Minnesota Journal of Law, Science & Technology

Volume 18 | Issue 1 Article 6

1-2017

Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary?

Jody L. Ferris

Note

Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary?

*Jody L. Ferris**

The collection of data about individuals has created much debate both in the legal community and society as a whole. The debate includes such issues as what constitutes proper notice to consumers that their data is being collected, privacy, unauthorized disclosure of information to third parties, and the security of systems on which collected information is stored. These issues are certainly present in one particular industry where the large-scale collection of information is becoming increasingly popular—the agriculture industry.

The agriculture industry, like many others, has been driven by technological development and innovation.[1] Growing more crops, on less land, using fewer resources, is a main focus of this development and innovation.[2] The production of food in a way that is efficient and highly productive is of utmost importance to society. To quote one individual in the agriculture industry, "once in your life you need a doctor, a lawyer, a policemen and a preacher but every day, three times a day, you need a farmer."[3]

---

* JD & Master of Public Policy Candidate, 2017, University of Minnesota; BA Political Science & Communications, 2013, Dickinson State University. Special thanks to the staff at MJLST for their work on this piece.

1. *Historical Timeline-Farm Machinery & Technology*, NAT'L AGRIC. IN THE CLASSROOM, https://www.agclassroom.org/gan/timeline/farm_tech.htm (last visited Oct. 24, 2016) (presenting a timeline describing noteworthy landmarks in agricultural production throughout history).

2. *See, e.g.*, Tim Folger, *The Next Green Revolution*, NAT'L GEOGRAPHIC, http://www.nationalgeographic.com/foodfeatures/green-revolution/ (last visited Feb. 14, 2016) (describing how "the green revolution" spearheaded by scientist Norman Borlaug assisted producers in producing more wheat and rice per acre).

3. BRENDA SCHEOPP, http://brendaschoepp.com/ (last visited July 1, 2016).

The practice of precision agriculture is an important technological development in the agriculture industry because it enables crop production to be more efficient and more productive.[4] Precision agriculture is the practice of using a segmented management approach in which the various aspects of crop production are tailored to meet the unique needs of each individual segment of land.[5] The practice consists of the integrated use of various individual tools, and is itself constantly evolving.[6] A number of these tools have the capacity to collect extremely large amounts of data, what may be termed "big data," from the agricultural producers who utilize the tools in their farming practices.[7] As with any area in which information may be collected about individuals through their use of a product or service, significant concerns about the privacy and security of this information have arisen.[8]

The goal of this note is to argue that the current data privacy and security regulations in the United States are not sufficient to protect agricultural data, and that a federal scheme should be put into place to govern data practices in the

---

4. John Hart, *Efficiency, Accuracy Biggest Advantages of Precision Agriculture*, SOUTHEAST FARM PRESS (Mar. 4, 2015), http://southeastfarmpress.com/management/efficiency-accuracy-biggest-advantages-precision-agriculture (explaining how targeted application of chemicals and fertilizers, the ability to take on-the-go soil samples and analysis, etc., has been able to improve crop yields).

5. Aaron DeJoia & Matt Duncan, *What Is "Precision Agriculture" and Why Is It Important?*, SOILS MATTER, GET THE SCOOP! (Feb. 27, 2015), https://soilsmatter.wordpress.com/2015/02/27/what-is-precision-agriculture-and-why-is-it-important ("Growers are able to take large fields and manage them as though they are a group of small fields. This reduces the misapplication of products and increases crop and farm efficiency.").

6. *Id.*; Hart, *supra* note 4 ("You need to be able to interface your tractor, your truck, your home, your sprayer and your combine. You need to be able to integrate all that you do. This integrated approach brings the full value to precision agriculture.").

7. *See* Tiffany Dowell, *Big Data on the Farm (Part I): What Is It?*, TEX. AGRIC. L. (Sept. 1, 2015), http://agrilife.org/texasaglaw/2015/09/01/big-data-on-the-farm-part-i-what-is-it/ ("[B]ig data refers to the ability to collect and analyze large amounts of information. Today, technology allows producers to gather mountains of information about their own operations.").

8. Isabelle M. Carbonell, *The Ethics of Big Data in Big Agriculture*, 5 INTERNET POL'Y REV. 1, 8–9 (2016) (concluding that one reason security must be protected in the agriculture industry is to ensure that big data collectors in agriculture, like Monsanto, do not secretly use the gathered data for commodity market speculation, which would cause a detriment to farmers using information gathered from them).

agricultural industry. Part I will give an overview of the practice of precision agriculture, the ways in which producer data is being collected, and the ways in which producer data is being stored and utilized. It will also briefly describe some characteristics of precision agriculture data. Part II will examine in depth what current regulations and statutes relating to data privacy and security are in place and which ones may govern activity in the agriculture industry. Part III will propose that a solution to ensure that agricultural data is protected should come in the form of new federal data privacy and security legislation targeted specifically to the agriculture industry, similar to those regulations which target the healthcare and financial services industries.

I. BACKGROUND

A. A BRIEF HISTORY OF PRECISION AGRICULTURE AND AGRICULTURAL DATA COLLECTION

"The fundamental concept of precision agriculture, collecting data and making decisions based on that data, has been around for many years. This was easier to do without technology on small plots. But as the size of farms grew, this no longer was possible."[9] More sophisticated approaches than the age-old practice of recording information with a paper and pen are required to collect information and strategically manage increasingly larger agricultural operations with thousands and tens of thousands of acres of land.[10] The modern concept of precision agriculture, using a number of new technologies to manage crop production at a section-by-section level, came into being in the 1980s.[11] Precision agriculture has been defined as

---

9. *History of Precision Agriculture*, DELMAR CENGAGE LEARNING, http://www.delmarlearning.com/companions/content/140188105X/trends /history_pre_agr.asp (last visited Oct. 24, 2016). For an interesting historical example of early agricultural record keeping, see generally *George Washington as a Farmer*, GEORGE WASHINGTON'S MOUNT VERNON, http:// www .mountvernon.org/research-collections/digital-encyclopedia/article/george-washington-as-farmer/ (last visited Jan. 16, 2016) (explaining how Washington kept handwritten records of what he planted and which products he used to guide his farm management decisions).

10. *History of Precision Agriculture*, *supra* note 9.

11. James Taylor & Brett Whelan, Austl. Ctr. for Precision Agric., *A General Introduction to Precision Agriculture*, *in* PRECISION AGRICULTURE FOR GRAIN PRODUCTION SYSTEMS 1 (2006), http://www.agriprecisione.it/wp-

"a management system that is information and technology based, is site-specific and uses one or more of the following sources of data: soils, crops, nutrients, pests, moisture, or yield, for optimum profitability, sustainability, and protection of the environment."[12]

One of the first technologies to be used for this purpose was variable-rate application equipment paired with soil fertility maps, which allowed fertilizer to be applied to the land at varying amounts depending on the location of the equipment in the field.[13] Variable-rate application was paired with Global Positioning System (GPS) technology to track the location of equipment via satellite.[14] The introduction of GPS technology to agriculture also facilitated the development of crop yield monitoring systems, which allowed for "the fine-scale monitoring and mapping of yield variation within fields. The linking of yield variability data at this scale with maps of soil nutrient changes across a field marked the true beginning of [precision agriculture] in broadacre cropping."[15]

Today, these tools and others continue to be used in the practice of precision agriculture.[16] GPS receivers, yield monitors, and variable rate application systems are now combined with other tools such as cellphones, personal computer systems and tablets to permit agricultural producers to collect and store a sizable and comprehensive amount of information about their farming operations.[17] This data has

---

content/uploads/2010/11/general_introduction_to_precision_agriculture.pdf ("[P]recision Agriculture in cropping systems emerged in the late 1980's with the matching of grid-based sampling of soil chemical properties with newly developed variable-rate application (VRA) equipment for fertilisers.").

12. U.S. DEP'T AGRIC. NAT'L. RES. CONSERVATION SERV., PRECISION AGRICULTURE: NRCS SUPPORT FOR EMERGING TECHNOLOGIES 1 (2007), http://www.nrcs.usda.gov/Internet/FSE_DOCUMENTS/stelprdb1043474.pdf.

13. *Id.* at 1. Variable rate fertilizer application was developed before GPS technology was utilized in precision agriculture. To coordinate the equipment with specific locations in a field, compasses and dead-reckoning principles were used to compare to maps of soil fertility that had been developed by soil sampling a field in multiple locations. These maps show characteristics of the soil such as nutrient levels which allows producers to determine the necessary level of fertilizer that needs to be applied to that specific area.

14. *Id.* at 1–3.

15. Taylor & Whelan, *supra* note 11, at 1.

16. *See generally id.* (discussing how these different technologies are used in precision agriculture).

17. Lauren Manning, *What is Ag Big Data? How 8 Companies Are Approaching It*, AGFUNDER NEWS (Nov. 12, 2015), https://agfundernews.com

been classified into three categories: agronomic data, which refers to information regarding the yields of crops and the amount of input products applied; machine data, which refers to information about farm equipment; and weather data.[18]

B. WHAT ARE THE BENEFITS OF DATA COLLECTION IN PRECISION AGRICULTURE?

The practice of data collection in precision agriculture has many benefits.[19] It permits producers to better manage their crops to increase their yields, and therefore, their profits by giving them the ability to collect and analyze more information about their operations.[20] This encourages better management decisions because a producer can review past performance to improve crop production on their unique fields. It also allows producers to grow more food for consumers using less land and resources, which is beneficial to the environment.[21] Another environmental benefit of precision agriculture technology is that agricultural products may be applied only where and when they are needed, so less may ultimately be used.[22] It has also been suggested that the information collected by precision agriculture will provide an incentive for producers to improve their environmental stewardship, as this data can provide evidence of good environmental practices that may be

---

/what-is-ag-big-data5041.html ("[M]ost [precision agricultural] programs are now accessible through computers, tablets and smartphones, and often include a customizable dashboard of the various data sets he or she is tracking.").

18. Dowell, *supra* note 7 (crediting Todd Janzen for recognizing these three main data categories in the agriculture industry).

19. *See* Jennifer Carrico, *Secure Data Helps Farmers Become More Efficient*, HIGH PLAINS/MIDWEST AG J. (Aug. 31, 2015) http://www.hpj.com /carrico/secure-data-helps-farmers-become-more-efficient/article_8a18759d-c1e7-5473-8a73-798785375d44.html (suggesting such benefits may include increased profit, more sustainable farming technique, and benefits to the environment).

20. *Id.* (explaining how companies such as the Climate Corporation, provide "digital data on agronomics" in order to help farmers more efficiently grow their crops).

21. DeJoia & Duncan, *supra* note 5 ("[U]sing precision agriculture, farmers are able to produce more food at a fraction of the cost. Farmers also conserve soil for sustainable food production.").

22. Taylor & Whelan, *supra* note 11, at 5–7 ("If better management decisions are being made to tailor inputs to meet production needs then by default there must be a decrease in the net loss of any applied input to the environment.").

advertised to consumers, or may be used to avoid litigation based on claims of environmental damage.[23]

C. HOW IS THE INFORMATION COLLECTED AS PART OF PRECISION AGRICULTURE UTILIZED?

Ultimately, precision agriculture is used to improve the performance of agricultural operations based on lessons learned from looking at agricultural data from previous years.[24] Data collected from various tools may be stored and used in a variety of ways. Producer data can be collected in the field and sent directly to an agricultural technology provider (ATP) through cloud technology.[25] An ATP may offer to provide storage for a producer's data.[26] It may also offer to conduct analysis of the data and provide agronomic advice for a fee.[27]

Producers may store and analyze their data on their own personal or business systems.[28] They can compare yields from the current year with prior years themselves to understand which production methods and products are most successful.[29] They can choose to share their information with a local agronomist, or send it away to be analyzed by a service

---

23. *Id.* at 6 ("This gives producers physical evidence to contest any claims against negligent management or alternatively provide information on 'considerate' practices to gain market advantage.").

24. *See id.* at 10 (explaining that precision agriculture encompasses the "use of advances in information technology in agriculture").

25. *Startups, Major Agribusinesses Compete in Big Data Market Space*, AGRIMARKETING (Sept. 3, 2015), http://www.agrimarketing.com/s/98423 (explaining how companies are "developing computer systems that will enable farmers to capture data streaming" from their farm equipment). Agricultural technology providers are companies that sell precision agriculture tools as well as other agricultural products and services to producers. Examples include companies like Monsanto and others similar to it. *See Privacy and Security Principles for Farm Data*, AM. FARM BUREAU FED'N (Mar. 3, 2016), http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf.

26. *See generally Startups, Major Agribusinesses Compete in Big Data Market Space*, *supra* note 25 (discussing how "data silos" allow producers to store their data on a company's platform).

27. *Id.* (discussing how such data could help big agriculture companies advise clients on the types of seeds to use, fertilizers to utilize, etc.).

28. *See generally id.* ("[C]rop producers can get the most from their data by compiling and analyzing it themselves—for instance, to determine the best time to apply fertilizer to their soil and how much.").

29. *See id.*

providing agronomic advice.[30] These methods allow producers to keep control over their data and with whom it is shared.[31]

Some newer companies hope to provide producers with an option to store data on a system independently of large ATPs.[32] These companies are developing platforms to store agricultural data in "digital silos," which would allow producers to analyze their data themselves, give access to third parties they may choose to analyze the data for them, or perhaps even take part in opt-in programs which may help them disclose their data to third parties for a profit in which they would share.[33]

When producer data is transmitted to companies that offer to store or analyze the data, these companies take on the responsibility of keeping the data secure.[34] It follows that these companies have a responsibility to protect the data and the privacy of producers supplying the data both in accordance with producer wishes and applicable law.[35]

D. CHARACTERISTICS OF PRECISION AGRICULTURE DATA

A simple definition of big data states that it "is a collection of data from traditional and digital sources inside and outside [a] company that represents a source for ongoing discovery and analysis."[36] Regardless of the industry it is collected in, what is referred to as big data has certain characteristics. These

---

30. *Id.* ("[S]tartups . . . are developing computer systems that will enable farmers to capture data streaming from their tractors and combines, store it in digital silos and market it to agriculture companies or futures traders.").

31. *See generally id.*

32. *See id.* (stating that startups are now competing with larger agribusinesses in the ATP market).

33. *Id.* Companies such as Farmobile LLC and Grower Information Services Cooperative are spearheading these efforts.

34. Will Rodger & Mace Thornton, *Farmers, Agriculture Technology Providers Reach Agreement on Big Data Privacy and Security Principles Expected to Accelerate Technology Adoption*, AMER. FARM BUREAU FED'N (Nov. 13, 2014), http://www.fb.org/newsroom/news_article/188/ (detailing how many major farming organizations reached an agreement wherein ATPs will ensure steps are taken to protect farmer's private agricultural data). *But cf.* Carbonell, *supra* note 8, at 7–9 (arguing that collected agricultural data should be made public so that farmers around the world can make use of the data in their own practices).

35. *See* Rodger & Thornton, *supra* note 34.

36. Lisa Arthur, *What Is Big Data?* FORBES (Aug. 15, 2013, 8:17 AM), http://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/#390bafc03487.

characteristics are: volume, as organizations collect large amounts of data from varied sources; velocity, as "data streams in at an unprecedented speed"; and variety, as "[d]ata comes in all types of formats – from structured, numeric data in traditional databases to unstructured text documents."[37] These characteristics and other features of big data collection and storage systems, like "large-scale cloud infrastructures, diversity of data sources and formats, streaming nature of data acquisition, and high volume inter-cloud migration" present greater privacy and security challenges to organizations than data collection did in the past.[38]

The data about farming operations collected using the tools of precision agriculture has many characteristics that make it sensitive.[39] The data collected may contain the personal information of individual producers.[40] This information may include names and addresses,[41] property locations, as well as crop yield information, which may lead to inferences about a producer's income and the value of their farmland.[42] Producers are understandably unenthusiastic about the risk of this information getting into the hands of unauthorized third parties, for example, citing a history of environmental groups

---

37. *Big Data: What It Is and Why It Matters*, SAS, http://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited Oct. 24, 2016). SAS has also begun to consider variability (peaks in the data loads), as well as complexity (difficulty in linking and matching different source data) when analyzing "big data."

38. CLOUD SEC. ALL., TOP TEN BIG DATA SECURITY AND PRIVACY CHALLENGES (2012), http://www.isaca.org/groups/professional-english/big-data/groupdocuments/big_data_top_ten_v1.pdf.

39. Meghan Grebner, *Addressing Privacy Concerns with Big Data*, BROWNFIELD (Jan. 31, 2014), http://brownfieldagnews.com/2014/01/31/addressing-privacy-concerns-big-data/. *See also* Carbonell, *supra* note 8, at 8–9 (arguing that such data collected by big-agriculture has the potential to allow companies to make projections regarding which markets to support, and which markets to avoid).

40. Dowell, *supra* note 7 (expressing that some "fear that farmers names, addresses, social security numbers, and other personal information could be inadvertently given to third parties through the sharing of datasets with others").

41. *Id.*

42. *See generally* Jacob Bunge, *Big Data Comes to the Farm Sowing Mistrust*, WALL STREET J. (Feb. 25, 2014, 10:38 AM), http://www.wsj.com/articles/SB10001424052702304450904579369283869192124 ("If nearby farmers saw crop-yield information, it might spur unwanted competition to rent farmland, pushing land costs higher.").

targeting agricultural producers when they are able to access producer personal information.[43] Producers are also concerned about competitors gaining access to their data and who may use it against them.[44] Some producers also worry that collected data about their farm practices could be used for regulatory enforcement purposes.[45]

Another major reason producer data is sensitive is how economically valuable it is. Agricultural technology providers could use data gathered from producers to develop new products to sell and significantly increase their own profits.[46] Commodity traders may use the data gathered to better guide their activity on the stock market.[47] It is likely these or other third parties may be interested in purchasing producer information from a company collecting it on behalf of a producer. Additionally, the general concerns about data privacy and security that span all industries in which data is collected, such as whether data anonymization techniques are effective, are also present in the agriculture industry.[48]

---

43. Stephanie Mercier, *The Emergence of Big Data Issues for Agriculture*, STRAIGHT FROM D.C.: AGRIC. PERSP. (Sept. 9, 2015), http://www.agweb.com/blog/straight-from-dc-agricultural-perspectives/the-emergence-of-big-data-issues-for-agriculture/. For example, in 2004 the Environmental Working group used personal financial information of producers that they obtained from the Environmental Protection Agency to discredit producers by spreading it publicly on a website. *Id.*

44. Bunge, *supra* note 42. Yield data could easily demonstrate that one producer's methods are better than another's. Alternatively, a competitor finding out how productive a particular piece of land is may offer a landlord a higher price for it than the producer currently farming it. *Id.*

45. David Frohnen, *Problems with Strict Data Privacy in Agriculture*, FARM MKT. ID (May 21, 2015), http://www.farmmarketid.com/problems-with-strict-data-privacy-in-agriculture/ (citing an American Farm Bureau Federation survey in which 77% of respondents were concerned about their data being used for regulatory purposes).

46. Bunge, *supra* note 42 (noting some of the successful technology making the market is from Monsanto, releasing such products as FieldScripts, which assists farmers in sustainably farming their fields and maximizing their crop yields).

47. *See id.* ("Some farmers . . . worry their data might be sold to commodities traders").

48. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (arguing that keeping people's information private has been a shortfall of many large industries).

E. REGULATORY BACKGROUND

Data protection law is becoming one of the fastest growing areas of legal regulation.[49] A number of recent security breaches affecting high-profile companies in which unauthorized third parties gained access to consumer data have helped spur regulators to action.[50] However, there is currently no regulatory system in the United States specifically tailored to the data being collected and shared in the agriculture industry.[51] The House Agriculture Committee held a hearing on data practices in the agriculture industry in October of 2015.[52] Although the Committee heard concerns regarding big data practices in the industry, "most panelists agreed that little to no government intervention was desired."[53] Industry groups have attempted to come up with best practices regarding data privacy and security for companies in the agriculture industry.[54] However, these are simply voluntary standards which do not hold the force of law. Legal requirements for agricultural technology providers are limited to current general federal and state data privacy and data protection laws that apply.

The current regulatory system for data protection in the United States "resembles a patchwork quilt. Unlike other jurisdictions, the United States does not have a dedicated data protection law, but instead regulates primarily by industry, on

---

49. Ieuan Jolly, *Data Protection in United States: Overview*, PRAC. L. (July 1, 2016), http://us.practicallaw.com/6-502-0467.

50. *See, e.g.*, *id.* (highlighting some of the recent action being taken at both the state and federal level, in order to impose regulations on industry designed to protect private data); *see also* Sai Ramanan, *The Top 10 Security Breaches of 2015*, FORBES (Dec. 31, 2015, 4:14 PM), http://www.forbes.com /sites/quora/2015/12/31/the-top-10-security-breaches-of-2015/print/ (identifying companies like BlueCross BlueShield as verified victims of cyber attacks).

51. MEGAN STUBBS, CONG. RES. SERV., BIG DATA IN U.S. AGRICULTURE 3 (2016), https://www.fas.org/sgp/crs/misc/R44331.pdf (finding that no congressional action has yet been taken to regulate "big data" in the agriculture industry).

52. *Id.* at 3. The hearing was held on October 22, 2015.

53. *Id.* Furthermore, Stubbs states that "[n]o bills have been introduced in the last two Congresses relating specifically to big data in agriculture. Several bills in the 114th Congress could address issues that are potentially relevant to big data applications in agriculture, such as information sharing in cybersecurity, privacy, and notification of data breaches." *Id.*

54. *See Privacy and Security Principles for Farm Data*, *supra* note 25.

a sector-by-sector basis."[55] At the federal level, there are two major industries in which data practices are regulated: the financial services industry, regulated under the Gramm-Leach-Bliley Act; and the healthcare industry, regulated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[56] Additionally, the Federal Trade Commission (FTC) is "the primary federal privacy regulator in the US. Section 5 of the FTC Act, which is a general consumer protection law that prohibits 'unfair or deceptive acts or practices in or affecting commerce,'" and "is the FTC's primary enforcement tool in the in the privacy area."[57]

In addition to federal efforts to regulate data privacy and protection practices, states have independently enacted and enforced their own data privacy and data protection laws and regulations.[58] Two examples of states which have enacted their own data privacy and protection laws are California and Massachusetts.[59] However, state laws may not apply to the

---

55. Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* DATA PROTECTION AND PRIVACY 2014, at 191, 191 (2014), https://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdf.

56. *Id*. at 191.

57. *Id*.

> [T]he FTC has used its authority under Section 5 to bring numerous privacy enforcement actions for a wide-range of alleged violations by entities who information practices have been deemed 'deceptive' or 'unfair'. Although section 5 does not give the FTC fining authority, it does enable the Commission to bring enforcement actions against alleged violators, and these enforcement actions typically have resulted in consent decrees that prohibit the company from future misconduct and often require audits iennially for up to 20 years. Under section 5, the FTC is able to fine businesses that have violated a consent decree.

Id.; *see also Enforcing Privacy Promises: Making Sure Companies Keep Their Privacy Promises to Consumers*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Oct. 25, 2016) (explaining how the FTC takes "law enforcement action to make sure that companies live up these [consumer privacy] promises").

58. Sotto & Simpson, *supra* note 55, at 195. Attorneys general have the authority to enforce unfair or deceptive trade practices, as well as the ability to enforce specific state laws.

59. *Id*. at 192–198. The California law requires an organization collecting personal information from individuals to notify them about the categories of personal information collected through the website, the categories of third-parties with whom the company may share the data, the process someone

specific types of data collected by companies in the agriculture industry.

II. ANALYSIS

This section will examine current federal data protection regulation, focusing on FTC authority and how it may apply to the agriculture industry. It will include a discussion of two examples of state data protection laws and how these may apply to agricultural data. It will also include a discussion of the attempts of an agricultural industry coalition to come up with its own "best practices" to guide behavior in this area. This section will close with an explanation of why current data privacy and security regulations, as well as industry self-regulation efforts, are insufficient to protect agricultural data.

A. REGULATION OF DATA PRIVACY AND SECURITY IN THE UNITED STATES

1. Regulation at the Federal Level

At the federal level, the primary regulatory body that polices data privacy and protection practices across all industries is the FTC.[60] The FTC uses its authority under Section 5 of the FTC Act to regulate the data privacy and protection practices of companies, seeking to protect consumers against "unfair or deceptive acts or practices in or affecting commerce."[61] The FTC has been granted enforcement authority under the Act in the form of its ability to grant cease-and-desist orders,[62] to seek injunctive relief in federal court,[63] and to promulgate rules.[64]

In the context of data privacy and protection issues, the FTC has used its authority to take action against both deceptive and unfair practices. The FTC has used its authority

---

must follow to review and request changes to any of their personal information collected, among other requirements.

60. *See generally id.* (highlighting the enforcement duties and enforcement capabilities of the FTC).

61. 15 U.S.C. § 45(a)(1) (2012).

62. *Id.* § 45(b).

63. *Id.* § 53(b).

64. A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY, FED. TRADE COMM'N (2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

to take action against deceptive practices to discipline companies that "tell consumers they will safeguard their personal information" and then break these promises by disclosing sensitive information or failing to adequately keep consumers' personal information secure.[65] For example, the FTC has pursued enforcement action against companies who did not follow their own posted privacy policies.[66] The FTC has also taken action against companies whose data protection and privacy policies it has deemed to be unfair.[67]

For a practice to be considered "unfair" under the FTC Act, it must "cause[ ] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[68] The FTC applies an objective test to determine whether the injury is substantial: the "injury must be real, and it must be large compared to any offsetting benefits."[69] In order to determine whether the injury is reasonably avoidable by consumers, the FTC looks to whether a consumer has the ability to make a different choice than using the product or service in question, but chose that particular product or service anyway.[70]

In *FTC v. Wyndham Worldwide Corp.*, the FTC filed a suit in Federal District Court against a company for its unfair data security practices.[71] The FTC claimed that the company had unfair practices in the form of "unreasonabl[e] and

---

65. *Enforcing Privacy Promises*, *supra* note 57.

66. Jolly, *supra* note 49 ("The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorized disclosure of personal data.").

67. *See* FTC v. Accusearch, Inc., 570 F.3d 1187, 1193–1195 (10th Cir. 2009) (holding that the FTC could establish the substantial injury element of an unfair practice claim by demonstrating subversion of consumer privacy protection afforded by the Telecommunications Act); Antony Kim, *Third Circuit to Wyndham*, MONDAQ BUS. BRIEFING (Aug. 28, 2015) (reporting the Third Circuit's affirmation of the FTC's ability "to regulate 'unfair' cybersecurity practices under Section 5 of the FTC Act").

68. 15 U.S.C. § 45(n).

69. J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

70. *Id.*

71. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

unnecessar[y]" exposure of consumer information to unauthorized third parties.[72] The company was the subject of three security breaches, stored customer credit card information in readable text, failed to use basic security measures, allowed third party vendors to connect to its network without adequate precautions, used out-of-date operating systems, and failed to adequately respond to security related incidents.[73] In an interlocutory appeal, the company challenged the FTC's authority to regulate its conduct under the FTC's "unfairness authority" and whether it had been given fair notice regarding the insufficiency of its own data privacy practices.[74] The Third Circuit disagreed with Wyndham, and upheld the FTC's authority to pursue enforcement action against the company for its unfair data security practices.[75]

An FTC enforcement action in the areas of data privacy and security will often result in a settlement between the parties and a consent decree.[76] A consent decree "is a judgment or order that reflects the settlement terms agreed to by the parties, and that contains an injunction."[77] After the FTC brings an enforcement action by filing a complaint, it and the regulated party enter into settlement negotiations.[78] The ultimate settlement usually results in the regulated party agreeing to a consent decree in which the party agrees to make changes in the data privacy and security practices, submits to audits, and promises to adhere to the decree for a specified length of time.[79]

---

72. *Id.* at 608.

73. *Id.* at 608, 626.

74. *See id.* at 607–08.

75. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

76. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 223 (2016) ("The FTC and the defendant typically work out a consent order that includes changes in the defendant's practices, without the defendant conceding that those practices were unlawful."); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV., 583, 606 (2014).

77. Anthony DiSarro, *Six Decrees of Separation: Settlement Agreements and Consent Orders in Federal Civil Litigation,* 60 AM. U. L. REV. 275, 277 (2010).

78. MCGEVERAN, *supra* note 76, at 223.

79. *Id.*

An example of a consent decree is the one that Snapchat, Inc. entered into with the FTC in 2014.[80] The decree included requirements: that, for a period of twenty years, the company would no longer "misrepresent in any manner, expressly or by implication, in or affecting commerce, the extent to which respondent or its products and services maintain and protect the privacy, security or confidentiality of any covered information";[81] that the company would implement "a comprehensive privacy program" tailored to its own practices, and document the program and its implementation in writing;[82] that the company would obtain an independent third party audit of their data privacy and security practices biennially;[83] and that the company would keep on file to provide to the FTC upon request copies of any statements regarding its data privacy and protection practices, any consumer complaints about such practices, any documents that demonstrate the company's failure to comply with the consent decree, and copies of the third party audits.[84]

One commentator argues that, since there are so few judicial decisions in this area, these consent decrees function as "de facto common law."[85] While these instruments have the legal function of a contract in binding the party that was the subject of an enforcement action, they do not serve as binding precedent to other regulated parties.[86] However, in practice, the instructions set forth in a consent decree are examined with great interest by privacy practitioners and often viewed as though they have precedential force.[87] Therefore, the content of these decrees may serve as guidelines for what the FTC considers to be minimum appropriate data privacy and data

---

80. *Id.* at 223–24; Snapchat, Inc., Docket No. C-4501, 2014 WL 7495798 (F.T.C. Dec. 23, 2014) (Complaint preceding the consent decree).

81. Snapchat, Inc., 2014 WL 7495798, at *7.

82. *Id.* at *7.

83. *Id.* at *8–9.

84. *Id.* at *8–10.

85. *See* Solove & Hartzog, *The FTC and The New Common Law of Privacy*, *supra* note 76, at 606.

86. *Id.* at 607.

87. *Id.* at 620. *See also* DiSarro, *supra* note 77, at 290 ("Consent decrees . . . have significant information value to those monitoring the federal courts.").

security principles.[88] Critics of the FTC's use of consent decrees to convey their conception of adequate data protection practices have claimed that the FTC does not provide proper notice or articulate clear enough expectations for other regulated parties.[89]

Although the FTC Act would allow it to regulate the data privacy and security practices of companies in the agriculture industry, it may not hold agricultural technology providers to high enough standards. The "deception" prong of the Act allows the FTC to hold companies to their posted data privacy and data collection policies,[90] but it does not go so far as to set a minimum requirement for what these policies need to be. An agricultural producer may not understand what an effective data privacy and data protection policy should contain, and so may not be aware that the promises a company was making were not adequate to protect sensitive information, even though the company kept the promises. In this scenario, the company would not be engaging in deceptive practices to warrant enforcement action by the FTC,[91] but may not be taking adequate steps to protect producer data either.

Should a company's data security be extremely ineffective, it may be enough to warrant an FTC enforcement action as an unfair practice if comparable to the defendant company's outrageously insufficient data protection and privacy practices in *Wyndham*.[92] However, it seems likely that there is a large gray area between what constitutes unfair practices worthy of an enforcement action in the eyes of the FTC and what constitutes data security best practices.[93] Increasing this gray area is the reality that the FTC has limited resources and

---

88. *See* Solove & Hartzog, *The FTC and The New Common Law of Privacy*, *supra* note 76, at 621–22.

89. Woodrow Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2232 (2015).

90. Jolly, *supra* note 49.

91. *Id.*

92. *See generally* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D. N.J. 2014) *aff'd*, 799 F.3d 236 (3d Cir. 2015).

93. *See* PATRICIA BAILIN, WESTIN RESEARCH CTR., STUDY: WHAT FTC ENFORCEMENT ACTIONS TEACH US ABOUT THE FEATURES OF REASONABLE PRIVACY AND DATA SECURITY PRACTICES 2 (2014), https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf (last visited Nov. 12, 2016) (showing that the current scope of FTC involvement in data privacy cases has been limited to only forty-seven citations since 2002).

focuses enforcement action on some types of companies more than others.[94]

FTC enforcement decisions are affected by the agency's limited resources, and the Commission often focuses on the most "egregious cases with more serious harms," including cases involving extremely sensitive information, very large companies, or companies handling the data of vulnerable groups such as children.[95] It is estimated that the FTC brings only between "ten to twenty-five privacy and data security cases per year."[96] The FTC also focuses its enforcement actions on cases "with a high likelihood of success and where companies have no viable defense."[97] This strategy seems to leave open scenarios where a company is engaging in unfair or deceptive practices but may have the ability to put up a reasonable defense out of the realm of enforcement. Despite being able to reasonably defend poor data protection practices, a company may not be adequately protecting consumer data. Some have also argued that FTC enforcement is too unpredictable, with unfairness actions for poor data security practices filed "at random."[98] All of the above factors suggest that certain companies, with particular types of practices, are more likely to be the target of enforcement actions than others.

Based on the above factors, companies in the agriculture industry do not appear very likely to find themselves a target of an FTC enforcement action. Agricultural technology providers do not collect extremely sensitive personal data (unlike Snapchat, Inc.'s collection of occasionally racy photographs), do not collect data about children, and often are not high-profile

---

94. MCGEVERAN, *supra* note 76, at 225 ("The FTC has limited resources, so it must select its cases carefully to maximize their impact."); *FTC Staff Directory*, FED. TRADE COMM'N (Sept. 18, 2013), https://www.ftc.gov/sites/default/files/attachments/contact-federal-trade-commission/whitepages.pdf (showing the limited number of staff the FTC has).

95. MCGEVERAN, *supra* note 76, at 225.

96. Hartzog & Solove, *The Scope and Potential of FTC Data Protection*, *supra* note 89, at 2234.

97. Solove & Hartzog, *The FTC and The New Common Law of Privacy*, *supra* note 76, at 613.

98. *Id.* at 607 (discussing the views of those who argue that FTC action is unpredictable, while the majority of their article argues the opposite view).

entities.[99] These characteristics make it unlikely that an agricultural company technology provider would be a traditional target for an FTC enforcement action.

The FTC has not issued any minimum data privacy and protection standards for companies to follow through new regulations.[100] Although consent decrees can provide some guidance as to what behavior the FTC would like to see in companies, this type of guidance may not be very valuable for companies that are organized much differently than the target of the consent decree.[101] Therefore, if agricultural technology providers do not see themselves as prime candidates for an FTC enforcement action, as discussed above, they may not have much incentive to adhere to good data privacy and security practices. Additionally, if these companies see themselves as very different types of entities than the companies subject to previous consent decrees, they may find little guidance from consent decrees binding other companies as they structure their unique data privacy and security policies.

2. Regulation at the State Level

In addition to federal regulation, a number of states have implemented their own data protection legislation.[102] One prominent example of a state that has taken data privacy and security regulation into its own hands is California.[103] There

---

99. For example, Snapchat, Inc. was known by the FTC to involve photographs involving various types of immoral activity. *See* MCGEVERAN, *supra* note 76, at page 225.

100. *Id.* at 245–46. Although the FTC has the ability to promulgate rules, the complex congressionally required rulemaking procedures specific to the FTC that it must follow makes it unreasonable for it to do so. *Id*. Occasionally, Congress will authorize the FTC to promulgate rules under the less stringent Administrative Procedures Act standards. *Id*.

101. Solove & Hartzog, *The FTC and The New Common Law of Privacy*, *supra* note 76, at 625 ("[T]he company brokering the compromise might not be representative of all stakeholders or even of a majority of stakeholders. The compromise might be workable for that company and others of a similar size and structure, but might not be as workable for other companies.").

102. Heather Sussman, *Tracking State Data Protection Enforcement in 2014*, LAW360 (Dec. 19, 2014), http://www.law360.com/articles/606359/tracking-state-data-protection-enforcement-in-2014.

103. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/. One commentator said that the California digital privacy law is the "the most comprehensive in the country." However, the commentator also stated that five other states "have warrant

are a number of statutes the state has enacted in this area.[104] For example, the Electronic Communication Privacy Act contains provisions that: "[b]ar[ ] any state law enforcement agency or other investigative entity from compelling a business to turn over any metadata or digital communications – including emails, texts, documents stored in the cloud – without a warrant."[105] The law also does not permit law enforcement agencies to track an electronic device's location without a warrant.[106]

Another California statute, the Shine the Light Law,[107] requires that companies which share consumer data to third parties must tell consumers which parties they share any data with.[108] A third statute, the Data Security Law, requires companies to "implement and maintain reasonable security procedures . . . to protect personal information from unauthorized access, destruction, use, modification, or disclosure."[109] Additionally, the California Online Privacy Protection Act "applies to an operator of a commercial website, online service or mobile app, that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service."[110] This law requires a website to post its privacy policy publicly and describe the procedures it uses to handle consumer information.[111] California also has a security breach notification law in place,[112] which requires companies to notify all California

---

protection for content, and nine others have warrant protection for GPS location tracking." *Id.*

104. *Id.*

105. *Id.* (emphasis omitted).

106. *Id.* (stating that the Electronic Communication Privacy act "requires a warrant to track the location of electronic devices").

107. CAL. CIV. CODE § 1798.83 (West 2016).

108. *Id.*; Jolly, *supra* note 49.

109. CAL. CIV. CODE § 1798.81.5(b).

110. Jolly, *supra* note 49; *see also* CAL. BUS. & PROF. CODE §§ 22575–79 (West 2016).

111. CAL. BUS. & PROF. CODE § 22575.

112. CAL. CIV. CODE § 1798.82.

residents whose data was accessed by an unauthorized third party.[113]

Massachusetts is another example of a state implementing data protection legislation.[114] The state enacted the Massachusetts Data Protection Law in 2010.[115] The Law imposes a legal obligation on companies conducting business in the state to protect the personal information of any Massachusetts resident.[116] Some of the requirements of the law include: the routine maintenance and monitoring of computer systems that process consumer data,[117] that companies only work with third parties "capable of maintaining appropriate security measures to protect such personal information,"[118] and the encryption of any consumer personal information kept on company laptops or other portable devices.[119]

The state regulations in California and Massachusetts, as well as other states which have enacted data privacy regulation and protection laws, may apply to some of the producer data collected by agricultural technology providers in those particular states.[120] However, much of the data collected through precision agriculture would not fall into the categories protected by California and Massachusetts law. The California and Massachusetts laws only cover narrow categories of personal information.[121] For example, the California Security Breach Notification law regulates personal information which it defines as a consumer's first name or initial and last name combined with the consumer's social security number, driver's

---

113. *Id.* California was the first state to enact a security breach notification law. Currently, forty-seven states have enacted laws requiring notification in the case of a security breach. *See* Jolly, *supra* note 49.

114. Kelly Todd, *Understanding the New Massachusetts Data Protection Law*, TENABLE NETWORK SEC. (Jan. 26, 2010), https://www.tenable.com/blog/understanding-the-new-massachusetts-data-protection-law.

115. *Id.*

116. *See* 201 MASS. CODE REGS. § 17.01 (2016); *see also* Todd, *supra* note 114.

117. *See* 201 MASS. CODE REGS. § 17.04; *see also* Todd, *supra* note 114.

118. *See* 201 MASS. CODE REGS. § 17.03; *see also* Todd, *supra* note 114.

119. *See* 201 MASS. CODE REGS. § 17.04; *see also* Todd, *supra* note 114.

120. Other states regulating data privacy and security include Arkansas, Connecticut, Florida, Indiana, Maryland, Nevada, Oregon and Rhode Island. *Outlook for State Data Security Laws: More than Breach Notification*, PRIVACY TRACKER (Dec. 16, 2014), https://iapp.org/news/a/outlook-for-state-data-security-laws-more-than-breach-notification/.

121. *See* Jolly, *supra* note 49; Todd, *supra* note 114.

license number, health insurance information, medical information, or an account number or bank card number with accompanying access code.[122] The Massachusetts data protection law applies to the personal information of any Massachusetts resident collected and defines it nearly the same way as California, except that a consumer's banking account number does not need to be in combination with the accompanying access code for it to be considered protected information.[123]

Some of the information collected by precision agriculture tools may fall into the categories enumerated by the above laws, such as a producer's name and financial information. However, much of it does not, such as crop yield data, fertilizer and pesticide application information, land locations, etc. Though these types of information do not fall into the usual categories of personal information that companies are legally obligated to protect, they deserve to fall into a protected category in the agriculture industry.

3. Industry Self-Regulation Attempts

Various parties in the agriculture industry have come together to establish principles for the use of producer data in the agriculture industry.[124] One coalition of entities has developed the Privacy and Security Principles for Farm Data.[125] These principles seek to standardize the way companies collecting agricultural data interact with producers.[126] The principles recommend that companies be transparent regarding the data their technology can collect, and only collect such data with the "affirmative and explicit" consent of the producer.[127] The principles recommend that transactions between producers and companies be governed by contracts, in which specific terms should be clearly defined in an understandable way.[128]

---

122. CAL. CIV. CODE § 1798.82(h)(1) (West 2016).

123. 201 MASS. CODE. REGS. § 17.02.

124. *Privacy and Security Principles for Farm Data*, *supra* note 25.

125. *See* Rodger & Thornton, *supra* note 34.

126. *See generally id.*

127. *Id.* ("An ATP's principles, policies and practices should be transparent and fully consistent with the terms and conditions in their legal contracts.").

128. *Id.* (stating that farmers will be able to "compare and contrast specific issues" in their ATP contracts).

The principles also include recommendations regarding how a company shares data with third parties.[129] They recommend that companies must disclose whom they share data with, obtain producer consent prior to sharing data, and alert producers to how they may prevent their data being shared with third parties.[130] The principles also recommend that any third party who receives shared data should be held to the same privacy standards that the company is held to in its contracts with the producer.[131]

The companies who have signed off on these voluntary principles have pledged to follow them in their business operations and interactions with producers.[132] While the FTC supports industry attempts at self-regulation, "[p]rivacy advocates sometimes criticize these structures as fig leafs and argue that they are vague and self-serving and lack real enforcement."[133] Although the principles do provide recommendations for how companies should communicate and interact with the producers from whom they collect agricultural data, they fail to set any sort of detailed, minimum guidelines for the types of data privacy security systems and procedures companies should have in place to protect producer data.[134] The biggest issue with these voluntary industry principles is, however, the hard fact that they are voluntary.

B. CURRENT DATA PRIVACY AND SECURITY REGULATIONS ARE INSUFFICIENT TO ADEQUATELY PROTECT AGRICULTURAL DATA

As discussed above, despite the protections against "unfair" and "deceptive" trade practices that the FTC provides, the FTC does not set out minimum standards for data privacy and security that companies must follow.[135] Additionally, the FTC focuses its enforcement efforts on particular types of companies

---

129. *Id.*

130. *Id.* ("Farmers must be notified that their data is being collected and about how the farm data will be disclosed and used.").

131. *Id.*

132. *Id.*; *see also Privacy and Security Principles for Farm Data*, *supra* note 25.

133. MCGEVERAN, *supra* note 76, at 178.

134. *See generally Privacy and Security Principles for Farm Data*, *supra* note 25.

135. *See supra* note 100 and accompanying text.

and magnitudes of violations.[136] Without minimum data protection standards to follow and without guidance from FTC enforcement action taken against similarly situated companies, agricultural technology providers may not be gleaning sufficient guidance from the FTC as they develop their own data privacy and protection standards. And, should their practices be insufficient but not egregiously insufficient, these companies may consider themselves to be reasonably safe from an enforcement action by the FTC.[137]

There are a number of states that regulate the data protection practices of companies doing business in their state, as discussed previously.[138] Agricultural data could fall under the protective umbrella of the laws in those particular states. However, as seen using California and Massachusetts as illustrations, much of the agricultural data collected may not fall into the categories of personal information that these laws regulate.[139] These laws also apply only to activities within their respective jurisdictions, and therefore do not provide broad regulation nationwide.[140]

In sum, companies in the agricultural industry are not likely candidates for FTC enforcement actions,[141] there are no federally mandated minimum standards for data privacy and security that apply to companies in the agricultural industry,[142] state regulation of data practices is not uniform and does not cover many categories of agricultural data,[143] and voluntary industry standards are simply that—voluntary.[144] Therefore, the current regulatory environment is not sufficient to protect sensitive agricultural data, as companies nationwide are not

---

136. MCGEVERAN, *supra* note 76, at 225.

137. Solove & Hartzog, *The FTC and The New Common Law of Privacy*, *supra* note 76, at 613 ("[G]iven the FTC's limited resources, the Commission . . . tends to target cases with a high likelihood of success and where companies have no viable defense . . . [,]" not those where companies have implemented some, albeit insufficient, data privacy and protection standards and can pose a semblance of a defense).

138. *See Outlook for State Data Security Laws: More than Breach Notification*, *supra* note 120.

139. *See supra* Part II.A.

140. *Id.*

141. *See supra* Part II.A.1.

142. *Id*.

143. *See supra* Part II.A.2.

144. *See supra* Part II.A.3.

held to any minimum standard of behavior in their data protection practices. As will be further discussed below, the current regulatory environment seems especially inefficient in light of the fact that more categories of data are personally identifiable than previously thought and techniques such as data anonymization are not as effective as previously assumed.[145]

III. SOLUTION

A solution to the current ineffectiveness of data privacy and security regulations in the agriculture industry may be federal regulation of the data practices of companies that collect agricultural data. Agricultural data is sensitive enough to warrant such precautions.[146] One source in the agriculture industry has stated that "[m]any farmers guard their data like a chef guarding a prized recipe. They've worked diligently to tweak the ingredients of their secret sauce that leads to a successful season."[147] The information collected from a farm can give third parties insight into a producer's income or the value of their land.[148] Pesticide and fertilizer application information can give environmental groups ammunition to protest a producer's farming practices or can serve as evidence of violation of the law.[149] Therefore, producers may face negative consequences should unauthorized third parties obtain their data, similar to the consequences that consumers of financial services face if their personal financial data is obtained and the consequences that health care consumers may

---

145. *See infra* Part III.

146. *See, e.g.*, Bunge, *supra* note 42 (discussing the potential business advantages if one farmer has access to a competitor's data).

147. Laurie Bedord, *2016 Commodity Classic: Data Privacy & Security Principles Encourage Use of Tools*, AGRICULTURE.COM (Mar. 9, 2015), http:// www.agriculture.com/technology/data/2016-commodity-classic-data-privacy _575-ar47862.

148. *See* Lyndsey Gilpin, *How Big Data is Going to Help Feed Nine Billion People by 2050*, TECHREPUBLIC (last visited Oct. 11, 2016), http:// www .techrepublic.com/article/how-big-data-is-going-to-help-feed-9-billion-people-by-2050/ ("If someone knows the data of an operation, they also know when and where the crops are, how much yield, how much it costs, and the farm's profits . . . [a]nd then that data is used against the farmer by being sold to a competitor or undercutting a neighbor for a better deal on land prices.").

149. *See* Mercier, *supra* note 43.

face should their private treatment data be released without permission.[150]

One argument against taking new legislative or regulatory action to protect agricultural data is that the types of data collected may not be personally identifiable (unlike, for example, medical data which must include information like an individual's height and weight).[151] This may not be correct. Although agricultural data does not fall into traditionally protected categories of personally identifiable data (PII) that other privacy and security laws focus on protecting,

> PII is an ever-expanding category. Ten years ago, almost nobody would have categorized movie ratings and search queries as PII, and as a result, no law or regulation did either. Today, four years after computer scientists exposed the power of these categories of data to identify, no law or regulation yet treats them as PII.[152]

Therefore, the idea that agricultural data does not need to be regulated because it often does not contain information traditionally considered to be highly identifiable may not be accurate, as many more types of data may be identifiable than previously realized. The argument that agricultural data should be protected can be further supported by evidence that producers themselves are worried: about not receiving adequate notice regarding data collection and use from agricultural technology providers, about their data not being adequately protected, and about data getting into the hands of unauthorized third parties.[153]

There may also be an argument that current data privacy and security regulations are sufficient because agricultural data may be protected by other means, such as anonymization.[154] However, anonymization may not be as

---

150. *See infra* notes 161–76 and accompanying text (discussing the Graham-Leach-Bliley Act).

151. Todd Janzen, *What Agriculture Can Learn from Medical Data Privacy*, AGWEB (Aug. 29, 2014), http://www.agweb.com/blog/janzen_ag_law_blog/what_agriculture_can_learn_from_medical_data_privacy_laws/ (claiming that anonymization means "a farmer wanting to share his data doesn't have to give up much privacy").

152. Ohm, *supra* note 48, at 1742 (footnote omitted).

153. *See generally* Bunge, *supra* note 42 (discussing concerns that farmers have about their data ending up with rival farmers, commodities traders or giant seed companies); Gilpin, *supra* note 148.

154. Janzen, *supra* note 151.

effective as previously thought.[155] Data anonymization has been thought to protect the sensitive information of individuals stored on company databases, and a company will often follow this process to anonymize data: "First, it will delete personal identifiers like names and social security numbers. Second, it will modify other categories of information that act like identifiers in the particular context."[156]

However, even these steps are not enough to adequately protect personal information.[157] Recent developments in reidentification techniques have made thwarting anonymization processes "easy."[158] Current privacy laws that only apply to certain categories of data but leave others unregulated open up the possibility of reidentification, which "an adversary with rich outside information can use to defeat anonymity."[159] As reidentification techniques become increasingly sophisticated, they are able to use more and more categories of data to achieve reidentification of anonymized data sets.[160]

Federal, industry-specific regulations are already in place governing the data practices of institutions in the health care industry and financial services industry: The Gramm-Leach-Bliley Act governs institutions in the financial services industry and the Health Insurance Accountability and Portability Act governs health care entities.[161] Similar federal regulation tailored for companies collecting agricultural data could effectively protect producer information.

The Gramm-Leach-Bliley Act (GLBA) is an example of an industry-specific federal regulation.[162] While the GLBA was enacted with the goal of improving the perceived lack of

---

155. *See, e.g.*, Ohm, *supra* note 48, at 1716 (noting that researchers have cast "doubt on the power of anonymization" and found its theoretical limits).

156. *Id.* at 1703.

157. *See generally* Cindy Waxer, *Precision Agriculture Yields Big Data Challenges*, DATAINFORMED (Sept. 22, 2014, 5:30 AM), http://data-informed.com/precision-agriculture-yields-big-data-challenges/ ("[H]ow can farmers make sure their highly confidential data isn't leaked, misused by vendors, or poorly anonymized when aggregated and repackaged for competitors?").

158. Ohm, *supra* note 48, at 1706–07.

159. *Id.* at 1740.

160. *Id.* at 1741.

161. 15 U.S.C. § 6801 (2012); Pub. L. No. 104-191, 110 Stat. 1936 (1996).

162. *See* Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 497 (2002).

competition on the finance industry, it also had the goal of improving the privacy and security of consumer information.[163] The legislation was the first at the federal level that established "a minimum federal standard of privacy for financial information."[164]

The GLBA instructs agencies to develop standards for financial institutions to adhere to in order to have adequate

> administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[165]

The regulations promulgated by federal agencies in enforcing the privacy requirements of the GLBA cover three broad areas: notice requirements regarding privacy policies and practices to consumers; the disclosure of consumer information to third parties; and the allowance of consumers to prevent the disclosure of their information to third parties.[166] The Act requires covered financial institutions to adhere to a number of data privacy and protection standards.[167] Regulated institutions must accurately provide notice of data collection and information sharing practices to consumers.[168] This notice must contain: what categories of information is being collected; what types of third parties the institution shares the information with; and, how the consumer can opt out of disclosure of their information.[169]

Financial institutions may only disclose personal information to a third party when the consumer has been given notice regarding the disclosure and the opportunity to prevent the information from being disclosed.[170] This requirement is subject to an exception that the institution may provide personal information to an unaffiliated third party

> to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own

---

163. *See id.* at 499.
164. *Id.* at 502.
165. 15 U.S.C. § 6801(b).
166. 16 C.F.R. § 313.1(a)(1)–(3) (2016).
167. 15 U.S.C. § 6802.
168. *Id.* § 6802(a).
169. *See id.* § 6802.
170. *Id.* § 6802(b)(1).

> products or services . . . if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.[171]

There are also exceptions for when companies do not need to disclose when entering into joint agreements to jointly offer products with other companies, or when sharing information to other institutions in anticipation of a sale, merger, or other type of transaction.[172] Additionally, financial institutions must disclose annually the institution's policies and practices regarding disclosing personal information to third parties, disclosing the information of consumers who are no longer customers, and for protecting the nonpublic personal information of consumers.[173]

The regulations promulgated by federal agencies enforcing the data security portion of the GLBA "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[174] The regulations require financial institutions to "develop, implement, and maintain a comprehensive information security program" and such programs must contain safeguards that are appropriate to that institution, taking into consideration "size and complexity," "nature and scope of [the] activities," and "the sensitivity of any customer information at issue."[175] The regulations require information security programs to contain a number of required elements including: the designation of an employee to coordinate the program; the development and implementation of safeguards to control risks identified through risk assessments; the "regular[ ] test[ing] or otherwise monitor[ing of] the effectiveness of the safeguards' key controls, systems and procedures"; the oversight of third party service providers; and the evaluation and updating of the security program following changes to a company's structure or performance of the security program.[176]

---

171. *Id.* § 6802(b)(2).
172. Cuaresma, *supra* note 162, at 504.
173. *Id.* at 503 n.43.
174. 16 C.F.R. § 314.1(a) (2016).
175. *Id.* § 314.3(a).
176. *Id.* §§ 314.4(a)–(d).

Another example of federal regulation of data practices in a particular industry is the health care industry.[177] This industry is governed primarily by the Health Insurance Portability and Accountability Act and accompanying legislation and regulations.[178] The original legislation was enacted in 1996 and intended to enhance the ability of Americans to transfer health insurance more easily, to lessen occurrences of fraud in the industry, and to improve how sensitive patient information is handled and secured.[179] There are two major rules governing institutions under HIPAA.[180] These are the "Privacy Rule" and the "Security Rule."[181] The purpose of the Privacy Rule is to regulate the transfer of sensitive health information, and to provide for penalties for institutions who do not use that information correctly.[182] The purpose of the Security Rule is to protect personal information of patients in electronic form and require institutions to adequately protect this information by setting a minimum required standard for security.[183]

Under HIPAA and its resultant regulations, regulated institutions must adhere to a number of stringent requirements.[184] The institutions must provide a statement with required language explaining to patients how their personal information may be disclosed and how they may request access to their information.[185] The institution must also correct any incorrect information upon patient request.[186]

---

177. *See generally Health Insurance Portability and Accountability Act*, CAL. DEP'T OF HEALTH CARE SERVS., http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx (last visited Oct. 9, 2016) (discussing the rationale behind, and general goals of, HIPAA).

178. *Id.*

179. *Id.*

180. Young B. Choi et al., *Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules*, 30 J. MED. SYS. 57, 57 (2006).

181. *Id.*

182. *Id.* at 58 ("Generally speaking, the Privacy Rule protects individuals' [protected health information] by dictating how and when a person's [protected health information] may be disclosed and for what reasons.").

183. *Id.* at 58–59 ("The Security Rule establishes a minimum 'floor' of security that all covered entities must insure.").

184. *See generally id.* (discussing the challenges that the health care industry faces in implementing the HIPAA requirements).

185. *See* Jolly, *supra* note 49.

186. *Id.*

While an institution may disclose Protected Health Information to facilitate treatment without written authorization from the patient, any other disclosure requires written consent.[187] When an institution does make a disclosure of Protected Health Information, it has the responsibility of disclosing the minimum amount of information necessary.[188] Furthermore, the institution must track all disclosures of Protected Health Information.[189] If an institution wishes to disclose patient data (with the exception of disclosure necessary for medical treatment) they must receive the consent of the individual before disclosure in writing, with the HIPAA Privacy Rule requiring that the consent statement include specific, mandatory language.[190]

Institutions must draft and follow their own set of privacy policies and procedures.[191] They also must appoint a Privacy Official who is responsible for overseeing these policies.[192] They must include oversight systems for management to follow and must include a list of employees or designate types of employees who have access to protected information.[193] The institution must provide training to these employees regarding handling of patient information.[194] Institutions must have a set of emergency plans in place, including the ability to recover data should an issue with their systems occur.[195] Should institutions wish to transfer patient data to third parties, they must ensure that these third parties have a system in place that would independently satisfy HIPAA requirements.[196]

Institutions must follow a set of technical standards to protect the transmission of patient health information being transferred over their networks from being intercepted.[197] They are also required to keep in place necessary physical

187. 45 C.F.R. § 164.506(a) (2016).
188. *Id.* § 164.502(b).
189. *Id.* § 164.528(d)(1).
190. Jolly, *supra* note 49 ("Consent must generally be in writing . . . . The HIPAA Privacy Rule provides specific statements that must be included in the consent.").
191. 45 C.F.R § 164.530(i)(1).
192. *Id.* § 164.530(a)(1).
193. *Id.* § 164.308(a)(3).
194. *Id.* § 164.530(b).
195. *Id.* § 164.308(a)(7)(i).
196. *Id.* § 164.502(e).
197. *Id.* § 164.312(e)(1).

safeguards to protect patient information.[198] This includes having procedures regarding installation and uninstallation of any software to the institution's network, controlling access to the institution's network, and preventing employee workstations from being visible to the public.[199]

Any future legislative or regulatory scheme put in place to protect agricultural data should take place at the federal level like those in the health care and the financial services industry. This is preferred over a piecemeal state-by-state approach because it will allow large agricultural technology providers who operate across the country to develop a single set of policies and practices to conform to the law, rather than to rely on the different approaches of each individual state.[200]

There are arguments that the federal approach to data privacy and security regulation is already too fractured with an industry-by-industry approach to federal regulation of data protection.[201] However, absent a new comprehensive federal data privacy and security scheme being put in place covering businesses collecting consumer data across all industries, an agriculture-specific law is a way to put in place minimum standards that companies collecting agricultural data must meet. An industry-specific regulation may be more effective at protecting agricultural data as rules can be promulgated by an agency that deals with agricultural issues on a regular basis and whose expertise may be helpful in designing new data privacy rules for the agriculture industry.

Where should the stringency of an agriculture industry-specific regulatory scheme fall among the spectrum of other major industry-specific data privacy and security laws and

---

198. *Id.* § 164.310(a)(1).

199. *See, e.g.*, *id.* § 164.310(c) (discussing security measures for employee workstations).

200. *See infra* note 202 and accompanying text.

201. *See* Solove & Hartzog, *The FTC and The New Common Law of Privacy*, *supra* note 76, at 586–87. For example, "[c]omparisons between privacy regulation in the United States and European Union have often pointed out E.U. law's comprehensiveness in contrast with U.S. law's fragmentation and hollow standards, which provide few limits on the collection, use, and disclosure of personal data." *Id.* at 586. *See also* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 50 (2003) (noting that many U.S. privacy statutes "rely largely on individual self-policing as the primary control mechanism" rather than following a standardized system).

regulations? Somewhere between the GLBA and HIPAA. While HIPAA is the most stringent federal data protection scheme,[202] an agricultural data protection framework likely would not need to go as far as those requirements. Laws and regulations governing companies collecting agricultural data may not need the same level of complexity in the mandated components of their data privacy and security programs, and agricultural companies should be free to develop their own programs and technical standards provided they meet certain minimum standards and include specific elements prescribed by law. This approach would more closely mirror the approach of the GLBA.[203]

However, these laws and regulations should be stricter than the GLBA in some respects. The GLBA requires notice provided to consumers regarding what information is being collected and when a financial institution desires to share information to third parties.[204] The GLBA also directs that this notice should contain certain required statements.[205] These would be positive requirements for companies collecting agricultural data because the companies would be required to provide notice to producers about their data collection practices and mandatory statements would ensure that notice would be accurate from company to company. However, the GLBA only requires financial institutions to give consumers time to "opt out" of their data being shared to third parties after receiving notice.[206] Companies in the agriculture industry should be required to obtain the affirmative consent of their customers before sending data to third parties because this would give producers greater control over their data and place a higher burden on the company to communicate effectively to producers regarding any disclosure in order to gain consent. Additionally, the GLBA contains a number of exceptions in which financial institutions do not need to notify consumers of disclosure to

---

202. Daniel J. Solove, *HIPAA Mighty and Flawed: Regulation Has Wide-Reaching Impact on the Healthcare Industry*, AHIMA (Apr. 2013), http://bok.ahima.org/doc?oid=106326#.WBQAmvkrLb0 ("In comparison to the dozens of federal privacy laws for various industries, HIPAA is one of the most comprehensive and detailed.").

203. *See* generally Cuaresma, *supra* note 162.

204. *See id*. at 503.

205. *Id*. at 503 n.43.

206. 15 U.S.C. § 6802(b) (2012).

third parties,[207] and these exceptions should not be included in any regulation covering the agriculture industry. This will ensure that a producer's data is not transmitted to a company without the producer's consent.

The GLBA also requires financial institutions to develop their own policies regarding data security and to transmit these policies to their customers.[208] While they are permitted to develop their own data security programs, the law requires them to meet specific minimum standards, monitor the effectiveness of the programs, and to change their programs in regards to changes in their business operations or inadequate performance of the program.[209] This type of regulation would work well for companies in the agriculture industry, because it would allow companies to be innovative in designing their own data security policies for their own businesses, but still puts in place a number of elements that a company is required to meet to ensure a minimum level of security is provided for the data the company collects. These elements may be customized to meet the specific needs of the agriculture industry.

CONCLUSION

Precision agriculture technology is allowing for more productive, more efficient, and more environmentally friendly agriculture. The tools of precision agriculture allow for the collection of massive amounts of producer data. However, there are currently no laws or regulations setting minimum standards that companies collecting agricultural data must meet. While the FTC has regulatory authority over these companies, its enforcement actions may not be sufficient to ensure that companies in the agriculture industry are keeping in place adequate privacy and security measures. Additionally, although some states have data privacy and security laws that would apply to companies collecting agricultural data, these laws do not cover most of the categories of agricultural data being collected.

Agricultural data is sensitive and there may be negative consequences resulting from the unauthorized disclosure of this data. Therefore, new laws and regulations should be put into

---

207. *Id.*
208. *Id.* § 6803(a).
209. *See supra* notes 174–76 and accompanying text.

place to protect it. This may be done through a new federal law and regulations specifically tailored toward data privacy and collection in the agriculture industry. In designing this new federal law and regulations, guidance may be taken from both the GLBA and HIPAA. A new federal law would provide uniform guidance for companies collecting agricultural data across the United States and provide better protection to agricultural data than the current system affords.