor manufacturer may view the transaction more as a technology lease than a machine sale.⁶³ There are two issues here. First, software and technology in the farm machinery itself, and, second, who owns that technology and software in addition to the equipment. Traditionally, farmers have become adept at repairing, upgrading, and modifying farm equipment to save costs and meet farm needs.⁶⁴ However, according to manufacturers like Deere, with the dramatic increase in computerization of equipment,

Anything a farmer does on a modern tractor, beginning with opening the cab door, generates messages captured by its main onboard computer, which uploads the signals to the cloud via a cellular transmitter [often] located . . . beneath the driver’s seat. These machines have been meticulously programmed and tested to minimize hazards and maximize productivity.⁶⁵

Because of that programming, Deere argues that attempting to repair or modify equipment is too complicated for farmers and accordingly that only authorized dealers can modify or repair machinery.⁶⁶ This “right to repair” argument is not new, spanning technology such as iPhones and cars, but is taking on new life in the agricultural industry where reducing costs by maintaining older equipment for longer peri-

60. *Monoculture Farming in Agriculture Industry*, EARTH OBSERVING SYS. (Oct. 20, 2020), <https://eos.com/blog/monoculture-farming/> [<https://perma.cc/PYM8-CT8Q>].

61. Hubbard, *supra* note 58.

62. *Id.*

63. See Peter Waldman & Lydia Mulvany, *Farmers Fight John Deere Over Who Gets to Fix an \$800,000 Tractor*, BLOOMBERG: BUSINESSWEEK (March 5, 2020, 4:00 AM), <https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor> [<https://perma.cc/6MX2-5KD2>].

64. *Id.*

65. *Id.*

66. *Id.*

ods of time is not just the norm, but often a requirement to remain in business.⁶⁷ In addition, when Deere first “began gathering and transmitting production data from farmers’ machines, it didn’t immediately tell them.”⁶⁸ This was by no means just an issue tied to John Deere but was and is seen throughout the industry and was essentially what led to the rise of many concerns related to data misuse, abuse of trust, and basic ownership of the data itself.⁶⁹

1. Misuse and Abuse

How can agricultural data be misused in a way that would harm a producer, beyond perhaps the concern that smaller farmers may be left behind or forced out of business? In a *Journal of Agricultural and Environmental Ethics* article, Mark Ryan noted that agricultural big data analytics “can be used as a form of manipulative power to initiate cheap land grabs and acquisitions[,]” to “pressur[e] farmers into situations they would not have otherwise chosen[,]” and to “force farmers into precarious and vulnerable positions.”⁷⁰

Ryan’s article on agriculture, big data, ethics, and power identifies many potential ways in which those with power, typically larger agribusinesses and data aggregators, can utilize that power and data to harm producers.⁷¹ These tactics include using data provided by a producer to benefit that farmer through targeted management improvements but also for personal, more “nefarious means that the farmer is unaware of, such as farm acquisition and land grabs.”⁷² Third parties can analyze data to determine which land is most profitable and can use this information to manipulate farmers into selling high-quality land at lower prices, to apply restrictive and economically burdensome policies to certain customers, and to undercut asking prices on land deemed less profitable.⁷³ In these instances, the farmer has provided data, likely through a technology agreement with an agribusiness partner or through use of analytic software.⁷⁴ In turn, the partner sells that data to a third party to increase the partner’s profits.⁷⁵ While data may be anonymized and combined with that of other producers, in many instances the possibility of identifying farmers and field locations remains.⁷⁶ When this occurs, the farmer, who received some sort of initial benefit from the provision of farm data, may ultimately face

67. *Id.*

68. *Id.*

69. *Id.*

70. Mark Ryan, *Agricultural Big Data Analytics and the Ethics of Power*, 33 J. AGRIC. & ENV’T ETHICS 49, 49 (2020), <https://doi.org/10.1007/s10806-019-09812-0>.

71. *Id.* at 58.

72. *Id.*

73. *Id.* at 58–59.

74. *Id.* at 53.

75. *See id.* at 53, 58–59.

76. *See id.* at 58.

harm from others' use of the data.⁷⁷ This type of data-sharing abuse will only lead to further increase in corporate ownership of farms and increased farm size, as those most able to use the data in this way also have the funds to follow up on land purchases.⁷⁸

Ryan discusses other types of data-sharing abuse as well, including using power dynamics to convince a farmer that the only way to obtain some particular benefit or service is to share farm data with that service provider or a partner entity.⁷⁹ Farmers who either decline to share data or put restrictions on how farm data is used may find themselves without access to information and services that would help increase yield while managing costs. In other words, those farmers would be at a competitive disadvantage.⁸⁰ When farmers opt to share data and obtain services, they are unable to negotiate and are forced to agree to terms or conditions that they would not normally agree to.⁸¹ Agreeing to unsatisfactory terms may mean contractually giving up data ownership or, as discussed previously, forfeiting the right to repair equipment or access technology included in machinery.⁸²

Farmers often have longstanding relationships with their suppliers and rely upon them to make recommendations and provide advice that will sustain the farming operation's success.⁸³ Farmers' trust and reliance on suppliers and buyers can put them in precarious positions because they may be taken advantage of by agreeing to terms and conditions they do not fully understand.⁸⁴ Ryan notes that in a 2016 American Farm Bureau survey, "a disproportionate number of farmers did not know about their data or what the terms and conditions implied in their agreement."⁸⁵ The survey indicates that, while over 50% of farmers enter agreements in which they are unsure who owns the data and whether it could be shared with third parties, they trust that the various agribusiness or technology partner has the farmers' best interests in mind.⁸⁶ While that may often be true, it is also in the agribusiness company's best interest to get access to the data in a way that helps the farmer through the provision of better recommendations and management practices and helps the company by including as few data use restrictions as possible.

Another way in which companies abuse power and data access is by making it very difficult to switch technology, software, or data analyt-

77. *See id.* at 58–59.

78. *Id.* at 59.

79. *Id.* at 58–59.

80. *Id.* at 60.

81. *See id.* at 60–61.

82. *Id.*

83. *Id.* at 62.

84. *Id.*

85. *Id.*

86. *Id.*

ics providers.⁸⁷ Companies compete for access to farm data,⁸⁸ and it is in their interests to restrict how farmers could later share past analyses and summaries. While farmers may own actual raw farm data, technology providers retain ownership of the aggregated and analyzed data and may control how it is used.⁸⁹ This data analysis loss makes it difficult for farmers to consider switching providers and can coerce continued relationships due to information loss and prior investment.⁹⁰

Another concern regarding data misuse occurs when companies utilize production records to determine product costs. This type of pricing model, using production estimates and history to estimate outcomes for the upcoming season, can be a useful risk-management tool for farmers by sharing both potential loss and unexpected income with the supplier while managing costs based upon production.⁹¹ However, there are tradeoffs to this type of risk-management tool, such as the fact that data sharing is a necessity, and it is unlikely that farmers would be able to restrict how suppliers would use the data provided to them.⁹² However, input suppliers could use this data to manipulate pricing and markets, particularly if pricing and agreement determinations are not transparent. It is unlikely that a supplier would want to share that type of information publicly.⁹³ Suppliers may also drive customers into this type of model, potentially to the farmer's detriment, by limiting access to certain products or programs.⁹⁴ While a farmer could use a different seed or chemical, at times, those options could be limited, or alternatives may put the farmer at a disadvantage.⁹⁵ Instead of true risk-management opportunities for the farmer, this tactic could lead to price discrimination if a supplier were to "increase their production costs in accordance with what they know the farmer can pay for their goods and services," which could be "derived from the exact data that they are retrieving from the farmer under the auspice of helping them improve their management decisions."⁹⁶

IV. EXISTING DATA PRIVACY LAWS AND REGULATIONS

Farm data use can intentionally or unintentionally harm farmers and can have severe consequences. These consequences affect individ-

87. *Id.* at 62–63.

88. *Id.* at 60.

89. *Id.* at 63

90. *Id.*

91. Ben Nuelle, *Outcome-Based Pricing Aims to Reduce Farmers' Financial Risk*, HOOSIER AG TODAY (Jan. 9, 2020), <https://hoosieragtoday.com/outcome-based-pricing-aims-reduce-farmers-financial-risk/> [<https://perma.cc/9CVF-KWX2>].

92. *See id.*

93. Ryan, *supra* note 70, at 65.

94. *Id.* at 64.

95. *See id.*

96. *Id.* at 65.

ual farmers and impact larger industry issues related to land ownership and control, sustainability, and autonomy. As the farm data use continues to grow at an exponential level, concerns over misuse and abuse grow as well. Unlike other industries, there is no targeted farm data privacy law.⁹⁷ However, many data privacy laws and protections do exist, and as we consider whether a farm data-specific law is necessary to protect vulnerable farmers, reviewing similar laws is valuable.

A. *Federal Law—Industry Specific*

A number of federal statutes, including some dating back to the 1970s, have been enacted over the years to address a variety of concerns related to data privacy. One thing all of these have in common is their focus on personal data, which is data connected to an individual.⁹⁸ For agricultural data, much of that we are discussing is not personal data attributed to just one person. Instead, it is business data—data tied to the business of farming—even if the farm itself is not incorporated as a business entity. As noted above, farm data use creates risks, such that some privacy regulation may be warranted.

1. Fair Credit Reporting Act (“FCRA”)

The Fair Credit Reporting Act⁹⁹ was one of the first federal laws related to data privacy in the United States.¹⁰⁰ Passed in 1970, it regulates how businesses can use personal information when creating or furnishing consumer reports and aims to “promote[] the accuracy, fairness, and privacy of information in the files of consumer reporting agencies.”¹⁰¹ Consumers are provided rights related to the information contained within the file, including viewing it, disputing it, and notification of adverse actions based on report data.¹⁰² The law has been updated over the years to reflect advancements in information gathering and to reflect the breadth of companies that collect, use, and rely upon this type of information. As related to privacy, consumer report information cannot be provided to those without a purpose that is not specified in the FCRA.¹⁰³ Because entities can use this information in ways that lead to negative effects or prejudicial impacts

97. See Ellixson et al., *supra* note 20, at 65–66; see also Jody L. Ferris, Note, *Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary?*, 18 MINN. J.L. SCI. & TECH. 309, 318 (2017).

98. *What Is Personal Data?*, EUR. COMM’N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [<https://perma.cc/V9C9-864Z>].

99. 15 U.S.C. § 1681(a)–(x).

100. Morey Elizabeth Barnes, Note, *Falling Short of the Mark: The United States Response to the European Union’s Data Privacy Directive*, 27 NW. J. INT’L L. & BUS. 171, 173–74 (2006).

101. *A Summary of Your Rights Under the Fair Credit Reporting Act*, FED. TRADE COMM’N 1, <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> [<https://perma.cc/3SKG-GDLM>].

102. *Id.*

103. *Id.* at 2.

upon consumers, the importance of limiting access and assuring accurate information is vital. The rise of identity theft led to an increased realization that data privacy is of utmost concern to consumers and, ultimately, to increased protections for victims under the FCRA, both for financial data and that of other types as well.¹⁰⁴

2. Children's Online Privacy Protection Act ("COPPA")

The Children's Online Privacy Protection Act¹⁰⁵ is a 1998 federal law enacted to address concerns over the growth of the internet and increased use of that medium by minors.¹⁰⁶ COPPA limited the type of information that websites could collect from children under the age of thirteen and also required parent approval prior to collecting certain personal information from minors.¹⁰⁷ These rules are directed at "websites targeted towards children and general websites where operators have knowledge that children visit."¹⁰⁸ There are "five major requirements: (1) notice, (2) parental consent, (3) parental review, (4) security, and (5) limits on the use of games and prizes."¹⁰⁹

Most relevant to our discussion here is the definition of "personal information" that is limited for collection purposes. As amended, this includes data such as name, physical address, contact information (phone numbers, emails, screen names, etc.), identifiers such as IP addresses or device identifiers, social security numbers, photographs, video or audio files, and geolocation information.¹¹⁰

In addition, COPPA contains a notice requirement that websites "must provide notice of what information they collect . . . [.] how that information is used, and to whom that information is disclosed."¹¹¹ The notice cannot be hidden—instead, it "must be done in a 'clear and prominent manner.'"¹¹² Notice involves making parents aware of what information is collected, how it is used, and anyone to whom it is disclosed.¹¹³

While COPPA is far from perfect, it continues to be one of the main ways children's personal information is protected, despite dramatic in-

104. See 15 U.S.C. § 1681c-1; Brendan Delany, Comment, *Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Imposter Fraud*, 54 CATH. U. L. REV. 553, 564–65, 564 n.54 (2005).

105. 15 U.S.C. §§ 6501–6506.

106. See *Complying With COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#A.%20General%20Questions> [https://perma.cc/PWW5-7PGJ].

107. See 15 U.S.C. §§ 6501–6502.

108. Tianna Gadbow, *Legislative Update: Children's Online Privacy Protection Act of 1998*, 36 CHILD. LEGAL RTS. J. 228, 228 (2016).

109. *Id.*

110. 15 U.S.C. § 6501(8).

111. Gadbow, *supra* note 108, at 228.

112. *Id.*

113. *Id.* at 229.

creases in data collection, even from the time a child is born.¹¹⁴ Why does this matter? As discussed in a recent article looking back at thirty years of COPPA's existence, the author noted that information "may be used to market products to which they are particularly susceptible, leading to consumerism and family financial pressure, or the purchasing of inappropriate products."¹¹⁵ Advertisements, when regularly viewed, heavily influence children's decisions and actions. This type of profiling and marketing can cause emotional harm, unhealthy behaviors, and other negative consequences.¹¹⁶ Physical safety risks also continue to exist, and use of metadata and other personal information, often gathered from devices worn upon or carried by the person, may allow location to be identified.¹¹⁷ Risks associated with identifying them, including bullying, harassment, blackmail, enticement, and other social harms, are also increasingly occurring.¹¹⁸

Also relevant is how the use and risks related to "algorithmic decision making, black box processing, and systems that make[] guesses about and differentiat[ing]" between users may cause missed opportunities through the use of labels or limitations on data shown,¹¹⁹ and it could manipulate users by "subverting user choice and autonomy and creating compulsive usage."¹²⁰

While we are rightfully more concerned about these impacts and children's privacy rights, data manipulation to drive decision-making and limited or targeted access to options is a significant concern for even the savviest adults.¹²¹ While data privacy laws cannot resolve all of these issues, notice and awareness can make inroads towards mitigating the impacts in agricultural data use and collection.

3. Gramm-Leach-Bliley ("GLB") Act

The Gramm-Leach-Bliley Act¹²² is a comprehensive law focused on the financial services industry, with a significant aspect focused on privacy issues.¹²³ There are three broad restrictions included in the GLB. Specifically, the GLB prevents covered entities from sharing any

114. *Id.* at 231; see also Chavie Lieber, *Big Tech Has Your Kid's Data — And You Probably Gave It to Them*, VOX (Dec. 5, 2018, 6:10 PM), <https://www.vox.com/the-goods/2018/12/5/18128066/children-data-surveillance-amazon-facebook-google-apple> [<https://perma.cc/Q6V9-9J4T>].

115. Ariel Fox Johnson, *13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone*, 44 SETON HALL LEGIS. J. 419, 440 (2020).

116. *Id.* at 440–41.

117. *Id.* at 441–42.

118. *Id.* at 442.

119. *Id.*

120. *Id.* at 443.

121. See *id.*

122. See Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 13 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

123. See Paul J. Polking & Scott A. Cammarn, *Overview of the Gramm-Leach-Bliley Act*, 4 N.C. BANKING INST. 1, 3 (2000).

“nonpublic personal information” with a nonaffiliated third party.¹²⁴ “Nonpublic personal information” is defined as information provided by consumers as part of any type of transaction or service or otherwise “obtained by the financial institution.”¹²⁵ Account information cannot be provided to non-affiliated third parties for use in marketing efforts, such as telemarketing or email.¹²⁶ Finally, there is a list of information related to the financial institution’s privacy policies that must be disclosed to consumers annually.¹²⁷ There are, of course, many exceptions to these disclosure provisions. One key exception allows disclosure of nonpublic information if consumers are given information on how the institution will work with third parties to use that data, and consumers do not affirmatively “opt out,” meaning the consumer needs to affirmatively request that the nonpublic data not be disclosed to a third party.¹²⁸ Another exception allows information sharing with nonaffiliated third parties that engage in business on behalf of the information, but those third parties must maintain privacy of that data.¹²⁹ Finally, a third exception allows data use under a limited list of circumstances, including issues like fraud prevention, with consent, risk control, and to certain consumer representatives.¹³⁰

Those subject to the privacy provisions are members of the financial industry, but this definition is quite broad and inclusive.¹³¹ Those required to abide by the GLB privacy provision include “any institution the business of which is engaging in ‘financial activities’” and does not require that the regulated business be actually engaged in financial activities itself.¹³² This means that many entities, beyond what we consider traditional banking or lending entities, are impacted by the GLB, such as stores or car dealers that extend credit to consumers or individuals that manage mutual funds or advise on investments.¹³³ The GLB provisions are drafted in such a way that allow the expansion of regulations to include new entities that ultimately fall under the definition of regulated industries and potentially add new types of non-public data.¹³⁴

Of particular relevance here is the broad definition of those included in the industry. For example, the definition of “affiliate” under the GLB states that “[a]n affiliation exists when one company ‘controls’ . . . is controlled by, or is under common control with another

124. *Id.* at 28.

125. *Id.*

126. *Id.*

127. *Id.* at 28–29.

128. *Id.* at 30.

129. *Id.* at 30–31.

130. *Id.* at 31–32.

131. *Id.* at 27–28.

132. *Id.* at 27.

133. *Id.* at 27–28.

134. *See id.*

company.”¹³⁵ This includes those that are and are not financial institutions but still fall under the affiliate definition.¹³⁶ Recognizing the relationship between entities is important, particularly when entities could use information in a way that is not always in the consumer’s best interest, or is being used to further the goals of an interested third party.

Similarly, the definition of “publicly available information” is worth noting. It includes information that can be found in public records (including real estate), widely distributed media like the newspaper or telephone book, and that are required to be provided to the public based on local, state, or federal law (such as registration documents for corporations or shareholder reports).¹³⁷ When it comes to much of the agricultural data that we discuss in the article, there is a mix of both public and nonpublic information. Information related to real estate ownership, for example, is public information, but that related to yield or crop management practices may not be depending on the person and the situation. For example, if a paper featured a grower as a top producer for a particular crop and provided yield information, that would be public information. Specific field-by-field information gathered by the producer and tracked through equipment, personal computing, or other similar records likely would not be deemed public. As we consider that much nonpublic information is gathered by various affiliates within the agricultural industry throughout the course of doing business with agricultural producers, the value of that data to third parties, how it is used and to whom it is provided, is valuable and important information for those within the industry to be aware of, and have the opportunity, perhaps, to opt-out of disclosure as well.

4. Health Insurance Portability and Accountability Act (“HIPAA”)

The Health Insurance Portability and Accountability Act¹³⁸ is one of the more commonly known federal data privacy laws. Enacted in 1998, HIPAA aims “to combat waste, fraud, and abuse in health insurance and health care delivery . . . to simplify the administration of health insurance, and [] other purposes.”¹³⁹ The data privacy and protection aspects of HIPAA that we are reminded of at every visit to a medical office fall under the “other purposes” provision,¹⁴⁰ and create “a national framework for privacy protection, thereby changing the

135. 17 C.F.R. § 248 (2000).

136. *Id.*

137. *Id.*

138. See Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

139. *Id.*, see also Jonathan P. Tomes, *20 Plus Years of HIPAA and What Have We Got?*, 22 QUINNIPIAC HEALTH L.J. 39, 42 (2018).

140. Tomes, *supra* note 139, at 42.

treatment of personal medical information.”¹⁴¹ As relevant to this discussion, HIPAA requires covered entities to secure certain types of protected health information (“PHI”).¹⁴² “PHI is individually identifiable health information transmitted or maintained in electronic form that is specifically targeted by HIPAA and its security and privacy rules.”¹⁴³

The privacy rules regarding PHI apply not just to those who collect the data, but to third parties and other associated business entities that have access to the data through various business relationships.¹⁴⁴ PHI disclosure is appropriate for actions such as “treatment, payment, or health care operations, or in response to a valid authorization.”¹⁴⁵ Those who gather, maintain, and/or use PHI must meet a “minimum necessary” standard of sharing information, meaning they should only disclose the least amount of PHI necessary to accomplish the authorized activity.¹⁴⁶ When sharing PHI with other business-related associates, the covered entity is responsible for first receiving assurances from those associates regarding privacy practices and actions to safeguard PHI.¹⁴⁷ These assurances must be written and documented, ensuring all parties understand the responsibilities, ramifications, and penalties for improper use or storage, and the liability, if applicable, for failing to meet these privacy standards.¹⁴⁸

While on its face HIPAA appears to restrict PHI use in a fairly strict fashion, the authorization option opens many doors for PHI use in ways beyond the typical needs required to provide healthcare. Privacy concerns arise not just through an individual’s authorization, and perhaps lack of understanding what the authorization allows, but even in the initial notices or rights and various disclosures that health care providers and other entities provide patients with and ask them to sign. While patients are provided forms that are supposed to ensure awareness “of their rights regarding PHI and how medical information may be used, disclosed, or amended,” research shows that many patients do not read the form or fully understand its terms.¹⁴⁹ While only about half of those provided the HIPAA disclosure forms actually read them, of those that do, approximately “one-third are unable to correctly answer questions about its terms.”¹⁵⁰ This lack of understanding and failure to read thoroughly means many individuals do

141. Michael W. Drumke, *A HIPAA Primer*, 37 BRIEF 34, 35 (Spring 2008).

142. *Id.* at 37.

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.* at 38.

149. *Id.*

150. *Id.*

not truly understand what is happening with their PHI when they sign the forms.

PHI privacy regulations' effectiveness is also limited by the use of authorization forms, which patients sign to voluntarily disclose information. Like many contracts, waivers, and other legally binding documents, how thoroughly they are read and understood, and the extent to which patients feel pressured to sign are important questions. There are similarities here to the use of agricultural data, particularly that collected by a third party at the request of a producer. As noted previously, agricultural producers may feel pressured or that they have no power to not sign various contracts that share or provide ownership of agricultural data to third parties in order for the producers to utilize the services being offered, perhaps necessary to increase efficiency or sustainability practices. Similarly, medical patients may feel pressured to sign PHI disclosure authorization forms in order to obtain certain care or services, such as medical trials.¹⁵¹ Supported and valid concerns exist regarding the impact of HIPAA on medical research and the hesitancy of some individuals to share past, present, and future medical records to participate in a medical trial.¹⁵² Similarly, there are concerns that agricultural research needs the type of data that is being generated on agricultural operations today in order to continue to engage in research that benefits not just the private sector, but the public sector as well.¹⁵³

HIPAA itself is not a direct answer or example of how we should consider addressing concerns regarding agricultural data privacy and use, but there are a number of correlations that make it important to consider, particularly when it comes to use of data for public research, individuals understanding authorizations, a lack of choice or negotiation power when it comes to authorizations, and the plethora of ways that third parties can profit off an individuals' data.

B. *Trade Secrets on the Farm*

While the federal laws discussed above involve protection of data and strive to ensure privacy of certain data categories, they all primarily or solely protect individuals, not businesses.¹⁵⁴ And while we often describe farming as a family business and think of farmers as individuals out working the land, the truth is that farming is a business, and much of the data types at issue here are not covered under

151. See generally Stacey A. Tovino, *The Use and Disclosure of Protected Health Information for Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation*, 49 S.D. L. REV. 447 (2004).

152. See generally *id.*; see also Roberta B. Ness, *Influence of the HIPAA Privacy Rule on Health Research*, 298 J. AM. MED. ASS'N 2164 (2007).

153. See Andreas Kamlaris et al, *A Review on the Practice of Big Data Analysis in Agriculture*, 143 COMPUTS. & ELECS. AGRIC. 23 (2017).

154. See *supra* Part IV.A.

the category-specific types of legislation described above at the federal level.¹⁵⁵ Before addressing the question if an agricultural-specific type of legislation is needed, we must first look at other options that businesses may use to protect the privacy and use of certain types of data. One of the main ways businesses seek to protect data is through use of trade secret protection.¹⁵⁶

“Property is only able to be owned to the extent the law will recognize and enforce ownership rights, and typically, the type of property determines the associated rights and responsibilities.”¹⁵⁷ Prior colleagues have looked at the issue of application of intellectual property protections to farm data with thoroughness.¹⁵⁸ Of the various types of intellectual property protections available to owners, only trade secret protection is potentially applicable to farm data. However, classification of farm data as a trade secret is not a certainty, and numerous aspects of the law need to be considered.

The Uniform Trade Secrets Act provides the legal framework for trade secret protection for companies in the majority of the United States.¹⁵⁹ To qualify as a trade secret, three conditions must be met:

1. It must consist of information, including a formula, pattern, compilation, program, device, method, technique, or process;
2. It must derive independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and
3. It must be the subject of efforts that are fair, proper, or moderate under the circumstances to maintain its secrecy.¹⁶⁰

Ellixson, Griffin, Ferrell, and Goeringer do a thorough analysis of a typical farm operation and application to the conditions necessary for trade secret protection.¹⁶¹ They contend that “it is unlikely that many farmers are actively taking the steps that would be necessary to claim trade secret protection for data.”¹⁶² While condition one is likely met, it is less certain regarding condition two and whether or not there is

155. See *supra* Part IV.A.

156. See John Hull, *Protecting Trade Secrets: How Organizations Can Meet the Challenge of Taking “Reasonable Steps”*, WORLD INTELL. PROP. ORG. MAG. (Oct. 2019), https://www.wipo.int/wipo_magazine/en/2019/05/article_0006.html [<https://perma.cc/3JY2-6GGN>].

157. Ellixson et al., *supra* note 20, at 56.

158. See *generally id.*; see Shannon L. Ferrell, *Legal Issues on the Farm Data Frontier, Part I: Managing First-Degree Relationships in Farm Data Transfers*, 21 DRAKE J. AGRIC. L. 13 (2016); Todd Janzen, *Ag Data Ownership*, JANZEN SCHROEDER AGRIC. LAW: JANZEN AG TECH BLOG (June 13, 2017), <https://www.aglaw.us/janzenaglaw/2017/6/12/ag-data-ownership> [<https://perma.cc/AHS7-Z4TD>].

159. Ellixson et al., *supra* note 20, at 56.

160. *Id.* (citing Uniform Trade Secrets Act § 1(4) (UNIF. LAW COMM’N 1985)).

161. See *generally id.*

162. *Id.* at 61.

value to other producers or individuals.¹⁶³ As we learn more about the potential ways this data could be misused or abused by third parties, I contend that condition two is satisfied, particularly regarding third parties that may use the information to drive up prices for inputs, manipulate land rental, or otherwise use the data in a way that provides value to the third party and potentially harms the producer of the data.

As noted by Ellixson and others, whether or not trade secret protections apply hinges in large part on the question of steps to maintain secrecy.¹⁶⁴ Educating farmers on awareness of the value of trade secret protection and the types of steps necessary to obtain it is key should this type of protection be of interest to a producer. If data that is classified as a trade secret is misappropriated or misused, the owner of that data would have the opportunity to seek one of three types of damages.¹⁶⁵ Those types include actual damages (lost profits or additional expenses), reasonable royalties (what a producer would have received if a licensing agreement had been negotiated by the misappropriating party), and unjust enrichment (benefits gained by the misappropriation of data).¹⁶⁶ While trade secret classification of data offers important precedence and protection to producers, the award of monetary damages may not itself truly address the harm caused by the misappropriation and abuse of this data. For example, if increased costs lead to a family farmer going out of business and selling land that has been in the family for generations, monetary damages cannot replace the history, emotional pain to the family, and potential loss of home should the family farm no longer remain in the family. Unlike other businesses that utilize trade secret protection, farming operations often have significant ties to the land itself, emotionally and physically, and control of the land impacts more than just lost profits, but can determine future use of the land, loss of agricultural production, and various environmental impacts as well. Trade secret protection offers a valuable opportunity to a producer to protect misappropriation of agricultural data but may not be applicable in many cases, or this protection may not truly make the producer whole again due to the types of damage actually inflicted.

C. *Contracts and Data Protection*

As noted above in regard to trade secrets, data ownership remains an issue for farmers. While contract use may play into questions of power dynamics, as producers typically have no room to negotiate should they want to use the product in question, opportunities to limit

163. *Id.* at 58 (stating that farm conditions are variable and thus one may not confer value from the data of another).

164. *Id.* at 61.

165. *Id.* at 61–62.

166. *Id.* at 62.

or at least fully disclose how all collected data will be used exist. This is particularly true if farmers want to share data with certain individuals or companies, as there is value that can be realized through outside aggregation and analysis.¹⁶⁷ While most individuals skip reading through terms of service and similar documents when purchasing or downloading various forms of technology (i.e., Facebook, iTunes, Fitbit, a tractor, or even your vehicle), if personal data is being collected, it is extremely important that those provisions be read and understood regarding data access and control. While reading these documents is necessary, understanding the terms and what that means for you and your data is even more important. These are documents produced by, and that generally favor, the technology manufacturers. Not only do they want to maintain as much control as possible, they seek ways to increase the return on their investment of the development of the technology in question. As noted previously, individual ag data may be of use only to the producer who creates that data. But when this data is combined with that of others, the value to third parties increases.¹⁶⁸

The contracts in question, for purchase or use of a product, often detail the types of information being collected, who has access to it, and how it will be used.¹⁶⁹ Contracts provide an opportunity for farmers to negotiate protections for data, but the ability to negotiate with many major manufacturers, input suppliers, and other large companies is often limited.¹⁷⁰ Ellixson and her co-authors note that including data protection provisions in all types of contracts, including farmland lease agreements and nondisclosure agreements, is a way for farmers to protect and maintain control over ag data.¹⁷¹ But opportunities for negotiation remain minimal, and because of the data's complexity and its potential value, it may be difficult for producers to truly understand the terms of these agreements and what value the data can provide.

When it comes to damages for breach of contract, it can be a challenge for farmers to identify and prove damages in a way that will wholly compensate for the breach of contract much like trade secret damages. To establish breach of contract, most jurisdictions require: (1) proof a contract existed; (2) failure of a party to perform as promised within the contract that materially impacted the other party's expectations; and (3) proof of actual damages.¹⁷² Proving damages for a contract breach involving agricultural data may prove the biggest hur-

167. *Id.* at 52

168. *See supra* Part III.A.1.

169. Ellixson et al., *supra* note 20, at 63.

170. *Id.* at 63-64.

171. *Id.* at 63.

172. *See* Jud. Educ. Ctr., *Breach of Contract*, UNIV. N.M., <http://jec.unm.edu/education/online-training/contract-law-tutorial/breach-of-contract> [<https://perma.cc/5JNF-L5UH>].

dle for producers. To prove damages for an ag data contract breach, any claimed losses must be “directly and necessarily incurred by the breach of contract.”¹⁷³ These types of general damages may be difficult to prove given the nature of the agricultural industry and the difficulty in identifying the cause and effect aspect of the breach and related losses. While it may be possible to demonstrate the cost needed to replace land lost due to inappropriate use of agricultural data, proving losses that can be impacted by many factors or have more value than is recognized by objective assessment may be impossible, similar to trade secrets. While special (or consequential) damages allow for losses indirectly caused by the breach, those losses must still be proven with a level of certainty that may not be possible as needed in litigation.¹⁷⁴ Finally, while punitive damages are possible in many contract breach cases, they are rarely awarded.¹⁷⁵ Designed to provide additional punishment to those who “acted willfully, maliciously or fraudulently,” they compensate beyond actual losses.¹⁷⁶ Punitive damages provide a possible way to recover for losses more difficult to prove with actuality, but it is rare to see a case rise to this level. Monetary damages also do not guarantee that lost land, reputation, or other aspects of production can or will ever be recovered by the producer, limiting the effectiveness of this cause of action to make a producer whole.

D. *State Data Privacy Laws*

While federal data protection has typically been organized by type of data and industry, states are now looking at the issue more broadly. California, in particular, has focused on protecting an individual’s “personal data” and limiting how businesses that collect this personal data can use or sell it. While the primary goal of these laws is to give individuals, not businesses, control over personal data, there are similarities to the processes regulated here and the collection and use of agricultural data by the businesses that work with producers.

The California Consumer Privacy Act (“CCPA”)¹⁷⁷ focuses on providing consumers a “right to know” about the personal information businesses collect, providing them the right to opt out of the sharing of that information, and preventing discrimination against consumers for utilizing the rights the CCPA provides them.¹⁷⁸ Businesses are re-

173. See Jud. Educ. Ctr., *Remedies for Breach of Contract*, UNIV. N.M., <http://jec.unm.edu/education/online-training/contract-law-tutorial/remedies-for-breach-of-contract> [<https://perma.cc/Qz8K-HHKL>].

174. See *id.*

175. See *id.*

176. See *id.*

177. Cal. Civil Code § 1798.100, et seq. (2020).

178. *California Consumer Privacy Act (CCPA)*, CALIF. DEP’T JUSTICE, <https://oag.ca.gov/privacy/ccpa> [<https://perma.cc/V5Xt-9RRY>].

quired to provide notice to consumers of their rights related to data and to explain the business's practices related to privacy.¹⁷⁹

In order to overcome some of the issues related to discrimination or pressure to waive CCPA rights, businesses are not allowed to make consumers waive rights and contract clauses that waive CCPA rights are invalid.¹⁸⁰ Personal data control is of major emphasis, with consumers able to request that a business disclose what data it has, its sources of collection, how the data is used, and information sold to third parties (along with the types of third parties information is sold or disclosed to).¹⁸¹ Consumers can restrict use, deletion, or correction of certain types of information as well.¹⁸²

In the 2020 election, California residents approved the California Privacy Rights Act ("CPRA"),¹⁸³ which amends and enhances the CCPA and is similar to the European Union's privacy laws, discussed in Part V.¹⁸⁴ While most aspects of the CPRA are not effective until 2023, key provisions include the establishment of the first privacy protection agency in the United States, with the California Privacy Protection Agency ("CPPA") having administrative authority "to implement and enforce the CCPA, instead of the California Attorney General."¹⁸⁵ In addition, the CPRA added a new category of personal information, called sensitive personal information, provided consumers additional rights, and expanded breach liability for businesses that "fail[] to maintain reasonable security."¹⁸⁶

New York is another state focused on data privacy. It recently enacted the SHIELD Act,¹⁸⁷ effective March 2020, updating "the state data breach notification law" and "impos[ing] cybersecurity requirements on companies that collect or maintain private information of New York residents."¹⁸⁸ The types of information protected by the

179. *Id.*

180. *Id.*

181. *Id.*

182. *Id.*

183. Scott T. Lashway & Brandon P. Reilly, *The California Privacy Rights Act Has Passed: What's in It?*, Manatt Client Alert (Nov. 11, 2020), <https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed> [https://perma.cc/ST52-RP5L].

184. *See id.*; *see also* CPRA vs. CCPA vs. GDPR: How the Difference Impacts Your Data Privacy Operations, WIREWHEEL (2020), <https://wirewheel.io/wp-content/uploads/2020/11/WireWheel-GDPR-vs-CCPA-vs-CPRA-Cheat-Sheet.pdf> [https://perma.cc/K2WY-96Y8].

185. Jerel Pacis Agatep, *The California Privacy Rights Act ("CPRA") Headed to the November 2020 Ballot*, NAT'L L. REV. (June 30, 2020), <https://www.natlawreview.com/article/california-privacy-rights-act-cpra-headed-to-november-2020-ballot> [https://perma.cc/7KLY-8PCK].

186. *Id.*

187. Stop Hacks and Improve Electronic Data Security Act (SHIELD ACT), N.Y. Gen Bus. Law § 899-bb (2020).

188. Mylan Denerstein, Alexander Southwell & Amanda Aycok, *Prepare for NY Data Privacy Law to Catch Up to Calif.*, LAW360 (Jan. 29, 2021, 6:19 PM), <https://www.gibsondunn.com/wp-content/uploads/2021/02/Denerstein-Southwell-Aycok->

SHIELD Act are more limited than those protected by the CCPA, but the reach of the New York law appears broader, extending to any company in any location that collects protected information from even one New York resident.¹⁸⁹ While the New York law does not provide the same scope of protection or control over personal data that the California law currently provides, expectations are that New York's data privacy laws will soon provide a similar level of protection as California's, perhaps in 2022.¹⁹⁰

Other states are considering various laws and regulations tied to data privacy for residents, continuing the trend of patchwork regulations that increase the potential for confusion among consumers and businesses that work across state and country borders.¹⁹¹ As discussed below,¹⁹² this patchwork of regulations may lead to federal action, that could preempt state laws or establish a uniform set of standards.

V. INTERNATIONAL DATA PRIVACY REGULATIONS

While the focus of this Article is on U.S. data privacy protections, the European Union has made huge strides in providing a baseline level of data privacy protection and control over personal information for its residents, serving as a basis for some state law initiatives in the United States. The EU established a fundamental right tied to data privacy, stating that “everyone has the right to the protection of personal data concerning him or her [and] access to data which has been collected concerning him or her, and the right to have it rectified.”¹⁹³ As part of the process to ensure this fundamental right, the EU en-

Prepare-For-NY-Data-Privacy-Law-To-Catch-Up-To-Calif.-Law360-01-29-2021.pdf [https://perma.cc/LDD5-YVH7]; see also, John C. Cleary & Alexander D. Boyd, *New York Amends Data Breach Notification Law and Enacts Data Security Protections*, NAT'L L. REV. (Aug. 7, 2019), https://www.polsinellionprivacy.com/blog-five/2019/8/7/new-york-amends-data-breach-notification-law-and-enacts-data-security-protections [https://perma.cc/GBX4-BEDN].

189. *Id.*

190. *Id.*

191. Gretchen A. Ramos & Darren Abernethy, *Additional U.S. States Advance the State Privacy Legislation Trend in 2020*, NAT'L L. REV. (Jan. 27, 2020), https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020 [https://perma.cc/MX4W-UXET].

192. See *infra* Part VI.A.

193. *Protection of Personal Data: Know Your Rights*, EUR. COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en [https://perma.cc/YW9H-BQUJ].

acted the General Data Protection Regulation (“GDPR”),¹⁹⁴ touted by the EU as “the toughest privacy and security law in the world.”¹⁹⁵

The data privacy and security measures in the GDPR apply to all companies and organizations across the world that collect data from individuals located within the EU.¹⁹⁶ California’s regulations, particularly the recent CPRA, are similar to the GDPR in many ways, including the focus on the individual rights regarding personal data. Personal data in the GDPR “is any information that related to an individual who can be directly or indirectly identified” and includes things like location information, biometric data, and “pseudonymous data . . . if [it is] relatively easy to ID someone from it.”¹⁹⁷ Those required to adhere to the law include not just data controllers (those who “decide[] why and how personal data will be processed”), but also all data processors (“third part[ies] that process[] personal data on behalf of a data controller”).¹⁹⁸ Data processors include companies that provide email services and cloud storage services.¹⁹⁹ The primary goals are to ensure transparency to consumers regarding personal data collection and use, and to return control to the consumer in many ways. The GDPR also puts the onus on data controllers and processors to provide assurances as to data accuracy, privacy, and scope of collection.²⁰⁰ Consumers have the right to restrict use of certain data, object to its use, request erasure or correction, and review the personal data a company collects.²⁰¹ Enforcement and enactment immediately caused concern across the globe, as companies scrambled to understand the impacts and requirements that related to doing business in the EU.²⁰² The EU took a universal approach to data privacy, unlike the current state-by-state, fragmented actions seen in the United States.

The GDPR demonstrates the global scope of data collection and the value that is inherent in having the right to control data collected about the user because that data has value to others. When it comes to agricultural data, the expected impact of the GDPR is limited, likely

194. European Parliament Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) *Official Journal* L119, p. 1.

195. *What Is GDPR, the EU’s New Data Protection Law?*, GDPR.EU, <https://gdpr.eu/what-is-gdpr/> [<https://perma.cc/L8Z3-MTCB>].

196. *Id.*

197. *Id.*

198. *Id.*

199. *Id.*

200. *Id.*

201. *Id.*

202. Michael Nadeau, *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant*, CSO (June 12, 2020), <https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html> [<https://perma.cc/7MJM-UVD8>].

only to pseudonymous data that may contain information that could be used to identify a person.²⁰³ Most agricultural data itself is unlikely to fall under the “personal data” category as it is generated by an entity—a business—and not a natural person.²⁰⁴ While expected impacts are limited, that does not mean no impacts exist, and as collection and use of agricultural data expands across the world and agricultural companies continue to consolidate and globalize, these impacts may help clarify certain privacy and usage issues regarding agricultural data and increase focus on the importance of regulations that have global impact in this area.

VI. PROPOSALS AND RECENT ACTIONS AT THE FEDERAL LEVEL

A. *Considering a Federal Privacy Law*

As individual states and the EU have increased focus on control over personal data and enhancing data privacy laws, there has been limited action at the federal level. In September 2018, the Department of Commerce’s National Telecommunications and Information Administration (“NTIA”) sought public comment “on ways to advance consumer privacy while protecting prosperity and innovation.”²⁰⁵ The request noted concern over the fragmentation of privacy laws on a national and global scale and indicated a desire to alleviate that concern.²⁰⁶ Notably, the request did not call for a statutory standard to be created but instead sought comment on two areas: “(1) A set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and (2) a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections.”²⁰⁷ Specifically, the focus is “on the outcomes of organizational practices, rather than on dictating what those practices should be,” with end goals that lead to increasing transparency, consumer knowledge, and products and services inherently designed to manage privacy risks.²⁰⁸

The NTIA received over 200 comments,²⁰⁹ but as of publication the NTIA and other federal agencies have taken no further action. The NTIA’s 2018 request for comments noted a “parallel effort” at the

203. Marco Brini, *Agri Data Regulation (EU GDPR and US)*, ENVEVE, <https://www.enveve.com/agri-data-regulation-eu-gdpr-and-us/#::~text=despite%20the%20partial%20impact%20of,and%20excerpts%20of%20relevant%20articles> [<https://perma.cc/7WJ4-A7HT>].

204. *Id.*

205. 83 Fed. Reg. 48600 (Sept. 26, 2018).

206. *Id.*

207. *Id.* at 48601.

208. *Id.*

209. Press Release, Nat’l Telecomms. & Info. Admin., NTIA Releases Comments on a Proposed Approach to Protecting Consumer Privacy (Nov. 13, 2018) (available at <https://www.ntia.doc.gov/press-release/2018/ntia-releases-comments-proposed-approach-protecting-consumer-privacy> [<https://perma.cc/6WCV-GA3A>]).

same time by the National Institute of Standards and Technology (“NIST”) to develop “a voluntary privacy framework to help organizations manage risk.”²¹⁰ The NIST released the voluntary framework in early 2020, with a heavy emphasis on protecting data from breaches and other data security protocols.²¹¹

While there is continued discussion at the federal level about data privacy and control over personal information, the focus remains on self-regulation and voluntary protocols or actions by various entities. Like what we see in other federal and state privacy statutes, the focus for this voluntary or self-regulatory protocol remains personal information—that of various individuals and not entity or business-related data, like agricultural data. While keeping privacy issues on the forefront is important, two key issues remain: (1) concerns over agricultural data privacy and use would only be impacted by federal (or state) laws related to personal information on an extremely limited basis, if at all, and (2) voluntary programs fail to ensure that agricultural producers can expect uniform treatment of information across the spectrum of entities they work with or have control over what parties have access to farm data collected on their behalf.

B. *Defend Trade Secrets Act of 2016 (“DTSA”)*

Earlier discussion noted the challenges of applying trade secret protections to agricultural data.²¹² While most trade secret actions fall under state law, the Defend Trade Secrets Act of 2016 established a federal cause of action for trade secret misappropriation lawsuits.²¹³ The DTSA gives agricultural producers an option, one that in some cases may be more farmer-friendly than traditional state trade secret laws. For example, “[t]he DTSA definition appears to incorporate farm data more readily as the trade secret definition explicitly includes ‘intangible’ items, data, as well as techniques and processes which arguably include information such as as-applied fertility or site-specific yield data.”²¹⁴ Other key aspects favorable to farmers include whistleblower protections and broadening potential damages to include the possibility of injunctive relief, which would prevent the person or entity being sued from using the alleged trade secret.²¹⁵

The DTSA is not agricultural industry specific, but by broadening the definitions, allowing for injunctive relief, and establishing a federal

210. Press Release, Nat’l Telecomms. & Info. Admin., NTIA Seeks Comment on New Approach to Consumer Data Privacy (Sept. 28, 2018) (available at <https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy> [<https://perma.cc/L3PN-RYAV>]).

211. *Privacy Framework*, NAT’L INST. STANDARDS & TECH., <https://www.nist.gov/privacy-framework> [<https://perma.cc/9WM2-WBVJ>].

212. *Infra* Part III.B.

213. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

214. Ellixson et al., *supra* note 20, at 65.

215. *Id.*

standard, the potential impacts are high.²¹⁶ While not a perfect or complete response to concerns over use of agricultural data, this expanded protection provides additional support recognizing the value of ag data and dangers that can occur depending on who can acquire it without the farmer's knowledge or approval. Providing an additional remedy to agricultural producers in certain cases is a valuable tool in a limited toolbox.

VII. WEIGHING REGULATORY OPTIONS: PUBLIC VS. PRIVATE, VOLUNTARY VS. MANDATORY

Big data, beyond just agriculture, is in the eye of regulators. With hearings on Capitol Hill regarding Facebook, Google, and a host of other technology companies, there is concern at the state and federal level that goes beyond just data privacy.²¹⁷ As Ellixson and her co-authors noted, "the continuing growth of the debate around the propriety of Big Data applications in many arenas beyond just farm data suggests coming calls for data protections including both business information, including farm data, and personal information."²¹⁸ While those calls are starting to come,²¹⁹ the debate over how to best regulate big data highlights two key areas of debate: (1) private versus public regulation (industry standards versus government regulation)

216. See Ashley Ellixson, *Defend Trade Secrets Act 2016: Can It Help Protect Your Farm Data?*, COLL. AGRIC. & NAT. RES., <https://www.agrisk.umd.edu/post/defend-trade-secrets-act-2016-can-it-help-protect-your-farm-data> (July 9, 2020) [<https://perma.cc/CBN6-TQRC>].

217. See *FTC Hearing #6: Privacy, Big Data, and Competition: Event Description*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-6-competition-consumer-protection-21st-century> [<https://perma.cc/2NG5-TK76>]; *Hearings: Revisiting the Need for Federal Data Privacy Legislation*, U.S. SENATE COMM. COM., SCI., & TRANSP. (Sept. 23, 2020), <https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation> [<https://perma.cc/R4SG-3D68>]; Tony Romm, *Amazon, Apple, Facebook and Google Grilled on Capitol Hill Over Their Market Power*, WASH. POST (July 29, 2020, 5:55 PM), <https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/> [<https://perma.cc/MHJ8-T83U>]; *Senate Commerce Committee Holds Hearing on the Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Dec. 21, 2020), <https://www.huntonprivacyblog.com/2020/12/21/senate-commerce-committee-holds-hearing-on-the-invalidation-of-the-eu-u-s-privacy-shield-and-the-future-of-transatlantic-data-flows/> [<https://perma.cc/H8WM-2ACA>]; Ian Richardson, *Iowa Senate Passes Bill Outlawing Tax Breaks, Contracts for Tech Companies That 'Censor' Speech*, DES MOINES REG. (Mar. 17, 2021, 5:16 PM), <https://www.desmoinesregister.com/story/news/politics/2021/03/17/iowa-senate-passes-ban-tax-breaks-tech-companies-censorship-free-speech-twitter-facebook-amazon/4724692001/> [<https://perma.cc/QN39-QSJ2>]; Hayden Field, *States Have Been Busy With Big Tech Regulations. Here's the Rundown*, EMERGING TECH BREW (Feb. 17, 2021), <https://www.morningbrew.com/emerging-tech/stories/2021/02/17/states-busy-big-tech-regulations-heres-rundown> [<https://perma.cc/2449-E42A>].

218. Ellixson et al., *supra* note 20, at 64.

219. See *supra*, note 217; see also MEGAN STUBBS, *BIG DATA IN U.S. AGRICULTURE*, CONG. RSCH. SERV. (Jan. 6, 2016).

and (2) mandatory versus voluntary standards (legally enforceable versus optional methods of risk management or good practices). Current practices related to ag data privacy generally fall under the private, voluntary regulatory categories, and for the reasons discussed below, fail to sufficiently address the concerns of agricultural producers. Those issues were highlighted in a 2016 American Farm Bureau Federation study that highlighted three main areas of concern for farmers: lack of trust, loss of control, and complexity of agreements.²²⁰ The percent of farmers with these concerns was high. For example, over 60% of farmers “expressed worry that [Agriculture Technology Providers (“ATP”)] could use data to influence market decisions,” over 65% “believe[d] farmers should share in the potential financial benefits from the use of their data beyond the direct value they may realize on their farm,” more than 75% of respondents “expressed concern about which entities can access their farm data,” and almost 60% of producers “were confused about whether current legal agreements allowed ATPs to use their ag data to market other services . . . back to them.”²²¹ Industry, recognizing that this level of producer concern is problematic, has attempted to self-regulate to address particular items, as discussed below.

A. *Industry Example: Farm Bureau’s Privacy and Security Principles for Farm Data*

The AFBF developed its Privacy and Security Principles for Farm Data in 2014.²²² Described as “the most active initiative so far” regarding ag data privacy in the United States,²²³ thirty-nine organizations from a broad array of the industry signed on to the principles as of 2016.²²⁴ According to AFBF, “it is imperative that an ATP’s principles, policies[,] and practices be consistent with each company’s contracts with farmers.”²²⁵ The Principles focus on a variety of areas:

220. *The Future of Farming: Technological Innovations, Opportunities, and Challenges for Producers: Hearing Before the Subcomm. on Gen. Farm Commodities & Risk Mgmt. of the Comm. on Agric.*, 115th Cong. 21 (2017) (prepared statement of Todd J. Janzen, President, Janzen Agricultural Law LLC) (noting that “[a] farmer seeking to compare two similar products today might find that they are governed by two very different sets of contracts.”).

221. *Id.* at 20–21.

222. Agri-Pulse Staff, *Farm Groups and Ag Tech Companies Outline Data Privacy Protocols*, AGRI-PULSE (Nov. 13, 2014, 3:29 PM), <https://www.agri-pulse.com/articles/4599-farm-groups-and-ag-tech-companies-outline-data-privacy-protocols> [<https://perma.cc/NWV4-SXYW>].

223. Brini, *supra* note 203.

224. *Privacy and Security Principles for Farm Data*, AM. FARM BUREAU FED’N, <https://www.fb.org/issues/innovation/data-privacy/privacy-and-security-principles-for-farm-data> [<https://perma.cc/9JJP-JA4V>].

225. *Id.*

education, ownership, notice, choice, disclosure, portability, transparency, and security.²²⁶

There is no doubt the topics covered by AFBF's Principles are some of the most concerning when it comes to agricultural data. At first glance, the Principles appear to address many concerns. For example, the Principles state, "farmers must be notified that their data is being collected and about how the farm data will be disclosed and used."²²⁷ Notification is vital to ag producers understanding how data is collected by a variety of methods, some of which may not necessarily be readily apparent or known. Similarly, the Principles clearly state that transparency is important and that certain terms, such as farm data and those relating to third parties, should be clearly defined and that "farmers should know with whom they are contracting if the ATP contract involves sharing with third parties, partners, . . . or affiliates."²²⁸ The Principles by and large are not objectionable in terms of the articulated goals and standards. However, even if every ATP in the United States adopted the Principles, significant challenges for producers remain.

Importantly, there is no penalty if a company fails to adhere to the Principles. The program is purely voluntary, and while some bad publicity might deter some companies from taking steps that violate or are not in line with the AFBF Principles, the likelihood of that publicity having any significant impact is low. First, it would be difficult, if not impossible, for most producers to even determine that a company violated a Principle or changed contract terms from one year or product to the next. Even if a producer were to read through what is typically an extensive contract with an ATP one time, it is unlikely to thoroughly do so for every agreement with that company based on the time required, terminology used, and related issues.²²⁹ Nor is a producer generally able to track what happens with his or her data once the ATP obtains it, to determine if terms are being adhered to as described.

The Principles also fail to address concerns over how data could be used in ways that would harm a producer. While the ATP may truthfully disclose the third parties that will be able to purchase or have access to the producer's data, there is no certainty that the third party will use the data in a way that would not cause harm. Even if a producer were to want to track down all its data and determine all ATPs and third parties that have access to it, the technical expertise and time required to do so in a way that would allow a producer to understand how the data is being used would be beyond the capacity of most producers.

226. *Id.*

227. *Id.*

228. *Id.*

229. See generally *Ag Data Transparent*, *supra* note 15.

There is also nothing in the Principles that reduces the impact or concerns tied to power dynamics, as discussed previously. While the Principles state that “ATPs should explain the effects and abilities of a farmer’s decision to opt in, opt out[,] or disable the availability of services and features offered by the ATP,”²³⁰ this does nothing to alleviate the lack of negotiation power or potential other options to obtain services if they were to not agree or opt out. If a producer wants a certain product, he or she is bound by the terms of the contract offered. If the producer does not like how information is shared with third parties or that information may be sold, he or she cannot strike that portion of a contract and expect to be able to have access to the ATP’s technology or product. Even if the Principles were adopted and contracts were written in plain English and in half the typical number of pages, and producers were able to understand exactly why the ATP collects its data, to whom it sells it or gives access to the data, and provides access to the basic farm data should a producer end a contract, none of that does anything to prevent data from being used in a way that could harm the producer nor provides any ability for a producer to limit how even a third party, let alone the ATP, might use data. While producers can “opt out or have their data removed prior to . . . sale” to a third party, the pressure to consent in order to obtain services, maintain a relationship with the ATP for other purposes, and improve management practices are all high.

Finally, while the Principles state that “[i]t is imperative that an ATP’s principles, policies[,] and practices be consistent each company’s contracts with farmers,” the differences between contracts and providers may still be stark.²³¹ There is no standardization of terms so that farmers know from one contract to the next that terminology and definitions remain the same. There is no expectation that competitors will define terms similarly such that producers can more easily understand and compare products and opportunities. While the Principles are clearly aimed at easing the concerns identified by producers related to ag data and technology agreements, they do not bind companies in any way that would actually provide any real reassurance to farmers. The Ag Data Transparent Project, discussed in the next section, attempts to address some of these concerns, but does not create

230. *Privacy and Security Principles for Farm Data*, *supra* note 224.

231. See Nathan DeLay, Nathanael Thompson & James Mintert, *Farm Data Usage in Commercial Agriculture*, PURDUE UNIV. CTR. COM. AGRIC. (Jan. 23, 2020), <https://ag.purdue.edu/commercialag/home/resource/2020/01/farm-data-usage-in-commercial-agriculture/> [<https://perma.cc/E7DN-VVQ7>] (stating that “70% of software users subscribe to more than one product”); *The Future of Farming: Technological Innovations, Opportunities, and Challenges for Producers: Hearing Before the Subcomm. on Gen. Farm Commodities & Risk Mgmt. of the Comm. on Agric.*, 115th Cong. 21 (2017) (prepared statement of Todd J. Janzen, President, Janzen Agricultural Law LLC) (noting that “[a] farmer seeking to compare two similar products today might find that they are governed by two very different sets of contracts.”).

one, set standard of terms, definitions, and requirements for privacy and use of data that would eliminate many of the key issues.

B. *Industry Example: Ag Data Transparent Project*

Third-party certification symbols are everywhere we look, from our food (Non-GMO Project and its butterfly logo²³²) to our clothes (organic), and even certifications that cross industries (Certified B Corp²³³). There is even a third-party certification program for agricultural data agreements, the Ag Data Transparent Project.²³⁴ This project was meant to take AFBF's Principles to the next step: "make sure that ATPs that say they follow the Data Principles *actually do just that*."²³⁵ Ag Data Transparent was established as an independent third party to evaluate an ATP's contracts and policies and determine whether the ATP is transparent and actually abiding by the Principles in its agreements with producers.²³⁶ If found transparent, the ATP "receives a license to use the 'Ag Data Transparent' seal on its marketing materials."²³⁷ On the other hand, if the evaluation identifies concerns and inaccuracies in how the ATP answered the questions regarding its agreements, the ATP is not awarded the license and has the opportunity to revise policies and contracts to meet the Principles.²³⁸

Third-party certification does, in my mind, relieve some of the opportunity an organization has to support and sign on to programs such as AFBF's Principles, but then takes no significant steps to implement the policies in a way that favors the intended audience. In those cases, there is more image maintained by being seen as a signatory and concerned about customers than actual substance in terms of change. The use of third-party certifications and evaluations ensures at least some level of adherence to a minimum set of standards. Third-party certification is more valuable when the qualifying data and evaluation questions are transparent and made public, and that is something that the Ag Data Transparent project does through its website. The evaluations of all twenty-six companies that currently have the license to use the Ag Data Transparent seal are available on the ADT website,

232. *Inside the Making of the Non-GMO Project Logo*, NON-GMO PROJECT (Dec. 4, 2013), <https://www.nongmoproject.org/blog/ddwngplojo/> [<https://perma.cc/V248-XGLB>].

233. *About B Corps*, CERTIFIED B CORP., <https://bcorporation.net/about-b-corps> [<https://perma.cc/ZA7F-7GU2>].

234. *See What Does It Mean To Be Ag Data Transparent*, AG DATA TRANSPARENT, <https://www.agdatatransparent.com/about> [<https://perma.cc/2KMV-YEYC>].

235. Todd Janzen, *Bringing Transparency to Ag Data Contracts*, DIRT (June 27, 2016), <https://dirtforfarmers.com/bringing-transparency-to-ag-data-59673abf961a> [<https://perma.cc/89XG-2WDD>] (emphasis in original).

236. *Id.*

237. *Id.*

238. *Id.*

meaning anyone can see a certified ATP's answers to the evaluation questions.²³⁹ The ATP's contracts and documents used to evaluate the accuracy of those answers, though, are not generally publicly available, meaning the ability to determine the accuracy is limited for non-customers.

Around twenty-five companies are currently licensed to use the ADT seal.²⁴⁰ While the ADT seal does provide assurances to producers that an ATP is implementing the Principles into its agreements, the program does not address the issues and concerns noted about the Principles themselves above. While many of the biggest names in U.S. ag technology are part of ADT, these companies are only a handful of the many that producers work with around the globe. One annual ranking of ag technology companies identifies just a "Top 50" each year of "leading . . . companies exemplifying the best in agriculture technology around the globe,"²⁴¹ while a search for "monitoring and growing" industry companies and "precision farming" companies on the *AgriTech Tomorrow* listing service listed 116 and 50 companies, respectively.²⁴² The number of ag tech companies continues to grow quickly, with 2018 and 2019 seeing investments of "\$4 billion in startups in the agtech space" each year, and expectations were that 2020 would meet or exceed that number.²⁴³ While the number of companies that are *not* part of ADT is unknown, the number is certainly high and likely growing.

As an industry-funded initiative, ADT makes progress towards ensuring transparency in ATP contracts and in developing more understandable agreements and terms. However, substantive issues, such as negotiating power, perceived pressure, or need to consent, and power dynamics are not addressed by a program such as this. It is also possible that producers may rely upon this third-party certification as some sort of endorsement of these companies or agreements, and not thoroughly read, research, or understand the agreements, not realizing that the industry itself developed and formed ADT and the Principles

239. *Ag Data Transparent Certified Companies*, AG DATA TRANSPARENT, <https://www.agdatatransparent.com/certified> [https://perma.cc/L3HL-SDEP].

240. AG DATA TRANSPARENT, <https://www.agdatatransparent.com> [https://perma.cc/7RNF-H8UV].

241. Matt Hopkins, *Annual Ranking of Agricultural Technology Companies Released*, PRECISIONAG (Jan. 30, 2018), <https://www.precisionag.com/digital-farming/analytics/annual-ranking-of-agricultural-technology-companies-released/> [https://perma.cc/FP2B-VRD4].

242. *See Company Directory: Results*, AGRITECH TOMORROW, https://www.agritechtomorrow.com/company_directory_search.php?company=industry=2®ion=§or=&keyword=&Search=active&search=search#results [https://perma.cc/7C7M-6TV9].

243. Christine Hall, *Agtech Sector Blooms as More Dollars and Startups Rush In*, CRUNCHBASE NEWS (Aug. 20, 2020), <https://news.crunchbase.com/news/agtech-sector-blooms-as-more-dollars-and-startups-rush-in/> [https://perma.cc/348K-NMDE].

which ADT evaluates.²⁴⁴ That, perhaps false, sense of security may actually lead to less personal responsibility and evaluation of contracts, despite the Principle's focus on grower education "to create educated customers who understand their rights and responsibilities."²⁴⁵

C. *Federal Proposal: Agriculture Data Act of 2018*

The federal government is one of the largest entities gathering ag data in the United States and has been a major source of highly utilized and respected public data for many years.²⁴⁶ However, much of that data is scattered among many of the USDA's agencies, and coordination collaboration that brings all of this data together for evaluation rarely occurs.²⁴⁷ The Agriculture Data Act of 2018²⁴⁸ was proposed to "strengthen the USDA's management of producer data so that it can be used to study the impacts of farm conservation practices . . . while protecting the privacy of farmers."²⁴⁹ Under the proposed legislation, the USDA would create a secure data warehouse to collect and aggregate agricultural data, improve procedures for greater data interoperability, and create opportunities for producers to voluntarily elect to participate in additional research and data-generation activities.²⁵⁰ In addition, it would have enacted strong safeguards prohibiting the sale of data and requiring published research to release only aggregated data to provide anonymity to individual farmers.²⁵¹

The bill itself never made it out of Committee,²⁵² but the scope of this legislation and the resulting regulations, had it passed, may have set baseline standards, definitions, and practices at a federal level that ideally trickled down into use by all ATPs. Extremely intriguing was the focus on the use of producer data for public good and use, for research, and to address concerns such as increasing effectiveness of conservation and risk management (crop insurance) programs. This recognition of how valuable this type of information is—particularly in the public sector for research—demonstrates the need to consider public access of data as a necessity of any sort of ag data regulation. Because the legislation did not progress, we are left with a lot of ques-

244. *What Does It Mean To Be Ag Data Transparent*, *supra* note 234.

245. *Privacy and Security Principles for Farm Data*, *supra* note 224.

246. See generally *FAQ: The Agriculture Data Act of 2018 and Producer Privacy*, AGREE, <https://www.edf.org/sites/default/files/content/FAQ-Ag-Data%20Act-and-Producer-Privacy.pdf> [<https://perma.cc/HFW2-LV63>].

247. See generally Laurie Bedord, *Coalition Urges Support of Agriculture Data Act of 2018*, SUCCESSFUL FARMING (Apr. 12, 2018), <https://www.agriculture.com/news/technology/coalition-urges-support-of-agriculture-data-act-of-2018> [<https://perma.cc/8LB5-ACEQ>].

248. Agriculture Data Act of 2018, S. 2487, 115th Cong. (2018).

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

tions about how this would have been implemented: how would producer data be collected, would ATPs from the private sector be involved, would data collection through technology be mandatory for those participating in USDA programs at some point, and what limits would be set on access and use of the data? Working to demonstrate or improve efficiency of USDA programs is exactly what should be done with this type of data, an evaluation and research that was not possible at this scale or level just a few years ago. Whether or not this would work on a voluntary basis is uncertain—producers would likely be wary of providing a lot of this data to the government for fear of potential enforcement actions by the government or use in private litigation. The proposal appears to address some of those concerns in the text, but those questions would need to be specifically addressed should we see this type of legislation be successful in the future or if the USDA was to develop a voluntary program of data collection for internal and external use.

D. *Identifying Priorities: Political, Environmental, Social, and Economic Debates*

As we think about how to protect producers from misuse or abuse of agricultural data, questions arise as to what the priorities should be when it comes to collection and use of this type of information. This is complicated as we consider more general goals such as encouraging entrepreneurship and innovation in business, developing infrastructure and access to high-speed data sources, competition among agricultural industry participants (including producers), and economic costs associated with development and adoption of new technologies. As we recognize that “many farmers [across the world] do not benefit from this sharing and exchange of agricultural data” how do we balance protection with innovation, entrepreneurship with privacy, contracts with legal limitations, and all the other unique aspects that come from balancing the government’s interests in agriculture, food production, the environment, privacy, economic success, competition, and data, just to name a few, and do so while recognizing that all of this has an impact on the local, state, federal and global levels?

As noted above, voluntary actions like AFBF’s Principles and the Ag Data Transparent project, in addition to those elsewhere such as the “New Zealand Farm Data Code of Practice”²⁵³ and the “EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement”²⁵⁴ provide a good start in addressing some concerns. However, the reliance on self-regulation poses challenges to providing the neces-

253. NEW ZEALAND FARM DATA CODE OF PRACTICE, <https://www.farmdatacode.org.nz> [<https://perma.cc/LQ8G-DX2G>].

254. *EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement*, FOOD & AGRIC. ORG. UNITED NATIONS, <http://www.fao.org/family-farming/detail/en/c/1370911/> [<https://perma.cc/87GH-8VPT>].

sary assurances to producers that these companies will actually keep the producer interests up front and protected while also continuing to focus on profit-building and expanding company scope. These voluntary codes also do not address the inequalities in the industry that limit access to technology, use of data, wide power discrepancies, and other economic and social concerns.

The World Bank noted that an additional concern of the voluntary codes is the primary target audience are not “farmers or Farmers’ Organizations (let alone smallholder farmers) . . . but rather the agribusiness and ag tech companies that work with farmers and use their data.”²⁵⁵ This means that it may not necessarily be the interests of farmers that are truly the focus here, but instead companies understanding that they need to at least appear to recognize and address farmer concerns in order to continue to have increased access to data that companies in turn can monetize in a variety of ways. Access to data is of primary concern, not producer privacy, equity, or other public benefits.

The public benefits of access to ag data should be a high priority as data privacy is considered. Members of Congress recognized this in their support of the Agriculture Data Act of 2018 as discussed above,²⁵⁶ when focusing on using data to improve efficacy of environmental and other government programs, and the value of providing public researchers access to anonymized data.

Those same goals, in addition to focusing on improving opportunities for smallholder farmers in developing nations, are seen on a global scale in CGIAR’s Platform for Big Data in Agriculture.²⁵⁷ CGIAR is focused on developing a data platform: “a multi-sided, technology-enabled network that facilitates the interaction of stakeholders.”²⁵⁸ Focused on a series of communities of practice, the platform works to “foster collaboration spaces and opportunities, facilitate connectivity and sharing of methodologies, and support the organization of capacity-building workshops.”²⁵⁹ The platform’s goals include reducing hunger, improving sustainable practices, closing yield gaps, and encouraging agricultural development as addressed by collaboration and the sharing of research, data, and information across the platform. The Bill & Melinda Gates Foundation is also investing in digital technology to support global initiatives and smallholder farm-

255. Foteini Zampati, *Does Data Mean Power for Smallholder Farmers?*, WORLD BANK BLOGS (Sept. 26, 2019), <https://blogs.worldbank.org/opendata/does-data-mean-power-smallholder-farmers> [<https://perma.cc/TX2Y-LLFQ>].

256. *See supra*, Part VII.C.

257. *About the Platform*, CGIAR, <https://bigdata.cgiar.org/about-the-platform/> [<https://perma.cc/5VQQ-28S3>].

258. *Annual Report 2019*, CGIAR, <https://bigdata.cgiar.org/annual-report-2019/> [<https://perma.cc/6U2R-34FW>].

259. *Convene*, CGIAR, <https://bigdata.cgiar.org/convene/> [<https://perma.cc/Q6YU-GJ7T>].

ers, setting a goal to ensure that over the next “[ten] years, at least half [] of the smallholder farmers in [its] focus geographies are benefitting from digitally enabled services.”²⁶⁰ The Gates Foundation investments focus on helping advance “cost-effective technologies and business models and support[ing] scaled platforms that harness the interests of the public sector, private sector, and smallholder farming communities.”²⁶¹

Finding some sort of balance between public and private sectors, global and local farmers, and smallholder versus large scale producers is not an easy task for any government, let alone here in the United States where large-scale agriculture has become a driving force influencing agricultural policy and priorities. For any potential movement in the area of agricultural data use and regulation to have meaningful impact, there needs to be involvement of all aspects of the industry in these discussions and priority-setting meetings. This involvement must also put everyone on equal footing, removing some of the power dynamics and competition concerns that exist in the industry and providing all involved an equal voice. Without that, there is the potential that key benefits to the public and smaller producers will get lost in the push forward to continue the digital transformation, widening the data gap and perhaps increasing the potential negative uses of agricultural data collection and sales to third parties.

As we think about the potential benefits in the public sector for this data, ensuring equity, fairness, access, and use—individually and collaboratively—becomes a question of ethics as well. This is where our focus on setting priorities should begin, considering the ethical aspects of our global food system and how to use this information to meet development, economic, and sustainability needs to better prepare our world for the future. The ethical concerns also tie into the broader producer concerns regarding trust, consent, and data use.²⁶²

Building databases consisting of “externalities and vulnerabilities” of environmental and health concerns tied to issues like monoculture, pesticides (such as neonicotinoids), and biodiversity “would be of the upmost ethical and practical importance for research on the best agricultural model for the future of global food production.”²⁶³ As we consider the ethical and moral implications of maintaining the land, soil, and technology to feed a growing global population, we cannot overlook the significant impacts that technology could have, not just in increasing yield and efficiencies in production, but in reducing the

260. *InfoAg 2019 Presentation: Last Mile Digital Services for Smallholder Farmers*, INFO AG, <https://www.infoag.org/Program/Speakers/Presentation/?id=1607> [<https://perma.cc/2Q6B-NVG4>] (providing presentation information from speaker Stewart Collis of the Gates Foundation).

261. *Id.*

262. See Zampati, *supra* note 12.

263. Isabelle M. Carbonell, *The Ethics of Big Data in Big Agriculture*, 5 INTERNET POLICY REV. 1, 3 (2016).

environmental footprint. It is easy to imagine the tension between the competing priorities briefly discussed here and those left yet unwritten. As we consider possible next steps and solutions, my belief is that focusing more on the ethical and moral considerations, particularly those of the general population and producers, should be of utmost importance.

E. *Next Steps: Potential Options*

Suggestions for areas of focus moving forward involve both long-term and short-term initiatives. There is no easy answer, nor even just one solution, to addressing challenges of the use and collection of agricultural data. Aspects of the following proposals, if adopted and developed in part or whole, could help the industry and country move toward a stronger level of equality in the process.

1. Enact Legislation Similar to the Agriculture Data Act of 2018

While the 2018 legislation failed to move out of the Senate Agricultural Committee, it did receive support from a variety of bipartisan agricultural interests.²⁶⁴ Enacting legislation similar to this 2018 proposal would have significant impacts on establishing federal standards for a variety of the issues discussed here. Establishing baseline definitions for essential terms, recognized standards for security and data privacy, regulations related to third party use of data for public research, anonymization, and access, as well as demonstrating a commitment to increasing the effectiveness and evaluation of government programs, would all have a significant impact looking to the future.²⁶⁵ Passage of this legislation also has potential to support other initiatives discussed below, including increased producer education, access to technology, and further development of infrastructure in this area. While certain aspects of the 2018 bill were included in the 2018 Farm Bill,²⁶⁶ the Farm Bill's language was not a mandate for the USDA to act to collect data, provide data collection tools to farmers, and make data available for public research.²⁶⁷ The directives of developing a report looking at these issues does make the USDA take the step of evaluating the vast amount of data it collects across its agencies and divisions, and ideally evaluate steps taken to protect that data and the understanding that producers have as to how data is used. However, it is going to take some sort of official Congressional action for true change to occur and to get the USDA on track to be a leader in setting

264. Bedord, *supra* note 245.

265. Agriculture Data Act of 2018, S. 2487, 115th Cong. (2018).

266. Agriculture Improvement Act of 2018, H.R. 2, 115th Cong. (2018).

267. Todd Janzen, *The Ag Data Act of 2018 in the Next Farm Bill*, JANZEN AG L.: JANZEN AG TECH BLOG (Dec. 13, 2018), <https://www.aglaw.us/janzenaglaw/2018/12/12/ag-data-act-slips-into-the-2018-farm-bill> [https://perma.cc/49J3-B8QL].

the standard for agricultural data collection, use, privacy, and public research.

2. Expand Access to Open Data

An entity not yet discussed in this Article and yet extremely relevant and valuable to its focus is the Global Open Data for Agriculture & Nutrition (“GODAN”) initiative.²⁶⁸ GODAN contends that “data is knowledge and knowledge is power” and that “[i]f data allows for the collation of information and knowledge, then open data has the potential to make this knowledge available to everyone, everywhere, at any given time.”²⁶⁹ Through the use of reasonably priced, accessible licenses, GODAN strives to make data easily accessible and usable across the spectrum of agricultural and nutrition interests.²⁷⁰ With almost 1,200 partners across the world, GODAN wants to use this data to “encourage collaboration and cooperation across existing agriculture, nutrition and open data activities and stakeholders to solve long-standing global problems.”²⁷¹ The U.S. government, along with the United Kingdom, India, Germany, the United Nations, and other entities, helps support GODAN financially.²⁷² In fact, the USDA sits on the GODAN steering committee.²⁷³

A quick review of U.S.-based partners demonstrates that few of the major agribusiness and food companies are GODAN partners.²⁷⁴ While there are some well-known exceptions, such as Kellogg’s, University of Arizona, the Gates Foundation, and Michigan State University, as well as internationally based companies such as Nestle and Syngenta, the majority of the U.S.-based partners are not household names or well-known agribusiness institutions.²⁷⁵ Imagine the work that could be done if the agribusiness giants across the globe, let alone here in the United States, became actively involved in GODAN. The externality and vulnerabilities databases discussed above could be developed in a way that would allow for significant and immediate impact on human and environmental health.²⁷⁶

268. GLOB. OPEN DATA AGRIC. & NUTRITION, <https://www.godan.info/> [<https://perma.cc/NBQ4-DG5W>].

269. *What Is Open Data?*, GLOB. OPEN DATA AGRIC. & NUTRITION, <https://www.godan.info/pages/about-open-data> [<https://perma.cc/2YAM-WQQ9>].

270. *Id.*

271. *Our Partners*, GLOB. OPEN DATA AGRIC. & NUTRITION, <https://www.godan.info/pages/partnership> [<https://perma.cc/PFA8-CJD4>].

272. *Id.*

273. *Id.*

274. *Id.*

275. *Id.*

276. *See supra*, Part VII.D. *See also* Sjaak Wolfert et al., *Big Data in Smart Farming – A Review*, 153 AGRIC. SYS. 69, 76 (May 2017) (noting that “[p]ublic institutions like the USDA . . . want to harness the power of agricultural data points created by connected farming equipment, drones, and even satellites to enable precision agriculture for policy objectives like food security and sustainability”).

One of the biggest challenges to encouraging agribusiness companies to share more data to open access systems like GODAN is overcoming the need to monetize the data collected. Overcoming the need to consider profits and recovering investment costs is not necessarily something that can be addressed through legislation. While the USDA and the government should encourage broad and active participation in GODAN across the agricultural and food industries, success in ensuring data is shared by these companies in a way that may not necessarily meet their interests or bottom line is likely going to need to happen due to consumer and industry pressure. Consumer demand can make significant changes in the agricultural and food sectors, as demonstrated by the new federal bioengineered food label²⁷⁷ and California's recent referendums focused on animal welfare.²⁷⁸ Perhaps more significant impact can happen through supply-chain pressure from those within the food industry that participate in GODAN and want to increase transparency to consumers from field to fork. Supply-chain pressure to share data through open exchanges such as GODAN is likely one of the most efficient and effective ways to increase participation across the U.S. agribusiness industry. The growing globalization of the industry, increased demand for transparency by consumers, and increased regulations on environmental and sustainability concerns all create pressure points that could make GODAN an even more valuable initiative.

3. Address Agricultural and Food Industry Consolidation

As we consider the challenges of power dynamics within the agricultural industry and concerns over technology agreements, informed consent, and disclosure, some of those concerns must be considered in the light of competition. Antitrust, competition issues, and concerns about corporate control are often discussed but not easily addressed.²⁷⁹

277. See generally National Bioengineered Food Disclosure Standard, 7 C.F.R. § 66 (2018); GENEVIEVE K. CROFT, THE NATIONAL BIOENGINEERED FOOD DISCLOSURE STANDARD: OVERVIEW AND SELECT CONSIDERATIONS (Feb. 7, 2020), <https://crsreports.congress.gov/product/pdf/R/R46183> [<https://perma.cc/8F3X-P4J3>].

278. See generally *U.S. Appeals Court Rejects Injunction Against California's 'Cage-free' Prop 12*, FERN'S AG INSIDER (Oct. 15, 2020), https://thefern.org/ag_insider/u-s-appeals-court-rejects-injunction-against-californias-cage-free-prop-12/ [<https://perma.cc/4ACE-PH3S>]; *Proposition 2*, INST. GOVERNMENTAL STUD., <https://www.igs.berkeley.edu/library/elections/proposition-2> [<https://perma.cc/8VAF-VUZQ>].

279. See generally *The Time Is Ripe for Competition and Antitrust Reform in Agriculture*, NAT'L SUSTAINABLE AGRIC. COAL.'S BLOG (Feb. 12, 2021), <https://sustainableagriculture.net/blog/the-time-is-ripe-for-competition-and-antitrust-reform-in-agriculture/> [<https://perma.cc/Y7JT-LZZA>]; *Antitrust and Competition in American Agriculture*, YALE L. SCH. (Sept. 30, 2020), <https://law.yale.edu/yls-today/news/antitrust-and-competition-american-agriculture> [<https://perma.cc/3MR3-KPLQ>]; Hannah Kass, Opinion, *Breaking Up Big Ag Requires Reasonable Antitrust Enforcement*, REGUL. REV. (Dec. 26, 2019), <https://www.theregreview.org/2019/12/26/kass-breaking-up-big-ag-antitrust-enforcement/> [<https://perma.cc/3T3Z-VQA4>]; *How Corporate*

While the focus of this paper is not consolidation or antitrust, concerns about power dynamics, pressure to sign disclosure agreements, ability to negotiate, and alternative service provider options cannot be truly addressed without consideration as to the impacts of consolidation and competition within the industry as a whole, but also in particular segments across the country. The new administration in 2021 is reinvigorating aspects of the industry focused on these concerns,²⁸⁰ but history indicates many challenges and limited chances of (1) passage and (2) significant success or impact.²⁸¹ Even with many of the other steps suggested within this Article, the significant disparities in power dynamics between producers and agribusiness will continue to cause producers to engage in transactions and agreements with significant benefit to the companies and limited ability for producers to provide input, change terms, or find other service providers.

4. Reinforce Producer Education and Understanding of Responsibilities

It cannot be overlooked or understated that despite the need to address agricultural data privacy and use concerns, agricultural producers have a responsibility to review and understand the terms of the agreements they enter with technology service providers. Due to the complexity of these agreements, this is not always an easy task, but failure to review or understand does not provide any level of protection to a producer should issues arise. AFBF's Principles and other initiatives all include a focus on producer education and simplification of terms and contracts. These initiatives should be of primary importance and all producers should understand the responsibilities that are

Control Squeezes Out Small Farms, PEW (July 18, 2012), <https://www.pewtrusts.org/en/research-and-analysis/fact-sheets/2012/07/18/how-corporate-control-squeezes-out-small-farms> [https://perma.cc/TK2A-VNVB].

280. See *The Time is Ripe for Competition and Antitrust Reform in Agriculture*, NAT'L SUSTAINABLE AGRIC. COAL.'S BLOG (Feb. 12, 2021) <https://sustainableagriculture.net/blog/the-time-is-ripe-for-competition-and-antitrust-reform-in-agriculture/> [https://perma.cc/Q4Z5-5LHP]; Bryce Oates, *Lawmakers Take Aim at Antitrust and Lack of Competition in Ag Markets*, HOPTOWN CHRON. (Feb. 11, 2021, 10:58 AM), <https://hoptownchronicle.org/lawmakers-take-aim-at-antitrust-and-lack-of-competition-in-ag-markets/> [https://perma.cc/C85V-LJ48].

281. Food and Agribusiness Merger Moratorium and Antitrust Review Act of 2019, S. 1596, 116th Cong. (2019) (introduced by Senator Cory Booker and Senator Jon Tester seeking "to impose a moratorium on large agribusiness, food and beverage manufacturing, and grocery retail mergers, and to establish a commission to review large . . . mergers, concentration, and market power"); Press Release, Cory Booker, Senator, Booker, Tester Reintroduce Bill to Halt Ag Mergers Immediately, Indefinitely (May 22, 2019), <https://www.booker.senate.gov/news/press/booker-tester-reintroduce-bill-to-halt-ag-mergers-immediately-indefinitely> [https://perma.cc/4KM4-Y6RD]; *Crisis on the Farm: The State of Competition and Prospects for Sustainability in the Northeast Dairy Industry: Hearing Before the Comm. on the Judiciary*, 111th Cong. (2009); *Ensuring Competitive and Open Agricultural Markets: Are Meat Packers Abusing Market Power?: Hearing Before the Comm. on the Judiciary*, 107th Cong. (2002).

inherent with signing any legal document, including technology agreements and contracts. Resources to help understand the agreements should continue to be readily available, particularly from independent sources to help producers understand and evaluate options without undue pressure. Standardization of certain terms and provisions through federal action would also help increase producer understanding of the agreements. Further, it is of utmost importance that producers are made aware and understand what is *not* included in the agreement or contract, particularly when tied to third parties. Disclosure agreements can and should be clearly written with as much detail as possible, and producers should understand what they are signing, even if they at times believe they have no option other than to sign. As technology adoption continues to grow and the types of technology continue to increase, the need for education is also going to grow. New technologies will require new explanations and producer information must be expressed in a way so it is understood by all—not just those with higher levels of education. While the goal is to protect producer agricultural data from misuse and abuse, producers have a role in protecting their own rights and data that needs to continuously be reinforced.

5. Expanding Trade Secret Law to Specifically Include Agricultural Data and Business Operations

While the Defend Trade Secrets Act of 2016 opened up a potential new avenue for agricultural producers in the area of trade secret protection,²⁸² Congress should consider a specific law to recognize agricultural data as a protected category of information under trade secret law. While trade secret protection requires that steps be taken to keep information secret,²⁸³ specific language could be included that establishes exceptions for companies that collect data on behalf of a producer and for traditional agricultural business practices that involve sharing information between a producer and a service provider. The exceptions would essentially recognize the service provider or company as an extension of the agricultural producer and establish minimum requirements for data storage, security, and privacy, similar to the typical requirement to take steps to keep the information private. In addition, limits on the types of data that could be potentially sold to third parties and an anonymization requirement may help mitigate service providers' concerns about profitability and yet maintain the limited knowledge aspects of trade secret law. This type of trade secret expansion could be done at the state and/or federal level, but

282. *See supra*, Part VI.B.

283. SHANNON L. FERRELL & TERRY W. GRIFFIN, MANAGING FARM RISK USING BIG DATA 35–43, <http://agecon.okstate.edu/farndata/files/Chapter%20%20-%20How%20does%20the%20law%20view%20agricultural%20data%20.pdf> [https://perma.cc/6X3M-F8B4].

might be an option for the government to address some producer protections and privacy concerns without taking steps toward higher levels of regulatory oversight.

6. Public Support to Increase Technology Infrastructure and Access

To address disparities in technology access and concerns over costs of adoption, public support from the USDA and other government entities is necessary. This public support will not only help reduce the digital divide, but also provide opportunities for increased access to public and open data. Support is needed not just in access to the actual technology itself, but to the infrastructure that makes it useful and accessible.²⁸⁴ In terms of increasing access to technology, the government should develop programs to help subsidize costs of adoption with provisions that data be submitted to the USDA for use in public research and related opportunities, specifically excluding any type of government enforcement action using the data to reduce producer concerns. Support for cooperatives to share technology among members, using membership to increase buying power to reduce technology or service costs, or sharing data infrastructure services would make dollars more effective while also reducing barriers to adoption and increasing data available for public research to potentially benefit more stakeholders. There are also opportunities to increase collaboration and cooperation across government entities, through use of weather sensors that farmers use, while also collecting data for the USDA, the Environmental Protection Agency, or the National Oceanic and Atmospheric Administration. Technology provides opportunities for collaboration and shared information, not just within the USDA or agriculture, but in all agencies. Agriculture is not an island, and information that is valuable to the agricultural sector also has potential value in areas such as public health, commerce, transportation, environmental, weather, and more. Data is often seen as falling into silos, and the government tends to operate in silos as well. How can that be overcome? Can development of open data resources provide opportunities to share data across agencies in ways we have not yet accomplished? I think the opportunities and potential benefits are real, but they require investment from the government, increased communication, and a focus on open data resources. At a minimum, government investment in this infrastructure and increased access will see benefits within the USDA, like those envisioned by the Agriculture Data Act of 2018. The potential for much more though, on a

284. See *Realising Digital Opportunities in Agriculture Requires a Data Infrastructure*, in DIGITAL OPPORTUNITIES FOR BETTER AGRICULTURAL POLICIES, <https://www.oecd-ilibrary.org/sites/d2fbeat0-en/index.html?itemId=/content/component/d2fbeat0-en> [https://perma.cc/2JER-EVT4].

global scale, is real if the resources and the data exist and are accessible.

7. Enacting a Federal Agricultural Data Protection Law

While an industry-specific data protection law similar to HIPAA or the FRCA is seemingly the most straight-forward way to address the concerns about agricultural data privacy, misuse, and abuse, determining how to federally establish those protections is far from clear. As discussed in Part IV.A, the majority of federal data privacy laws focus on (1) a particular industry and (2) protection of personal data for individuals. While the focus on an industry remains the same, challenges arise when attempting to apply the same types of protections to business data rather than personal data. However, this type of legislation is a way to establish consistent standards across the industry for private or public use, set minimum security expectations for those collecting and storing data, require base anonymization standards, and reduce some concerns regarding power dynamics from the discussion.

Jody Ferris similarly came to the conclusion that some sort of federal ag data privacy law was needed due to the potential impacts of misuse and lack of adequate protections through other enforcement mechanisms such as the Federal Trade Commission or practices such as anonymization.²⁸⁵ As Ferris noted, while agricultural data is not the typical type of personal, identifiable data protected under federal privacy laws, protection remains warranted as “reidentification techniques have made thwarting anonymization processes ‘easy’” and “more types of data may be identifiable than previously realized.”²⁸⁶

Aspects of existing privacy laws are easily transferable to ag data. Those already in effect regulate how companies gather information, store information, and use information. These basic elements of regulating companies gathering agricultural data are also necessary, establishing the minimum security expectations and protection expectations. Aspects of HIPAA’s and GLB’s regulations tied to sharing information with third parties and requirements prior to doing so are also essential to ensure protection of producer data, making the third parties adhere to the same security, protection, and use requirements to protect that potentially identifiable data, even if anonymized prior to transfer. While many of the voluntary programs and guidelines call for producers to agree to transfer agdata to third parties and suggest signed disclosure forms, a requirement assures that at least this level of minimum disclosure and knowledge is provided to producers who agree to data transfer.

Development of an agricultural data, industry-specific privacy law based off existing federal laws such as HIPAA is certainly possible and

285. See Ferris, *supra* note 97.

286. *Id.* at 333.

would not take extensive amounts of modification to address numerous concerns. As Ferris pointed out, this type of ag industry legislation would likely not need to be as stringent as HIPAA, but more restrictive than other federal industry regulations.²⁸⁷

However, a federal data privacy law alone will not address concerns related to pressure to sign, inability to negotiate terms, and fear of discrimination if rights were exercised under the law. As noted above, this requires a deeper dive into issues of competition and antitrust and power dynamics within the industry. Incorporating aspects of California's non-discrimination provisions should also be considered, as it may provide a way for some producers to decline to sign disclosure forms or negotiate agreement terms and remain confident in the ability to continue to work with service providers.

Any successful law, and subsequent regulations, in this area also needs to consider potential impacts of public access to data. Access to data for public use and through open data systems should remain a priority and the law needs to reflect that focus. Considering the competing priorities and influences and the speed at which technology develops makes drafting this type of legislation difficult. Flexibility and adaptability are important as well, allowing stakeholders and particularly those whose interests are being protected to maximize the benefits of technology while also feeling confident that same data will not be used against them. Ensuring the focus is on priorities such as (1) protecting interests of producers of all sizes, (2) encouraging public research and open access to data in safe and secure manners, and (3) reducing the digital divide makes for a series of hurdles for any legislative drafter. Yet this type of legislation may ultimately be the best, and perhaps the only, option to provide basic levels of privacy, security, and use limits to all producers, no matter size, scope, or type of production.

VIII. CONCLUSION

Considering how to use technology to advance public and private needs, while not harming those upon whose work and data is necessary, is far from an easy task. While industry initiatives on a voluntary basis are a start, the government needs to step in and ensure that it provides minimum levels of security and protection to producers and their data to prevent misuse and abuse and to encourage innovation and research in ways that benefit the public good.

Problems arise when attempting to determine what is the best step, or even the best first step, to address the concerns discussed within this Article. Considering the options or suggestions discussed above, no one will work alone. All require coordinated efforts and more cooperation in Congress and between state and federal regulators than

287. *Id.* at 340–41.

may be possible in current political times. Voluntary efforts and self-regulation within the industry are likely to continue, but without greater coordination, increased involvement of technology providers, and more focus on addressing power dynamics and access to technology, those efforts will have limited impact.

No attempt to manage agricultural data privacy concerns can be successful without considering impacts upon and interests of all stakeholders. Providing producers, agribusinesses, research institutions, and governments of all sizes a seat at the table, with all having an equal voice in the discussion, is key to developing ethical and fair programs and policies that look at more than just contract terms. In our highly divisive and competitive agricultural industry, that itself may seem an insurmountable task. Yet for hundreds of years, we have put a priority in this country on valuing agricultural production and those that engage in farming.²⁸⁸ If we see value in farmers and their relationship with the land and role in our health and economy, then we need to take steps now to ensure that the technology and data needed to engage in this industry in the modern era is not used to cause harm.

288. See Susan A. Schneider, *A Reconsideration of Agricultural Law: A Call for the Law of Food, Farming, and Sustainability*, 34 WM. & MARY ENV'T L. & POL'Y REV. 935 (2010).

