Journal of Food Law & Policy

Volume 11 | Number 1 Article 8

2015

Setting the Table for Feast or Famine: How Education will Play a Deciding Role in the Future of Precision Agriculture

Lauren Manning

SETTING THE TABLE FOR FEAST OR FAMINE: HOW EDUCATION WILL PLAY A DECIDING ROLE IN THE FUTURE OF PRECISION AGRICULTURE

*Lauren Manning**

I. INTRODUCTION

A. From Soil to Sky and Everywhere in Between

Precision agriculture has many names including satellite farming, or site-specific crop management.[1] Early forms of precision agriculture involved creating fertilizer maps, yield measurements, grid sampling, and soil pH content monitoring.[2] Roughly 25 years ago, the advent of global positioning systems, commonly known as GPS, enabled farmers to make more informed decisions about where to plant seed and how much seed to plant.[3] Precision agriculture technologies typically utilize sensors that are placed on tractors, combines, and other farm equipment, and which measure various conditions including seeding rates, soil conditions, and other indicators of production.[4] Over time, this technology has been expanded to provide a wide range of services like field mapping, tractor guidance, and yield monitoring.[5] These technologies also help farmers make the most efficient use of pesticides, herbicides, and fertilizers.[6] As a result, farmers are no longer forced to treat fields uniformly or to make guesses about the best courses of action for their fields.[7] Instead, precision agriculture enables farmers to micromanage their fields on a day-to-day basis, or even minute-by-minute basis, while relying on highly accurate data.[8]

Most modern day precision agriculture systems involve equipment-mounted hardware, like GPS devices, sensors, or remote equipment that is placed in the field or on farm equipment.[9] These devices collect information

---

* Lauren Manning graduated from Pacific McGeorge School of Law and practices food and agriculture law in California. She would like to thank Tad Bell and Johnny Bateman for their guidance and support.

1. Alex McBratney, et al. *Future Directions of Precision Agriculture*, 6 PRECISION AGRIC. 7, 7-23 (2005).
2. Lorelei Graham, *Precision Agriculture on the Global Stage*, NORTON ROSE FULBRIGHT (Sept. 2014), http://www.nortonfulbright.com/knowledge/publications/120848/precision-agriculture-on-the-global-stage.
3. *History of Precision Agriculture*, DELMAR CENGAGE LEARNING, http://www.delmarlearning.com/companions/content/140188105X/trends/history_pre_agr.asp (last visited Mar. 13, 2015).
4. *Id.*
5. *Official U.S. Government information about the Global Positioning System (GPS) and related topics*, GPS.GOV, http://www.gps.gov/applications/agriculture/ (last updated Nov. 25, 2014).
6. *Id.*
7. *Id.*
8. *Id.*
9. Graham, *supra* note 2.

that is sent to a software-enabled control system, which creates a variety of data sets.[10] For example, the data can be manipulated to create highly accurate field maps, or to illustrate vegetation density.[11] The GPS systems that these devices and programs utilize can provide accurate measurements down to the centimeter.[12] As a result, the geospatial maps are incredibly accurate, showing boundary markers, roads, and irrigation systems.[13] Armed with these maps, farmers can assess different areas of their fields by collecting soil samples and monitoring crop conditions.[14] Additional examples of precision agriculture technologies include automatic steering systems, precision seed planting systems, optical crop sensing technology, mobile phone and tablet applications, and yield monitors.[15]

Some Agricultural Technology Providers ("ATPs") offer farmers additional data analysis features.[16] For example, crop advisors compile the data that the GPS devices collect and interpret the data to identify an array of issues like pest infestations while also prescribing a solution for the problem.[17] This information is sometimes translated to an aircraft sprayer that sprays the affected portion of the field while leaving the unaffected areas untouched.[18] Remarkably, these prescriptions are not one-size-fits-all, and frequently isolate a specific area of a certain field.[19] A number of devices also enable farmers to make adjustments to their crop management systems with the push of a button, such as variable rate applications.[20] For example, some technologies suggest to farmers when the right time to water may be, whether irrigation is necessary, or whether a dose of fertilizer would improve crop growth.[21] The software is programmed with a catalogue of "best conditions" for a number of specific soil and plant species, which allows the optimization to be even more accurate.[22]

---

10. *Id.*
11. *Official U.S. Government information about the Global Positioning System (GPS) and related topics*, *supra* note 5.
12. Graham, *supra* note 2.
13. *Official U.S. Government information about the Global Positioning System (GPS) and related topics*, *supra* note 5.
14. *Id.*
15. Graham, *supra* note 2.
16. *Official U.S. Government information about the Global Positioning System (GPS) and related topics, supra* note 5.
17. *Id.*
18. *Id.*
19. *Id.*
20. Graham, *supra* note 2.
21. Pau Puigdollers, *5 Benefits of Precision Agriculture to Increase your Field Productivity*, IRIS (Feb. 5, 2014). http://iris.cat/5-benefits-of-precision-agriculture-to-increase-your-field-productivity/.
22. *Id.*

There are many different ways that the data collected from precision agriculture devices and programs can be utilized. For example, some ATPs offer services that analyze the data and design "prescriptions" for the farmer's land geared toward providing higher outputs and increasing profit margins.[23] Recently, multi-national corporations Monsanto and John Deere began offering data sharing services touted to help farmers increase their profits.[24] In order to participate, however, farmers must allow the companies to collect their data in real time and agree to participate in so-called big data pooling.[25] Big data is a term that can be coined as meaning the sorting and processing of extremely large amounts of data. Although farmers have shared various forms of crop data with private firms over the last several years, the technological ability to collect this data directly from a farm on a minute-by-minute basis is unprecedented.

As a result of these technologies, farmers are able to more accurately and effectively use pesticide and fertilizers, plant more accurately, and reduce crop damage.[26] Consequently, the ultimate yield for each particular field is maximized.[27] Current predictions estimate that the precision agriculture industry will grow approximately ten to fifteen percent each year between 2014 and 2019.[28] Currently, the United States is leading the world in development and implementation of these technologies with South America, Europe and Asia close behind.[29] In the United States, precision agriculture appears to be most commonly employed in corn and soybean operations, with auto-steering technology as the most common feature, while European countries have primarily utilized precision agriculture to address environmental concerns.[30]

B. A Digital Harvest and The Pests Who Prey Upon It

Unsurprisingly, there is growing concern among farmers and ranchers that their data could be obtained illegally or exploited by larger corporations and government agencies. The potential risks of agricultural data misappropriation are far-reaching for farmers and not without credence.

---

23. *See* Graham, *supra* note 2.
24. Dan Charles, *Should Farmers Give John Deere and Monsanto Their Data?*, THE SALT (Jan. 22, 2014, 4:45 PM), http://www.npr.org/blogs/thesalt/2014/01/21/264577744/should-farmers-give-john-deere-and-monsanto-their-data.
25. *Id.*
26. Graham, *supra* note 2.
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*

Given the intangible nature of digital data, once it is released into cyberspace the farmer relinquishes direct control over the information and where it goes. Marketing agencies could use this data to send a farmer smart-phone advertisements on a real-time basis that are tailored to the particular crop or fertilizer that the farmer is dealing with at the time. In recent years, growing attention has been directed toward corporations such as Facebook and Google and the issue of whether their collection of user information—with or without the users' knowledge and consent—infringes upon those users' privacy rights. For many individuals, the enjoyment and benefit they receive from using Facebook or Google outweighs the risks associated with the loss of privacy. Similarly, while some farmers deem precision agriculture and prescription services a dream come true, others see it as a threat to their privacy and business.

Some members of the agriculture community would argue that misappropriation of farm data poses even greater threats than unsolicited advertisements. The argument is that disclosing or sharing data about their operations would implicitly involve politically and socially contested issues, including pesticide usage, genetically modified products, and the treatment of livestock. As a result, opponents of agriculture data sharing would further contend that dissemination of information that reveals a farmer's particular practices poses an immediate risk to the farmer's livelihood, and perhaps his or her personhood as well. Other opponents have expressed concern that the Environmental Protection Agency or one of the many organizations that regulate agriculture may be able to subpoena individual farm data.[31] Some opponents underscore the potential for traders dealing in agricultural futures to purchase databases comprised of real-time yield data.[32] Currently, traders rely on private surveys and Department of Agriculture yield data, which reflect patterns from previous months or years.[33]

Concern over the potential misuse of precision agriculture has garnered the attention of a number of members of the United States Congress representing rural states.[34] These representatives have informed their fellow Congressional members about the growing use of precision agriculture technologies and the potential risks that unfettered data collection poses.[35]

---

31. Blake Hurst, *Big Farms Are About to Get Bigger*, AM. ENTER. INST. (Dec. 11, 2013), https://www.aei.org/publication/big-farms-are-about-to-get-bigger/.

32. *Id.*

33. *Id.*

34. *See* CONGRESSIONAL RESEARCH SERVICE, *Precision Agriculture and Site-Specific Management: Current Status and Emerging Policy Issues*, CRS REPORT FOR CONGRESS (Aug. 7, 2000), http://nationalaglawcenter.org/wp-content/uploads/assets/crsRL30630.pdf

35. *See id.*

The next several decades may witness the development and enactment of legislation that controls the relationship between farmers, ATPs and their data. Until then, many of these questions will remain unanswered.

Despite these potential dangers, the arguments in support of agricultural data collection and aggregation are wildly compelling. Proponents would argue that the benefits outweigh the risks, particularly when it comes to the potential for agricultural big data to correct imperfections in the market for farmland. Typically, information regarding soil types, weather patterns, and productivity has been limited to local communities. Access to broad-scale maps reflecting aggregate data could correct misconceptions regarding value-related matters, like land prices. Unless the maps and associated data are made publicly available, however, only the individuals and companies who own the property rights to the information would have the ability to reap its benefits

One aspect of precision agriculture that holds great promise is so-called big data pooling, which constitutes the aggregation of farm data on multiple levels.[36] Big data pooling may provide answers to some of the most threatening questions that face the global population. Undoubtedly, the growing population places tremendous demands on global food production. The ability of precision agriculture to help farmers achieve optimal working capacity and to compare productivity across a spectrum of geographical ranges may provide the method for meeting this demand. On an intra-farm level, precision agriculture can help farmers cut costs, increase yield, and address problems on a real time basis with the click of a button.

C. Sewing the Seeds of Safety and Prosperity

When it comes to data rights, the same concerns that plague consumers also inform farmers' and agricultural professionals' opinions of precision agriculture.[37] From a practical perspective, many farmers simply do not have the time or technological acumen to continually monitor the privacy, security, and control of their agricultural data.[38] As a result, farmers wishing to implement precision agriculture technologies must place a great deal of trust and blind faith in the ATP that they choose.[39] This creates an opportunity for some ATPs to potentially abuse these relationships, or to exploit this power imbalance. This is primarily true for farmers who possess

36. *See* Hurst, *supra* note 31.

37. Joseph Russo, *Data Privacy, Ownership in Precision Agriculture*, PRECISIONAG (Sep. 3, 2013), http://www.precisionag.com/opinion/joe-russo/data-privacy-ownership-in-precision-agriculture/.

38. *Id.*

39. *Id.*

only a novice, basic understanding of technology and the amorphous nature of information stored as data. Some farmers may be unaware that they have an ownership claim to the data because it does not conform to their understanding of traditional property rights, which are grounded in more tangible notions of physical possession and control. Conversely, data and digitally stored information are intangible and transported invisibly by wires and airwaves.[40]

Currently, many farmers and ATPs are taking the position that any information gathered regarding a farm or its operations remains the private property of the farm operator.[41] In order to address these growing concerns and in an effort to foster uniformity across the precision agriculture industry, a number of industry leaders joined forces and developed a set of principles that they would like to see implemented in precision agriculture contracts.[42] The Privacy and Security Principles for Farm Data agreement ("the Agreement") outlines a series of data principles that the signatories hope will be implemented in ATPs' contracts.[43] At the outset, the Agreement emphasizes the importance of ensuring alignment between an ATP's policies and practices and the contract terms it offers to farmers.[44] The Agreement highlights key principles that are intended to make farmers more comfortable with ATP service contracts so that they can make use of the benefits that precision agriculture has to offer.[45] These principles are similar to a number of guidelines currently utilized by large-scale data service providers, giving some confidence that their aim will have an impact on the future of precision agriculture.[46]

Overall, the Agreement is a respectable first effort at establishing universal policies that seek to ensure the protection of farmers' data. For precision agriculture to become the status quo and for the industry to take advantage of the benefits that it has to offer, however, substantial efforts must be undertaken to give farmers the tools that they need to hold ATPs accountable and to learn how to use these complex computer systems. Although the Agreement references the importance of educational programs, a greater call to action is needed. For example, many farmers may require legal assistance when it comes to interpreting ATPs' service contracts. On a

40. *Id.*
41. *Id.*
42. Karl Plume, *Farm Groups, Ag Tech Companies Agree on Data Privacy Standards,* REUTERS (Nov. 13, 2014), http://www.reuters.com/article/2014/11/13/us-usa-agriculture-data-idUSKCN0IX2NU20141113.
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*

practical level, many farmers are leery of adopting precision agriculture technologies because they do not have the basic technological skills required to navigate the hardware and software programs that it entails, or the acumen required to interpret the data. Accordingly, successful educational efforts will require specialists from many different backgrounds, including scientists, computer engineers, economists, and lawyers.

For now, the agreement is non-binding on ATPs, who retain the ultimate decision over which terms to include in service contracts and how to treat their customers' data.[47] While time will be the only true measure of the Agreement's success, one way to evaluate its potential effectiveness is to examine its provisions through the lens of some of the many recent data rights incidents that have been at the forefront of technological news. In today's world, there is no shortage of current events regarding data privacy rights, security breaches, and ownership battles. These events provide helpful "dos" and "don'ts" for farmers, ATPs, and their lawyers.

Part II of this article takes a closer look at the potential benefits and disadvantages of precision agriculture. Part III of this article provides a survey of recent data-related incidents and highlights three critical principles that farmers can use to evaluate a potential ATP: trust, transparency and choice. Part IV of this article examines the Agreement and its potential effectiveness through the lens of these guiding principles. Finally, Part V of this article argues that the only way to ensure the maximization of precision agriculture's benefits is by giving farmers the educational tools they need to both hold ATPs accountable and to learn how to utilize these technologies.

II. MODERN DAY PRECISION AGRICULTURE

A. Precision Agriculture in Action

One of the best ways to understand the application and benefits of precision agriculture is by considering it in action. The Rias Baixas region of Spain produces the unique Albariño grape, which is used to make a special varietal of white wine.[48] This grape has put Rias Baixas on wine connoisseurs' radar and has created a financial boom for the local economy.[49] Recognizing the promise of this grape, in 2012 the Spanish

47. Plume, *supra* note 42.

48. Javier Martinez, *Smart Viticulture Project in Spain Uses Sensor Devices to Harvest Healthier, More Abundant Grapes for Coveted Albarino Wines*, SENSORS MAG (Feb. 24, 2014), http://www.libelium.com/sensors-mag-smart-viticulture-project-in-spain-uses-sensor-devices-to-harvest-healthier-more-abundant-grapes-for-coveted-albarino-wines/.

49. *Id.*

government hired an international consulting group to launch a Smart Viticulture project that utilizes precision agriculture.[50] Part of this infrastructure update included the implementation of precision agriculture technologies, including the placement of wireless sensor devices in the vineyards.[51] The sensor's job was to monitor environmental conditions and to improve the field managers' environmental management of each vineyard.[52]

Approximately one thousand wine growers throughout the region participated in the project, and each participant's vineyards was outfitted with these sensors and devices.[53] The sensors tracked a multitude of environmental factors, like ambient temperature, soil moisture, humidity, and leaf wetness.[54] By optimizing these variables, the growers are able to enhance grape quality and to increase production capacity.[55] The data collected from these various sensors in turn allows the growers to make optimally informed decisions on a real-time basis.[56] For example, of particular concern to the Rias Baixas wine growers was the issue of phytosanitary conditions and the desire to minimize chemical treatment practices.[57]

The equipment that was installed consisted of three wireless gateways and a dozen sensors that are capable of measuring the four aforementioned parameters: soil moisture, leaf wetness, temperature, and humidity.[58] The wireless gateways collect the data recorded by the sensors and transmit it wirelessly to a Cloud.[59] The wireless gateways are equipped with GPS capabilities, which allows them to accurately record positioning and time of collection.[60] The sensors were placed strategically throughout the vineyards based on the establishment of different zones.[61]

Once in place, a computer application was developed that allowed the vineyard managers to control the system from any computer or device that was capable of connecting to the internet.[62] A statistical prediction model was also developed, which correlates weather conditions with the potential

50. *Id.*
51. *Id.*
52. *Id.*
53. Martinez, *supra* note 48.
54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*
58. Martinez, *supra* note 48.
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*

onset of disease throughout the vineyard.[63] The application is even capable of operating on a tablet.[64] Through this modality, the managers can walk through the rows of each vineyard and see the differentiation in readings as they travel past each plant.[65] Also, the system features a communications channel that facilitates the aggregation of each individual's knowledge, including the wine growers and the viticulture technicians.[66] By creating a theoretical "communal brain," the system can operate more intelligently.[67]

The results of the project were overwhelmingly positive.[68] From the initial pool of one thousand participants, roughly four hundred signed up as regular customers during the first year.[69] Throughout the region, participating wine growers reduced the use of phytosanitary applications, including fertilizers and fungicides, by over twenty percent and increased growing productivity by fifteen percent.[70] The wineries are not only more profitable, but are now operating according to environmentally sustainable practices.[71]

B. A Bounty of Benefits

As the Rias Baixas example illustrates, there are many benefits to utilizing precision agriculture, particularly when it comes to the aggregation of data at both the intra-farm and inter-farm levels. An essential feature of precision agriculture is the ability to establish standards based on real-time aggregated data from other farming operations both located within the same region and on broader, national scales.[72] A useful analogy that has been applied to this function is blood pressure.[73] One way we know whether our blood pressure is too high or too low is by comparing it to the average blood pressure readings of other people.[74] If individuals remained unwilling to share information about their blood pressure readings, we would not have enough collective data to calculate an average range.[75] Additionally, the more information that is provided, the more accurate our calculations

63. Martinez, *supra* note 48.
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. Martinez, *supra* note 48.
69. *Id.*
70. *Id.*
71. *Id.*
72. Russo, *supra* note 37.
73. *Id.*
74. *Id.*
75. *Id.*

become.[76] If participants are willing to also provide information about their age, weight, gender, and family history, we can provide people who share similar demographics with a more tailored estimation of a blood pressure range that is safe for them personally as opposed to the public at large.[77]

The same analogy applies to farming, and there can be little doubt that farmers benefit by contributing to collective data analyses.[78] If farmers nationwide provide information regarding when they planted certain crops, the type of seed that was planted, and the amount yielded at harvest, optimal planting and harvest times for particular seed hybrids could be pinpointed. On a national or global scale, if those farmers also provide information about the geographical region in which they are located, the type of soil on their land, and current weather patterns, more accurate recommendations regarding when farmers in those localities should perform certain farming functions may be identified.

The potential benefits of farm data pooling and aggregation are numerous and cannot be underemphasized.[79] For example, data pooling may help resolve many issues that plague farmers on the single-field level.[80] Community data analysis will likely enable farmers to reach quicker, more effective solutions to these problems.[81] By aggregating data, farmers can increase their breadth of knowledge.[82] As opposed to only possessing information about their individual fields, their farm, and perhaps their county of residence, farmers can access information about their state, country, and the world at large.[83] In such a vacuum, it can be difficult to know the particular meaning of a data set.[84] By comparing data or pooling data with a community of peers, the farmer will be able to glean a better, more informed understanding of his or her farming operation.[85] If restricted to the single-farm level, the data derived from those fields will possess only a finite value to the farmer.[86] When pooled with other farmers' data, however, the data value is optimized, production is optimized, and the farmer's yields are maximized.[87]

---

76. *Id.*
77. Russo, *supra* note 37.
78. *Id.*
79. Terry Griffin, Presentation, *Advantages of Aggregating Data*, CRESCOAG (July 16, 2013), *available at* http://infoag.org/abstract_papers/papers/abstract_149.pdf.
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. *See generally* Griffin, *supra* note 79.
85. *Id.*
86. *Id.*
87. *Id.*

From an economic standpoint, precision agriculture can be utilized to help farmers pinpoint with greater accuracy various optimal working capacities.[88] For example, one of the highest cost variables for many farmers is fertilizer.[89] Precision agriculture allows farmers to more accurately disperse fertilizer and reduces unnecessary waste of this expensive product.[90] The second-highest cost for farmers is seed.[91] Seed planting technologies that rely on GPS guidance systems and variable seed rate technology provide farmers with more accurate planting.[92] This means that seed waste is reduced and total crop yield is increased.[93] Additionally, auto-steering technologies cut down on fuel costs by ensuring that equipment is operated in the most efficient manner.[94] Farm equipment that is operated according to auto-steering or guidance technologies requires significantly lower fuel consumption than unguided machines.[95] There are also the obvious benefits of being able to obtain various types of data, like soil moisture content or vegetation density in real time.[96] The maximization of efficiency across these spectrums frees up the farmer to turn his or her attention to other things, while also reducing operator fatigue.[97]

When it comes to water, ATPs may be able to provide assistance to drought-stricken regions like California.[98] Precision agriculture offers the ability to measure water usage and water quality, and to identify potential avenues for making agricultural water usage more effective.[99] In fact, with the recent implementation of California's Sustainable Groundwater Management Act, precision technologies may soon become the regional standard.[100]

On a broader scale, precision agriculture may provide part of the answer to addressing the rapidly growing global population and the

---

88. *Official U.S. Government information about the Global Positioning System (GPS) and related topics*, *supra* note 5.

89. Graham, *supra* note 2.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. Graham, *supra* note 2.

95. *Id.*

96. Puigdollers, *supra* note 21.

97. Graham, *supra* note 2.

98. Sarah Gonzalez, *Ag Companies, USDA, Discuss Big Data Challenges*, AGRI-PULSE (Feb. 19, 2015), http://www.agri-pulse.com/Ag-companies-USDA-discuss-big-data-challenges-02192015.asp.

99. *Id.*

100. *Id.* The Sustainable Groundwater Management Act requires the creation of a groundwater management plan for most of California's groundwater basins by the year 2020 with the goal of reaching sustainability by 2040. *Id.*

increased production capacity demands that this creates.[101] With the world population projected to reach 9.6 billion people by 2050, the agriculture industry will be faced with an increase in production demand of approximately seventy percent of current levels.[102] Precision agriculture will likely serve a crucial role in meeting that demand.[103] For example, some of the primary issues facing the increasing global food demand are the limited availability of arable land for crops and the urbanization of rural and agricultural areas.[104] The diminishing availability of farmland puts a premium on existing farms and creates mounting pressure to ensure that farm production efficiency and field usage is maximized.[105] Precision agriculture and data pooling may provide farmers with the tools they need to accomplish this task.[106]

C. A Plague of Pitfalls

Many unanswered questions and potentially unidentified issues surrounding the use and benefits of precision agriculture lurk in its future.[107] According to the Open Ag Data Alliance ("OADA"), current precision agriculture practices suffer from an array of issues.[108] For example, the concerns regarding the ownership of agricultural data and the implications of deciding this question remain unanswered.[109] From a financial standpoint, implementing precision agriculture is expensive, both in terms of the cost of the physical equipment and maintaining the business relationship.[110] Undoubtedly, some farmers may face legal expenses should they reach a disagreement with their ATP regarding a particular aspect of their data rights.[111]

An additional concern and potential roadblock to the development of precision agriculture is the current inability to collect data from all aspects

---

101. *The Global Food Challenge*, CEMA, *available at http://www.cema-agri.org/page/global-food-challenge* (last visited Mar. 10, 2015).
102. *Id.*
103. *Id.*; Cema Agri, *Cema Animated Story on the Global Food Challenge*, YOUTUBE (Dec. 5, 2013), http://www.youtube.com/watch?v=wHMC2T_L_3m.
104. *The Global Food Challenge*, *supra* note 101.
105. *Id.*; Cemi Agri, *supra* note 103.
106. *The Global Food Challenge*, *supra* note 101; Cemi Agri, *supra* note 103.
107. *To Help Farmers Access and Control Their Data*, OPEN AG DATA ALLIANCE, http://openag.io/about-us/ (last visited Mar. 10, 2015) [hereinafter *Data Control*].
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*

of a farm and pool it in one location.[112] Currently, no ATP provides the ability to assess every single type of operational data on a farm.[113] From an inter-farm, broad scale data pooling perspective, it seems that the more participants that opt in, the better and more accurate the information will be.[114] Stated differently, the possibility and success of this benefit is tied directly to the ability to pool all of the data in one place for analysis.[115] With accurate information about growing patterns, soil quality, and other factors, farmers will be able to produce more robust and successful crops.[116] One potential solution to this problem is to place the burden on farmers to release their data for pooling purposes.[117] For many farmers, however, the risks of sharing their data outweigh these potential benefits.[118] Until more farmers opt in, or regulations are put in place that dispel the farmers' apprehensions about participating, the accuracy and robustness of the data will continue to fall short of reaching its full potential.[119]

At the intra-farm, single operation level, a farmer needs to be able to integrate the many types of data that his equipment yields.[120] The mountains of data that precision agriculture technologies create, including reports, charts, logs, images, and spreadsheets, can be overwhelming.[121] Many farmers, especially those from older generations, simply do not have the time or acumen to interpret this data and cross-reference between different analytical platforms.[122] In general, younger generations tend to be more comfortable around technology and experience less difficulty in learning how to operate it than older generations.[123] Ideally, hardware and software systems would communicate directly and share information to provide a more synthesized end result for the farmer to rely upon when making decisions about his or her farm.[124]

---

112. Cindy Waxer, *Precision Agriculture Yields Big Data Challenges*, DATA-INFORMED (Sept. 22, 2014), http://data-informed.com/precision-agriculture-yields-big-data-challenges/.
113. *Data Control*, *supra* note 107.
114. *See* Waxer, *supra* note 112.
115. *Id.*
116. *Id.*
117. *See* Russo, *supra* note 37.
118. *Id.*
119. Waxer, *supra* note 112.
120. *Data Control*, *supra* note 107.
121. *Id.*
122. Graham, *supra* note 2.
123. *Id.*
124. *Data Control*, *supra* note 107.

To address these roadblocks, OADA has taken the laboring oar on developing a safe and reliable means for farmers to aggregate their data.[125] OADA is in the process of developing a series of open application programming interface(s), or APIs, that will enable farmers' hardware and software devices to communicate directly through a secure cloud network.[126] These open APIs are compatible with a broad range of devices, regardless of the device manufacturers.[127] Recent reports have also indicated that OADA is in the process of developing guidelines to help ensure compliance with regard to OADA principles.[128]

In addition to the problems plaguing the practical application of precision agriculture technologies, even more unanswered questions arise in the context of data rights. Like many other sectors, the agriculture industry is no stranger to the impact of data security breaches. In March 2014, for example, Monsanto's Precision Planting unit suffered a data security breach that exposed the personal data of 1,300 employees and customers.[129] Monsanto discovered that on March 27, 2014, an unauthorized party had accessed Monsanto's Precision Planting servers.[130] Precision Planting is a form of precision agriculture technology, which promises the maximization of field usage by monitoring seed spacing and depth control.[131] The system contains a number of files including customer names, addresses, financial account information, and tax identification numbers.[132] Monsanto indicated that it was not aware of any misuse of the data and offered the affected customers complimentary one-year credit monitoring services.[133] On a broader scale, Monsanto increased the data security measures it uses to thwart future breaches and adopted new security protocols.[134] Monsanto acquired Precision Planting in 2012, and purchased a similar company called Climate Corp. in 2013.[135]

---

125. Waxer, *supra* note 112.
126. *Id.*
127. *Id.*
128. *Id.*
129. Jack Kaskey, *Monsanto's Data Security Breached at Precision Planting*, BLOOMBERGBUSINESS (May 29, 2014), http://www.bloomberg.com/news/articles/2014-05-29/monsanto-data-security-breached-at-precision-planting.
130. *Id.*
131. *Manage Your Farm*, PRECISION PLANTING, http://www.precisionplanting.com/#/ (last visited Mar. 11, 2015).
132. Kaskey, *supra* note 129.
133. *Id.*
134. *Id.*
135. *Id.*

As part of Climate Corp.'s new security protocols, the company offered a data storage service that acts as an off-farm computer for farmers to keep their data.[136] Farmers can share the data with others or delete it from the system at any time.[137] According to Climate Corp., the data will not be accessed by anyone unless the farmer gives express permission.[138] In some instances, Climate Corp. may request usage of a particular farmer's data for the purpose of enhancing certain services the company offers or to research certain issues such as fertilizer application.[139] In order to ensure that farmers' privacy rights are protected, Climate Corp. and Monsanto employed the services of a third-party auditor to provide a neutral assessment of whether their practices are fair and whether any data misuses are occurring.[140] The new data policy encompasses many of Monsanto's corporations, including FieldScripts, Climate Basic, and Climate Pro.[141]

Outside the realm of privacy rights and security breaches, some farmers may find themselves in a protracted tug-of-war with an ATP over the ownership rights to his or her farm data. In general, data ownership entails possessing the legal rights to, and complete control over, the information in question.[142] With legal rights and control, comes the ability to modify, edit, share, and restrict access to the data, and the right to transfer or assign some or all of these privileges to another party.[143] The farmer or ATP who holds these ownership rights can also exercise them in defense to any illegitimate use or access of the information.[144] Although some data sets may seem like they would not hold much intrinsic value, like a person's wearable fitness tracker or Facebook account, the aggregation of these data sets can provide a fairly robust and accurate view of an individual's life—or farming operation.[145] Acquiring ownership of multiple data sets would provide many

136. Willie Vogt, *Climate Corp, Monsanto Lay Out New Data Privacy Policies*, FARM INDUSTRY NEWS (Mar. 6, 2014), http://farmindustrynews.com/precision-farming/climate-corp-monsanto-lay-out-new-data-privacy-policies.
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. Vogt, *supra* note 136.
142. *Data Ownership*, TECHNOPEDIA, http://www.techopedia.com/definition/29059/data-ownership (last visited Mar. 11, 2015).
143. *Id.*
144. *Id.*
145. Alex Hern, *Sir Tim Berners-Lee Speaks Out on Data Ownership*, THE GUARDIAN (Oct. 8, 2014) http://www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership.

companies with a competitive edge or a sneak peek into their competitors' practices.

In the context of precision agriculture, data ownership has raised a number of issues, particularly when it comes to farm prescription services.[146] For example, Monsanto's prescription service requires farmers to transmit the data that Monsanto's precision agriculture equipment is recording to Monsanto's cloud-based service.[147] Monsanto then analyzes the data and provides the farmer with information regarding how to improve his or her operations.[148] The right combinations of data can be extrapolated to determine the specific fields in which the farmer should plant the most seed due to the ideal soil conditions versus areas in which he should plant fewer seed in order to reduce sunk costs.[149] Due to GPS capabilities, Monsanto can provide these recommendations with shocking specificity, often providing measurements down to the foot.[150] Although this creates incredible gains in terms of crop yield and economic efficiency, it creates a substantial gray area regarding who owns the data that is stored in Monsanto's cloud.[151] If Monsanto is able to acquire a substantial market share for prescription technology, it will also be able to make well-founded predictions regarding farm property values.[152] It would also allow Monsanto to forecast crop yields and pricing fluctuations, which would create untold advantages for Monsanto as one of the world's largest seed providers.[153]

Each of these potential issues must be viewed in light of the ever developing and changing landscape of precision agriculture. Each day, new innovations are announced and the bar is set higher and higher for ATPs. For example, many companies are exploring the use of unmanned aviation vehicles ("UAVs") in agriculture.[154] At present, the United States government has tasked roughly six research facilities with developing and evaluating the future of UAVs in agriculture.[155]

---

146. Daniel Burrus, *Who Owns Your Data?*, WIRED, http://www.wired.com/2014/02/owns-data/ (last visited Mar. 11, 2015).
147. *Id.*
148. *Id.*
149. *Id.*
150. *Id.*
151. Burrus, *supra* note 146.
152. *Id.*
153. *Id.*
154. Graham, *supra* note 2.
155. *Id.*

III. LEARNING FROM THE PAST

Over the last several decades, major technology companies, like Google and Apple, as well as several healthcare providers, have endured countless highly public events involving unauthorized access of user data. As these recent events suggest, the realm of data privacy, security, and ownership is becoming increasingly complex.[156] The Identity Theft Resource Center ("ITRC") organizes data breach statistics in a number of ways, including the type of incident.[157] Categories of data breach incidents include: insider theft, hacking, data on the move, accidental exposure, subcontractor liability, employee negligence, and physical theft.[158] As this array of categories suggests, data is susceptible to wrongful procurement in many different ways—even those that are arguably innocent.

The information age has spawned a host of technologies designed to make the world a more efficient place to live. For example, we can send messages instantaneously via email and text, we can check our bank accounts in a matter of seconds, and we can store vast amounts of data on a thumb drive device, which is no larger than a box of matches. Doctors have access to patient health records from various healthcare facilities, our telephone companies can provide us with records of nearly every single telephone call that we've made, and financial institutions can move our money in the blink of an eye.[159]

But with the inherent benefits of these new technologies come equal, if not greater, dangers. Many of these transactions require us to provide some sort of information or even to establish an account with the service provider. At the very minimum, this usually entails creating a username, password, and providing an email address for verification purposes. On the other end of the spectrum, we may be required to provide our social security number, address, telephone number, and employer information. The aggregation of these transactions and accounts creates a stockpile of ready information for would-be hackers and identity thieves, and creates mounting concern for consumers.

The potential repercussions of suffering a security breach, a privacy violation, or data misappropriation on a personal level are tremendous. When it lands in the wrong hands, financial information can be used for

---

156. *ITRC Breach Statistics 2004 – 2014*, IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/ITRC-Surveys-Studies/2008-data-breaches.html (last visited Mar. 3, 2015).

157. *Id.*

158. *Id.*

159. *What is Mobile Check Deposit?*, FIND A BETTER BANK, http://www.findabetterbank.com/mobile_check_deposit.html (last visited Mar. 2, 2015).

identity theft and fraud. Additionally, medical records frequently contain deeply personal information that, if exposed, could irreversibly damage an individual's life. And once this data is released into the cyber world, there is usually no way to retrieve it, or to remove it from the wrongdoer's possession. As the following examples illustrate, when it comes to the high-stakes game of data rights, farmers must ensure that any ATP with whom they contract adheres to the policies of transparency, trust, and choice.

A. Privacy Rights Rumbles

In any instance where personal information or sensitive data is collected and stored, whether it is digitally or in hard copy, a potential privacy concern arises.[160] The primary concern with data privacy is creating a way to share the data with appropriate recipients while protecting it from prying eyes or falling into the wrong hands.[161] There are a number of fields in which privacy rights have become a central component, including social media, healthcare, education, criminal justice, and cell phones. In some of these fields, like healthcare, laws prohibit companies from using the data for any ulterior purpose.[162] For example, an employer is prohibited from using information collected about its employees' health for the purpose of charging smokers with higher insurance rates.[163] Additionally, cloud-computing technology has given rise to a host of new privacy concerns and issues.[164] The simple act of placing your data into the cloud server involves a third party who has access to your information.[165] Many cloud computing providers sub-contract with other companies for various services, which further expands the network of individuals who have access to private data.[166]

The following examples illustrate how critical it is for service providers to be completely transparent when it comes to their data privacy policies. Without transparency, users will lose all trust in the service provider and will likely take their business elsewhere. An additional aspect of building this trust includes providing users with options when it comes to how their data is used, stored, and manipulated. Providing users with this choice will ensure

160. Vic Winkler, *Cloud Computing: Data Privacy in the Cloud*, TECHNET MAGAZINE (Aug. 2012), https://technet.microsoft.com/en-us/magazine/jj554305.aspx.
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.*
165. Winkler, *supra* note 160.
166. *Id.*

that they have a substantial, if not final, say in who is authorized to access their data.

1. Uber

Rideshare company Uber faced public backlash after a news report revealed that company leaders were considering accessing users personal information, like ride location data, to identify journalists who report on Uber's activities.[167] To quell the public backlash, Uber released a new data privacy statement, which, in part, delineated the circumstances in which Uber employees are permitted to access user data.[168] Examples include facilitating payment transactions for drivers, monitoring accounts for fraudulent activity, and addressing issues brought to Uber's attention by its collective user base.[169]

2. Gmail

In Spring 2014, Google updated the Gmail privacy terms and conditions.[170] According to the modified terms of use, any information that users submit, or share with the Gmail system, is considered fair game for not only Google's review, but its associates as well.[171] As emails are sent and received, Gmail scans and indexes the emails.[172] Part of this service is designed to organize a user's inbox and prioritize emails that might be more important to the user.[173] Information gleaned from the scan, however, is also used to provide tailored advertising and serve other marketing based purposes.[174] More specifically, one of the updated terms states:

Our automated systems analyse your content (including emails) to provide you personally relevant product features, such as customised search results, tailored advertising, and spam and malware detection. The analysis occurs as the content is sent, received, and when it is stored.[175]

---

167. Paul Carr, *Amid Escalating Scandal, Uber Publishes New Data Privacy Statement*, PANDODAILY (Nov. 18, 2014), http://pando.com/2014/11/18/amid-escalating-scandal-uber-publishes-new-data-privacy-statement/.

168. *Id.*

169. *Id.*

170. Dave Neal, *Google Admits It's Reading Your Emails*, THE INQUIRER (Apr. 15, 2014), http://www.theinquirer.net/inquirer/news/2340003/google-admits-its-reading-your-emails-because-advertising.

171. *Id.*

172. *Id.*

173. *Id.*

174. *Id.*

175. Neal, *supra* note 170.

Some users were so outraged by Gmail's prying eyes that they filed a federal lawsuit in California, alleging that Google violated users privacy rights.[176] Google ultimately reached a confidential settlement with adult plaintiffs, leaving claims that Google violated minors' privacy rights still up for dispute.[177] The litigation faces a significant hurdle, however, following a decision from the United States District Court Judge assigned to the case, who denied class certification, finding that the potential class' claims were too dissimilar to be grouped together.[178] The Ninth Circuit Court of Appeals denied the consumers' appeal seeking review of the class certification denial.[179]

3. OnStar

In 2011 General Motors ran into trouble with its OnStar GPS system, a subscription service that provides a number of safety and connectivity features.[180] The OnStar feature provides two-way communication between the vehicle occupants and OnStar's remote support location.[181] For example, if an OnStar supported vehicle is involved in a collision, the occupants can contact OnStar by pushing a button on their dashboard, and OnStar will then send help to the vehicle's exact location using GPS.[182] Many users expressed their concern about the potential dangers of the two-way system and the ability for OnStar or General Motors to track vehicles without the owners' permission.[183]

---

176. Alexei Oreskovic, *Google Explains Exactly How it Reads all Your Email*, HUFFINGTON POST (Apr. 14, 2014), http://www.huffingtonpost.com/2014/04/15/gmail-ads_n_5149032.html.

177. Wendy Davis, *Google Settles Portion of Lawsuit About Gmail Ads*, MEDIA POST (May 28, 2014), http://www.mediapost.com/publications/article/226815/google-settles-portion-of-lawsuit-about-gmail-ads.html#.

178. Jonathan Stempel, *Google Won't Face Email Privacy Class Action*, REUTERS (Mar. 19, 2014), http://www.reuters.com/article/2014/03/19/us-google-gmail-lawsuit-idUSBREA2I13G20140319.

179. Mealeys, *9th Circuit Denies Appeal Of Class Certification Denial In Gmail Privacy Case*, LEXISNEXIS LEGAL NEWSROOM (May 13, 2014), http://www.lexisnexis.com/legalnewsroom/mealeys/b/newsheadlines/archive/2014/05/13/mealey-39-s-litigation-procedure-9th-circuit-denies-appeal-of-class-certification-denial-in-gmail-privacy-case.aspx.

180. John R. Quain, *Changes to OnStar's Privacy Terms Rile Some Users*, N.Y. TIMES (Sep. 22, 2011), http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users/?_r=0.

181. *Id.*

182. *Id.*

183. *Id.*

In response to these growing concerns, General Motors made two changes to its OnStar policies.[184] The first change consisted of OnStar notifying its users that the two-way system would remain active following termination and that vehicles could be tracked through the system.[185] The second modification clearly notified users that OnStar may share the information it collects, including odometer readings, vehicle speed and location, seat-belt usage and air-bag deployment incidences, with third parties regardless of whether the user is a current OnStar subscriber.[186] In light of these policies, OnStar provided users who wish to cancel their service with the option of completely shutting down the two-way communication service following cancellation.[187] However, the default setting leaves the connection open, allowing OnStar to continue collecting data.[188]

B. Security Breach Blunders

A data breach results where "sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so."[189] A data breach can occur in a number of situations and can target a wide range of data types, including financial information, like debit card PIN numbers, health care information, corporate trade secrets, and intellectual property.[190] The accumulation of thousands or even millions of individuals' private information into one digital location can be analogized to taking that same individuals' money and storing it in a vault.[191] Like the vault, the digital file containing the data creates a target for hackers and other wrongdoers.[192] As a result, it is necessary to employ belt-and-suspenders security measures to thwart them.[193] In some contexts, this amounts to quite a feat.[194] Consider a college-level university, for example, which must

184. *Id.*
185. Quain, *supra* note 180.
186. *Id.*
187. *Id.*
188. *Id.*
189. Afrah Fathima and Badiuddin Ahmed, *Making Data Breach Prevention a Matter of Policy in Corporate Governance*, 2 Int'l J. of Sci. Engineering & Tech. 01, 01-07 (Jan. 1, 2013).
190. *Id.*
191. John Breyault, *Your Passwords Are Like Money In a Bank Vault: Column*, USA TODAY (Aug. 7, 2014), http://www.usatoday.com/story/opinion/2014/08/06/password-theft-cybercrime-column/13678023/.
192. *Id.*
193. *Id.*
194. *See* Fathima & Ahmed, *supra* note 189, at 1.

provide an open network, carry a massive amount of data, provide numerous access points, and support countless devices, like laptops and cell phones.[195]

It seems like each month news reports surface regarding another data breach incident, creating widespread apprehension regarding the safety of the personal information that we share with our doctors, teachers, banks, and social media outlets.[196] For many large companies, ensuring data security also becomes a matter of cost.[197] To employ the type of large-scale security protection measures that national corporations require is costly.[198] In many instances, the cost of employing certain security measures is weighed against the potential cost of enduring a security breach.[199]

There are a multitude of hackers who prey on sensitive data, including malicious insiders and well-meaning employees who make mistakes.[200] In the case of the well-meaning insider, a company must monitor the user's activity in order to identify, stop, and investigate suspicious activity.[201] A 2008 study revealed that eighty-eight percent of data breaches resulted from the negligence of an employee.[202] When it comes to the malicious insider, the company faces a more difficult task of attempting to thwart them before they can carry out the breach.[203] Unfortunately, the nature of a data breach will usually put the company in a reactionary posture.[204] Once the bank robbery has occurred, the bank's only option is to regain as much of the stolen money as possible, apprehend the perpetrator, and analyze the breach in order to make its security system stronger against a similar attack in the future.[205]

The following examples highlight the serious threat that data security breaches pose and the many different considerations that both users and service providers must make when choosing a particular service or security method. Additionally, it is critical to use multiple layers of security

---

195. *Id.*
196. *Id.*
197. *Id.* at 4.
198. Fathima & Ahmed, *supra* note 189, at 4.
199. Danny Yadron, *Companies Wrestle With the Cost of Cybersecurity*, WALL STREET JOURNAL (Feb. 25, 2014), http://www.wsj.com/articles/SB10001424052702304834704579403421539734550.
200. Fathima & Ahmed, *supra* note 189, at 2.
201. *Id.*
202. *Id.*
203. *Id.*
204. *Id.* at 3.
205. Kate Vinton, *How Companies Can Rebuild Trust After a Security Breach*, FORBES (Jul. 1, 2014, 9:29 AM), http://www.forbes.com/sites/katevinton/2014/07/01/how-companies-can-rebuild-trust-after-a-security-breach/.

measures, like passwords, antivirus software, and diligent monitoring.[206] In some cases, however, even the most elaborate security systems suffer a breach, which raises important concerns regarding the steps that users and service providers must take in the wake of unauthorized access to sensitive data.[207] Similar to privacy violations, users must place a great deal of trust in the service providers that they choose when it comes to protecting their data. Service providers who provide users with transparent information regarding the security of their data will foster this sense of trust, and make users feel comfortable with choosing to share their information with the service provider.[208]

1. HealthNet

California-based insurance company Health Net announced in 2011 that it suffered a privacy breach resulting in nearly two million of its customers' personal information being exposed.[209] The data, including social security numbers, addresses, names, and financial information, was stored in an unencrypted format on hard drives that went missing from a data center with whom Health Net contracted.[210] Connecticut filed a lawsuit against Health Net, seeking to enforce HIPAA privacy laws.[211] In 2009, Health Net suffered a similar breach, losing social security numbers and medical information for approximately one-and-a-half million policyholders, which was stored on a portable hard drive device in direct contravention to Health Net's policies.[212] Many policyholders and the public at large were shocked to learn that Health Net waited over six months before reporting that the information had gone missing.[213]

---

206. Bianca Male, *10 Essential Data-Security Measures Every Business Should Take*, BUSINESS INSIDER (Jun. 8, 2010, 11:08 AM), http://www.businessinsider.com/10-essential-data-security-measures-every-buiness-should-take-2010-6?op=1.

207. *BBB Offers Advice On What To Do After a Data Breach Compromises Your Identity*, COUNCIL OF BETTER BUSINESS BUREAUS (Feb. 5, 2015) http://www,bbb.org/council/news-events/news-releases/2015/02/bbb-offers-advice-on-what-to-do-after-a-data-breach-compromises-your-identity/.

208. Vinton, *supra* note 205.

209. Harley Geiger, *HHS Should Require the Encryption of Portable Devices to Curb Health Data Breaches*, CTR. FOR DEMOCRACY & TECH. (Mar. 16, 2011), https://cdt.org/blog/hhs-should-require-the-encryption-of-portable-devices-to-curb-health-data-breaches/.

210. *Id.*

211. Emily Berry, *Connecticut Sues HealthNet Over Data Security Breach*, AM. MED. NEWS (Feb. 1, 2010), http://www.amednews.com/article/20100201/business/302019958/7/.

212. Geiger, *supra* note 209.

213. *Id.*

As the Health Net case suggests, data stored on a portable device is susceptible to physical theft as well as digital theft.[214] Devices like thumb drives, laptops, and external hard drives are commonly used in a variety of business settings, and are often no larger than a box of matches or deck of cards, making them easy to slip into an employee's pocket or briefcase.[215]

2. iCloud

In the fall of 2014, Apple's iCloud suffered a major security breach.[216] Several news sources reported that at least one hacker had breached Apple's iCloud security measures and illegally obtained hundreds of photographs from celebrities' cell phones, many of which were personal and intimate in nature.[217] After conducting an investigation, Apple issued a statement claiming that the breach was not the result of an attack on the iCloud system, but was the result of hackers' concerted efforts to identify celebrities' user names and passwords.[218] Many journalists criticized this statement as placing blame entirely on users instead of the statement's suggestion that Apple iCloud accounts are easy to hack with the right tools.[219]

Apple's iCloud, which is categorized as a "cloud computing technology," allows users to upload a wide range of content, including files, music, pictures, word documents, etc., to a remote location.[220] Having the files stored remotely allows users to access the files from multiple sources like their computers, cell phones, tablets, and other devices.[221] One of the most attractive components of Apple's iCloud is that it is integrated with virtually all of Apple's software products, offering instant and streamlined usage.[222] This integration can be expanded to encompass Apple devices used by other family members or friends as well.[223] Additionally, in the event of

214. *Id.*
215. *Id.*
216. Charles Arthur, *Naked Celebrity Hack: Security Experts Focus on iCloud Backup Theory*, THE GUARDIAN (Sep. 1, 2014), http://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence.
217. *Id.*
218. Steve Kovach, *We Still Don't Have Assurance From Apple that iCloud is Safe*, BUSINESS INSIDER (Sep. 2, 2014), http://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9.
219. *Id.*
220. Stephanie Crawford, *How the Apple iCloud Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/cloud-computing/icloud.htm (last visited Mar. 2, 2015).
221. *Id.*
222. *Id.*
223. *Id.*

a computer crash, iCloud safely restores all of your data and files to your device.[224]

Despite the apparent benefits of using cloud-computing technology, there are many dangers as well.[225] For example, uploading your personal content to a remote system requires the user to relinquish ultimate control over the information.[226] The only way to be entirely sure that information remains secure is to forgo sharing that information with another individual or system.[227] The very act of uploading a file to the cloud requires a data transfer, which renders the information a prime target for data hackers.[228] Although Apple employs encryption programs, which scramble your information along its journey to the cloud with the intent of thwarting would-be hackers from stealing it, it is not infallible.[229] As the fall 2014 scandal indicates, hackers can focus their efforts on deciphering your password by using software programs and algorithms designed to run thousands of different potential password combinations based on easily collectible personal information, such as your birthday, your pet's name, or the city where you were born.[230]

3. Target Brands, Inc.

A security breach can occur even if a company is employing a variety of security measures and monitoring its data systems. In 2013, for example, retail giant Target Brands, Inc. ("Target") suffered a hacking event that exposed roughly forty million customers' credit card and debit card accounts.[231] The hackers infiltrated Target's system to acquire information known as "track data," which enables the hackers to create counterfeit credit cards and debit cards by encoding the stolen information onto a dummy

224. *Id.*
225. John W. Rittinghouse & James F. Ransome, *Cloud Security Challenges*, INFO. SYS. SEC., http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm (last visited Mar. 12, 2015).
226. *Id.*
227. *Id.*
228. *Id.*
229. *iPhone Encryption Stops FBI, But Not This 7-Year-Old*, CNN WIRE (Dec. 1, 2014), http://fox4kc.com/2014/12/01/iphone-encryption-stops-fbi-but-not-this-7-year-old/.
230. Adrian Kingsley-Hughes, *The Dangerous Side of Apples iCloud*, FORBES (Aug. 4, 2012), http://www.forbes.com/sites/adriankingsleyhughes/2012/08/04/the-dangerous-side-of-apples-icloud/.
231. *Sources: Target Investigation Data Breach*, KREBS ON SECURITY (Dec. 18, 2013), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

magnetic stripe.[232] Analysis of the breach has revealed a number of possible methods that the hackers employed to breach Target's system.[233] For example, by performing a Google search, a hacker may have been able to locate Target's Supplier Portal, which provides information for new and existing vendors on how to submit invoices and complete other interactions with Target.[234] Google also reveals information regarding maintenance and refrigeration companies with whom Target has done business in the past.[235]

Some studies have concluded that the hackers may have preyed upon a number of these third-party vendors in order to find a theoretical backdoor into Target's data stores.[236] Many of these third-party vendors do not employ sufficient security measures, including email-scanning software that scans each email to determine whether it contains malware or any other harmful viruses.[237] It is quite possible that one of Target's vendors opened one of the hackers' emails, which would have planted the bug on the vendor's computer system and provided the hackers with a route into Target's systems.[238]

As this example illustrates, even when a company is employing substantial security measures, interactions with third parties pose serious threats to the security of users' data. Many of these consumers remain entirely unaware of the relationship between the company, i.e., Target, and the third-party vendor.[239] Even if they are aware of the relationship, there is very little that the user can do to ensure that the third-party vendor is utilizing appropriate security measures, or to ensure that the service provider is monitoring each vendor.

C. Whose Data is it Anyway?

One of the most critical questions on users' minds, and particularly popular in discussions regarding precision agriculture, is the extent to which a user retains ownership and control of the data that it exchanges with a data service provider or ATP. Assuming that a user has authorized a service provider, whether it is Gmail, Facebook, a health insurer, or an ATP, to access certain information, under what circumstances can the service

232. *Id.*
233. Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.
234. *Id.*
235. *Id.*
236. *Id.*
237. *Id.*
238. Kassner, *supra* note 233.
239. *Id.*

provider disseminate that information to third parties? Several incidents of data ownership dust-ups have occurred in the realm of social media services, and as the following examples suggest, data ownership is a relatively new subject with many complexities.

1. Facebook Apps

In 2010, Facebook admitted that its top ten most popular application programs, known as "apps," sold user data to advertisers and internet tracking companies, including user names' and users' friends' names.[240] The information transmitted included Facebook identification numbers, which can be used to locate each user's name despite any security settings the individual has chosen on Facebook.[241] For some, the user identification number will reveal the user's age, location, occupation, and photographs.[242] These apps are rarely created by Facebook, but are instead developed by independent companies.[243] Some application developers claimed to be unaware that their programs were inadvertently collecting and disseminating user information.[244] Other developers were fully aware of these activities.[245] For example, one of the brokers in possession of Facebook user data, RapLeaf, Inc., was caught linking the user identification numbers with its own databases.[246] As part of its response to the situation, Facebook banned the app developers from accessing Facebook communication channels for six months and required the developers to submit their data practices to a substantial audit as a condition of future use.[247]

2. Path

Social media networking application Path was the subject of considerable public scrutiny in 2012 when a Singapore-based developer discovered that the app was uploading its users' address books to its

240. Jacqui Cheng, *Facebook Punishes App Developers Found Selling User Data*, ARS TECHNICA (Nov. 1, 2010), http://arstechnica.com/business/2010/11/facebook-punishes-app-developers-found-selling-user-data/.
241. Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, THE WALL STREET JOURNAL (Oct. 18, 2010), http://www.wsj.com/articles/SB10001424052702304772804575558484075236968.
242. *Id.*
243. *Id.*
244. *Id.*
245. Cheng, *supra* note 240.
246. *Id.*
247. *Id.*

servers.[248] The application's Terms of Use omitted any reference to this phonebook siphoning, and while the application featured an opt-out feature for the Android platform, the iOS version of the app did not.[249] Path is a social media application that allows users to share information with a network of individuals who they consider to be their closest friends and family.[250]

Many social media platforms, like Path, subscribe to the philosophy that collecting user data and using it for secondary purposes improves the user's experience.[251] On a technical level, this assessment is correct to the extent that the collection and manipulation of user data can lead to improved social media applications.[252] In the context of Path's collection of users' address books, this practice may enable Path to provide users with more accurate and useful "friends lists."[253] However, the potential ownership violation lies in Path's belief that because it has access to certain data stored on your cell phone or tablet, it can collect that data, keep it, and use it for other purposes.[254] Naturally, Path's access to users' phonebooks was tied to the application's performance in that it assisted users with locating their friends and family on Path.[255] When Path collected the phonebooks and stored them in a separate place without obtaining user consent, however, Path arguably misappropriated the information.[256]

Consider this helpful analogy: if you offer to lend your car to a friend in need, does it entitle them to borrow your car on any future occasion without first seeking your permission or even informing you that it intends to borrow your car?[257] Just because a user allows Path to view the user's phonebook for the purpose of finding friends and family members who are also current Path users, it does not automatically entitle Path to access the phonebook at any time for any purpose.[258] When Path accessed users'

---

248. Jon Phillips, *Path Social Media App Uploads IOS Address Books to Its Servers*, WIRED (Feb. 8, 2012), http://www.wired.com/2012/02//path-social-media-app-uploads-ios-adress-books-to-its-servers/.

249. *Id.*

250. *Id.*

251. Jay Garmon, *The Path Fiasco Wasn't a Privacy Breach, It Was A Data Ownership Breach*, BACKUPIFY (Feb. 9, 2012), http://blog.backupify.com/2012/02/09/the-path-fiasco-wasnt-a-privacy-breach-it-was-a-data-ownership-breach/.

252. *Id.*

253. *Id.*

254. *Id.*

255. *Id.*

256. Garmon, *supra* note 251.

257. *Id.*

258. *Id.*

phonebooks for the purpose of building its own database, it essentially snuck into the garage and took each user's car for a joyride.[259] Since this practice came to light, Path has uploaded a new version of the application that asks users for permission before uploading their phonebooks to its servers.[260]

3. Facebook Social Ads

One of the most recent examples of the tug-of-war between service providers and users occurred in 2014 when Facebook issued a notice that it intended to update its privacy policy.[261] Many users interpreted the policy change as permitting Facebook to commercialize any images that users upload to the website.[262] In response, Facebook's Privacy Communications Manager issued a statement indicating that the policy update would not result in Facebook taking ownership of uploaded data and that users own the information they share with the site.[263]

Looking at the privacy policy, however, it is not entirely clear what Facebook can or cannot do with information uploaded to the site.[264] When new users create a Facebook account, they must agree to a battery of terms, and agree to grant Facebook "'a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP [intellectual property] content that you post on or in connection with Facebook.'"[265] Facebook contends that this grant is necessary to enable Facebook to share content on its platform, but that it does not entitle Facebook to sell the information without the user's permission or knowledge.[266] The license, however, grants Facebook the right to the "use" of your information, which is vague and susceptible to many interpretations.[267] While it may be difficult for Facebook to share your photographs with third parties, it leaves the door open for Facebook to utilize those images in a host of other ways.[268]

One way that Facebook may be using the data uploaded to its site is social ads.[269] Social ads are designed to target a particular friend group and

259. *Id.*
260. *Id.*
261. Olivier Laurent, *No, Facebook is Not Planning to Sell Your Images*, TIME (Dec. 2, 2014), http://time.com/3615271/facebook-privacy-policy-photos/.
262. *Id.*
263. *Id.*
264. *Id.*
265. *Id.*
266. Laurent, *supra* note 261.
267. *Id.*
268. *Id.*
269. Kurt Wagner, *How Facebook is Using Your Photo Ads*, MASHABLE (Sep. 5, 2013), http://mashable.com/2013/09/05/facebook-ads-photo/.

distribute information regarding products and services that may appeal to the group at large based on one friend's Facebook activities.[270] For example, if you view Nike's Facebook page and click the "Like" button, Facebook may reproduce an image of your profile picture next to the Nike logo with a statement indicating that you "Like" Nike.[271] This social ad is then displayed on the Facebook pages of people within your network, i.e., people with whom you've connected on Facebook, or "friended."[272] On the subject, Facebook's Statement of Rights and Responsibilities states:

You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.[273]

This language provides users with some say regarding how their content can be used to create social ads.[274] For example, users can identify a limited group of users with whom they share specific information, and users can prevent the content that they contribute to social ads from being distributed to Facebook users who they do not know.[275] It is worth noting, however, that users receive no compensation for their participation in what is essentially a marketing campaign. By indicating that you "like" a particular product and by enabling that product manufacturer to access your Friends list, you are assisting them with their ultimate marketing goals—for free.[276]

D. Transparency, Trust, and Choice

These examples highlight several common threads between privacy rights, security breaches, and ownership battles. Many of these violations occurred as a result of a service provider's failure to be transparent or trustworthy, or to provide users with a choice regarding how their information is handled. In the context of privacy rights, transparency is the most critical factor. If service providers are not transparent regarding how user data will be manipulated, users will be less willing to share their

270. *Id.*
271. *Id.*
272. *Id.*
273. *Id.*
274. Wagner, *supra* note 269.
275. *Id.*
276. *Id.*

information or subscribe to a particular service no matter how beneficial that service may be. OnStar, for example, provides clear terms of use regarding the location tracking activities that it performs while also providing users with the ability to opt out of this practice.[277] OnStar clearly describes the nature and scope of its practices, offers its users a choice, and assures them that it will abide by that choice.[278] Although Gmail is transparent with its email scanning practices, users are faced with a take-it-or-leave-it decision.[279] Uber provides the best example of what not to do when it comes to privacy rights, by hinting at the possibility of spying on users without their consent and for a reason that in no way relates to enhancing users experience. ATPs can learn a great deal from these examples, and would realize the most success by modeling their practices after OnStar. By fostering a high sense of trust when it comes to privacy rights, more farmers will be willing to contribute their farm for aggregation and pooling purposes.

When it comes to data security, trust is perhaps the most critical factor at play. Once a user places his or her information in the service provider's hands, the burden is on the service provider to ensure that it is safe. Other than reviewing a company's data security practices before agreeing to use the service, there is very little that users can do to ensure the service providers are maintaining the highest level of security awareness. Because users have fewer choices in this regard, a strong sense of trust must be established between the user and the service provider. As the Health Net case illustrates, users have good cause to be concerned about whether their service providers are protecting their information. In light of the Health Net situation, farmers should inquire about the physicality of how their data is stored, i.e., whether any portable devices are used and who has access to those portable devices, and whether the service provider is employing adequate encryption protections.

Additionally, the iCloud hacking scandal provides an excellent example of how usernames and passwords are not a foolproof method of protecting user information and cannot serve as the only security measure. It also illustrates how careful farmers must be with their passwords and that they should consider changing them periodically. Finally, the Target example provides an excellent example of how even the most substantial security measures are still susceptible to breaches. In the event of a security breach, it is critical for an ATP to have a well-planned data breach protocol

277. *See* discussion *supra* Part III.A.3.

278. *Id.*

279. Justin Meyers, *You Can't Stop Gmail From Scanning Your Emails—But You Can Limit Their Ad Targeting*, DIGIWONK (June 2014), http://digiwonk.wonderhowto.com/how-to/you-cant-stop-gmail-from-scanning-your-emails-but-you-can-limit-their-ad-targeting-0154412/.

and to offer users remedial services, like credit monitoring. Farmers should ask questions about how ATPs would address a security breach and how diligently they monitor their systems to identify a breach.

In the realm of ownership rights, choice plays a significant role in determining whether an individual will sign up for a particular service. In the Facebook Social Ads example, we see how users are provided with a clear, transparent explanation of why Facebook collects certain information, how that information is used, and how users can opt out of participating in the Social Ads component. This illustrates the importance of allowing users to opt out of certain aspects of a particular service without requiring a "take it or leave it" decision. Facebook Social Ads strike a balance by offering users a flexible menu of services that they can customize to their liking.

Trust is also an important component of ownership rights. By agreeing to provide information to an ATP, a farmer is intrinsically trusting the ATP to use the data appropriately and in accordance with the agreed upon terms. Unfortunately, as the Facebook Apps example illustrates, data is sometimes misappropriated without users' knowledge or consent, and utilized for purposes beyond the scope of the service agreement. As a result, transparency must be employed in order to foster the trust that users need so they will share their information freely. For example, Path stated that it copied users' phonebooks in order to increase their overall experience with using the application.[280] Although this is an altruistic goal, many users are uncomfortable with the notion that the application was accessing and copying their information without consent. Path is now more transparent when it comes to informing users about this practice, and, most importantly, they provide users with a choice regarding whether they want to participate in the phonebook copying.[281]

As these examples illustrate, three of the most critical factors that farmers should consider when evaluating an ATP's policies on privacy, security, and ownership are trust, transparency, and choice. Farmers should keep these principles in mind when deciding whether to contract with a particular ATP. By doing so, farmers will be able to ensure that they understand how their information is being used, who has access to their information, and whether they will retain the ultimate choice over what happens to their data.

280. *See supra* Part III.C.2.
281. *Id.*

IV. SEWING THE SEEDS OF A SUCCESSFUL FUTURE

In the of Fall 2014, a group of major agricultural organizations and ATPs gathered in Kansas City, Missouri to execute the Privacy and Security Principles for Farm Data agreement ("the Agreement").[282] A representative for one of the participating organizations, the American Farm Bureau, described the agreement as providing "'a measure of needed certainty to farmers regarding the protection of their data.'"[283] One of the motivating factors that led to creation of the Agreement is the desire to encourage the use of precision agriculture technologies, and to provide certainty regarding how ATPs will utilize farm data.[284] The signatories to the Agreement expressed their hope that ATPs will implement the Agreement's policies into their service contracts.[285] If this hope is realized, it would result in a significant step for precision agriculture, and would serve the signatories' ultimate goal of moving the farming industry into the era of precision agriculture.[286]

At the outset, the Agreement acknowledges the many benefits of precision agriculture technology and its ability to increase farmers' "productivity and profitability."[287] At its core, the Agreement seeks to establish conformity between ATPs and the terms that are included in their respective agreements.[288] By establishing contract uniformity, farmers will have a better understanding of the scope of their security, privacy, and ownership rights.[289] Whether the Agreement's principles will achieve this effect remains to be seen. The Agreement delineates 12 main principles:

---

282. Matthew J. Grassi, *Major Farm Organizations Ratify Data Privacy Policy*, PRECISIONAG (Nov. 13, 2014), http://www.precisionag.com/data/major-farm-organizations-ratify-data-privacy-policy/.

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

284. Grassi, *supra* note 282.

285. *Id.*

286. *Id.*

287. AM. FARM BUREAU FED'N, *Privacy and Security Principles for Farm Data*, Nov. 13, 2014, FB.ORG, http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf (last visited Mar. 3, 2015).

288. *Id.*

289. Brian Lisik, *Farmers: Get Familiar with New Big Data Agreement*, FARM AND DAIRY (Nov. 20, 2014), http://www.farmanddairy.com/top-stories/farmers-get-familiar-new-big-data-agreement/226958.html.

- Education
- Ownership
- Collect, Access, and Control
- Notice
- Transparency and Consistency
- Choice
- Portability
- Terms and Definitions
- Disclosure, Use, and Sale Limitation
- Data Retention and Availability
- Unlawful or Anti-Competitive Activities
- Liability and Security Safeguards[290]

Many of these principles overlap and bear on multiple aspects of privacy, security, and ownership rights.[291] In theory, they seem to strike a solid balance between protecting the farmers' interests while also encouraging them to participate in data pooling. As previously discussed, data pooling is one of the most beneficial aspects of precision agriculture, both at the micro, intra-farm level and at the macro, inter-farm level.[292] While only time will tell if the principles are effective methods for creating this balance, one way to predict the Agreement's success is to examine its principles according to the guiding principles of transparency, trust, and choice.

A. Privacy Goals

The agreement outlines a number of measures that pertain to protecting farmers' privacy rights.[293] For example, the Agreement states that "[a]n ATP's collection, access, and use of farm data should be granted only with the affirmative and explicit consent of the farmer" and that "[f]armers must be notified that their data is being collected and about how the farm data will be disclosed and used."[294] As we learned from Gmail and OnStar, it is critical for ATPs to provide farmers with transparent explanations of the scope of their services. Without requiring ATPs to be upfront with their data collection and use practices, many farmers will avoid using these beneficial services altogether. To that end, the Agreement states that ATPs "should

290. AM. FARM BUREAU FED'N, *supra* note 287.
291. *Id.*
292. Griffin, *supra* note 79.
293. AM. FARM BUREAU FED'N, *supra* note 287.
294. *Id.*

provide information about. . . the types of third parties to which they disclose the data and the choices the ATP offers for limiting its use and disclosure."[295]

Requiring ATPs to provide notice and to obtain the farmer's consent before collecting *any* data will provide farmers with an opportunity to educate themselves about the particular implications of providing information to ATPs or participating in data pooling. Additionally, the Agreement acknowledges many concerns by prohibiting ATPs from using "the data for unlawful or anticompetitive activities, such as a prohibition on the use of farm data by the ATP to speculate in commodity markets."[296] Overall, the Agreement requires ATPs to be transparent in their privacy policies and to provide clear explanations of how farmers' data will be used.[297]

B. Security Goals

On the subject of security, the Agreement states that "[f]arm data should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure."[298] Additionally, "[p]olicies for notification and response in the event of a breach should be established."[299] The Agreement also specifies that an "ATP should clearly define terms of liability."[300] The Agreement does not provide any specifics regarding the types of security safeguards that would be considered reasonable, or address certain facets of data security like portable storage devices, encryption, and security breach protocols.[301]

As the signatories indicated, the heart of the Agreement is to establish uniformity among ATP contracts so that more farmers will adopt precision agriculture technologies and participate in data pooling.[302] The failure to provide a definition for reasonable security safeguards or to specify the security breach protocols that ATPs ought to adopt leaves a great deal of uncertainty. Many farmers are apprehensive about participating in precision agriculture at either the intra-farm or inter-farm level because of the real threat that security breaches pose. In light of the data breach that Monsanto experienced, their concerns are not misplaced. Accordingly, addressing the issue of security breaches in the context of precision agriculture is an

295. *Id.*
296. *Id.*
297. *Id.*
298. AM. FARM BUREAU FED'N, *supra* note 287.
299. *Id.*
300. *Id.*
301. *Id.*
302. *Id.*

important task that cannot be ignored. Although the Agreement makes a global effort at ensuring transparency and choice are common threads in ATP contracts, it falls short when it comes to fostering a sense of trust between leery farmers and ATPs. Because so many farmers are concerned about the misappropriation or theft of their farm data, the Agreement should include a stronger emphasis on requiring ATPs to include security breach measures, to describe those measures to prospective clients, and to have a clear security breach protocol.

C. Ownership Goals

The Agreement underscores the issue of ownership rights, stating unequivocally that the signatories believe "farmers own information generated on their farming operations."[303] This presents a tricky issue for many farmers who run their businesses in collaboration with other investors and landowners. It is not uncommon for a farmer to rent land from a property owner and then partner with a cooperative to achieve the actual farming operations.[304] Commonly referred to as collaborative farming, many farmers, and small outfits in particular, have heralded the communal support that collaborative farming provides.[305] With this many cooks in the kitchen, however, who will have the final say regarding dissemination of data accumulated from those farming operations? On this subject, the Agreement states that "[t]he farmer contracting with the ATP is responsible for ensuring that only the data they own or have permission to use is included in the account with the ATP."[306] The Agreement also states that "it is the responsibility of the farmer to agree upon data use and sharing with the other stakeholders with an economic interest, such as the tenant, landowner, cooperative, owner of the precision agriculture system hardware, and/or ATP, etc."[307] This policy would seem to require farmers seeking relationships with ATPs to make some sort of agreement, either formal or informal, with their collaborative farming partners. Perhaps a better policy would be to require the farmer to obtain the written consent of his or her collaborative farming partner(s), or to require them to also be a signatory to the ATP agreement. Otherwise, the result may be a tangled web of

303. Lisik, *supra* note 289.
304. Lindsay Rebhan, *Collaborative Farming: New Farmers Thrive by Working Together*, MIDWEST ORGANIC & SUSTAINABLE EDUC. SERV. (July/Aug. 2014), http://mosesorganic.org/projects/new-organic-stewards/news/new-farmers-thrive-by-working-together/.
305. *Id.*
306. AM. FARM BUREAU FED'N, *supra* note 287.
307. *Id.*

agreements, many of which will likely be informal verbal agreements between business partners.

The Agreement also states 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."[308] Additionally, "[i]f multiple options are offered, farmers should be able to choose some, all, or none of the options offered."[309] The emphasis placed on the ability to opt out of services in conjunction with placing a burden on ATPs to explain the ramifications of a farmer's decision to opt out facilitates an ability to make informed choices about precision agriculture.

Regarding the ability to recall data and delete it from a system, the Agreement states that "farmers should be able to retrieve their data for storage or use in other systems," and that ATPs "should include a requirement that farmers have access to the data that an ATP holds during that data retention period."[310] Additionally, the Agreement requires each ATP to "provide for the removal, secure destruction and return of original farm data from the farmer's account upon the request of the farmer or after a pre-agreed period of time."[311] The Agreement also provides that "ATPs should document personally identifiable data retention and availability policies and disposal procedures," and that "[f]armers should be allowed to discontinue a service or halt the collection of data at any time subject to appropriate ongoing obligations."[312] These policies clearly embrace the concepts of trust and transparency, and will help ensure that farmers retain ultimate control over the data and can withdraw their information at any time.

When it comes to data that has been anonymized or aggregated, however, the Agreement acknowledges that it would be difficult to retrieve this data and that ATPs should not be required to provide a method for the farmer to remove it from the system.[313] It will be critical for ATPs to be transparent about this point, and to provide farmers with a clear choice regarding whether they want to contribute their data to an aggregated pool. Farmers must be made aware that once their data is anonymized and aggregated, they will be unable to delete it from that system.

On the subject of disclosure, use, and sale limitations, the Agreement states:

---

308. *Id.*
309. *Id.*
310. *Id.*
311. AM. FARM BUREAU FED'N, *supra* note 287.
312. *Id.*
313. *Id.*

An ATP will not sell and/or disclose non-aggregated farm data to a third party without first securing a legally binding commitment to be bound by the same terms and conditions as the ATP has with the farmer. Farmers must be notified if such a sale is going to take place and have the option to opt out or have their data removed prior to that sale. An ATP will not share or disclose original farm data with a third party in any manner that is inconsistent with the contract with the farmer. If the agreement with the third party is not the same as the agreement with the ATP, farmers must be presented with the third party's terms for agreement or rejection.[314]

Noticeably, this provision only references *non-aggregated farm data*, which would seem to imply that aggregated farm data may be sold to a third party at the ATP's discretion. Nothing in this provision specifies whether the ATP must anonymize aggregated farm data prior to sale or distribution. Notwithstanding this uncertainty, this provision does an excellent job of ensuring that ATPs will be transparent in their distribution and sale of non-aggregated farm data. It also creates a situation in which farmers will virtually always have the choice to opt out of a sale or distribution before it occurs.

D. Measuring Up

Overall, the Agreement includes many provisions that are geared towards encouraging ATPs to conduct their businesses in a trustworthy, transparent, and flexible manner.[315] For now, however, its principles are only binding on ATPs if they are incorporated in the parties' contract.[316] Some predict that these policies will eventually become industry standard language regarding the collection of farm data.[317] Because so many farmers are reluctant to implement this beneficial tool, ATPs would benefit from adopting the Agreement's principles and striving to foster transparency, trust, and choice in their practices. Ultimately, farmers will dictate the future of precision agriculture through their decisions to implement the technologies on an intra-farm level, to agree to pool their farm data, or to avoid them altogether.[318]

When it comes to security, however, the Agreement's scant provisions do little to ensure that ATPs will use appropriate measures. The Agreement's

---

314. *Id.*
315. *Id.*
316. Lisik, *supra* note 289.
317. *Id.*
318. N.R. Kitchen et al., *Educational Needs of Precision Agriculture*, 3 PRECISION AGRIC. 341, 342 (2002), *available at* http://www.ndsu.edu/fileadmin/soils/pdfs/Educ_Needs_of_Prec_Ag.pdf.

provisions on this subject are vague and open to a great deal of interpretation by ATPs. At the very minimum, the Agreement should have provided a basic set of security protocols or measures that ATPs must provide. This would not be out of the ordinary, considering that many industries are subject to data laws that require specific security standards, like the healthcare industry. Without assuring farmers that their data is secure, they may be less likely to utilize precision agriculture technologies, or to participate in big data pooling.

V. IT ALL COMES DOWN TO EDUCATION

Although the Agreement is a respectable step toward facilitating the wide-scale implementation of precision agriculture, accomplishing this goal will require more than simply encouraging ATPs to adopt transparent, trustworthy, and flexible practices. For farmers to take full advantage of precision agriculture and for the world to derive the numerous benefits of data pooling, many farmers will need to undertake serious educational endeavors to learn about the applications, implications, and potential risks of these technologies.

While the Agreement's policies regarding privacy and ownership make substantial strides toward ensuring that ATPs play fair, the Agreement places a substantial burden on farmers to become computer literate, data savvy, and contract wise. On the subject of education, the Agreement emphasizes the importance of "grower education" and its ability to "ensure clarity between all parties and stakeholders," primarily when it comes to the grower's "rights and responsibilities."[319] Accordingly, the Agreement calls for ATPs to draft contracts using "simple, easy to understand language."[320] However, even the most simply drafted contracts can be vague, open to interpretation, and daunting to unsophisticated parties with little to no experience reading contracts.

The Agreement also states that "[g]rower organizations and industry should work to develop programs, which help to create educated customers who understand their rights and responsibilities."[321] The importance of grower education and the impact that it will have on whether the full benefits of precision agriculture are realized cannot be understated. For many farmers, the road to adopting precision agriculture technologies is littered with countless obstacles, and not only in regard to data rights.[322] At a basic level, many farmers lack confidence when it comes to computer literacy and

319. AM. FARM BUREAU FED'N, *supra* note 287.
320. *Id.*
321. *Id.*
322. Kitchen et al., *supra* note 318, at 341, 343.

navigating software programs.[323] Even so, some of the most technologically savvy farmers will struggle when it comes time to compile and interpret the mountains of data that precision agriculture technologies create.[324] As the Rias Baixas example demonstrates, there are limitless combinations of variables that remote sensors are capable of detecting.[325] For many farmers, knowing which variables to combine and how to manipulate the data provided poses a substantial challenge.[326]

But what would these educational endeavors need to entail in order to truly be successful? For starters, farmers who wish to implement precision agriculture will need educators who understand the ever-changing landscape of these technologies.[327] To be effective, educators need to understand the scientific aspects of how the technologies operate and to be able to communicate this information to a wide range of skill levels, including farmers who possess only a novice level of computer skills.[328] Many of the questions that farmers will need answered regarding precision agriculture focus on the nuts and bolts of how the technology is integrated into their operations, i.e., who will install the equipment, or what happens if it malfunctions.[329] Many other farmers will have questions regarding the storage and retention of their data and how they will be able to determine if the data readings are accurate.[330]

Additionally, many farmers will need assistance when it comes to filling the gaps between interpreting the data and identifying the appropriate solution for a particular problem, such as pest control or irrigation.[331] It is one thing to read several reports, and another to understand how the reports are related and to be able to identify the answers that they implicitly suggest.[332] Once farmers are able to process data, they may require guidance on how to use that data to make management decisions.[333] Naturally, each of these hurdles will vary depending on the specific type of farming practice involved.[334] For example, the methodologies that worked for the wine growers in Rias Baixas may not prove useful for alfalfa farmers in Fresno, California.

---

323. *Id.* at 342.
324. *Id.* at 348.
325. Martinez, *supra* note 48.
326. Kitchen et al., *supra* note 318, at 343.
327. *Id.* at 342.
328. *Id.*
329. *Id.* at 350.
330. *Id.* at 349.
331. Kitchen et al., *supra* note 318, at 347.
332. *Id.* at 346.
333. *Id.*
334. *Id.* at 347.

Beyond these technical and practical educational needs, farmers will require substantial assistance from lawyers who are well versed in both agricultural operations and contract law. Educational programs geared toward contract interpretation will help prevent farmers from entering agreements that they do not understand. A crash course in contract law will be essential when it comes to enabling farmers to read a particular ATP's contract and to understand the scope of the services to be provided and the terms to be agreed upon. For example, in the context of privacy, security, and ownership rights, one of the most critical aspects that a farmer must consider is whether he or she has the ability to opt out of a particular service or feature that results in the appropriation of the farmer's data. Although the Agreement emphasizes the ATP's responsibility to provide opt-out choices and to explain the scope of these decisions, many farmers will look for guidance from a neutral third party, such as a lawyer. Providing a broad range of legal services designed to assist farmers of all sophistication levels with reading and interpreting service contracts will be essential for both encouraging the use of precision agriculture technologies and ensuring that they are implemented fairly. This is particularly important for small- to mid-size farmers who may not have the resources to hire an attorney to represent them during contract negotiations. By encouraging educational opportunities for farmers to learn more about the legal implications of ATP contracts, it will likely quell their apprehension and mistrust of large ATPs while facilitating the potential benefits that these technologies afford. As lawyers, we have the opportunity to serve as liaisons between farmers and ATPs and to provide the guidance that farmers need to make the best, most informed decision for their businesses.

One example of a neutral, third party educational resource is Farmers' Legal Action Group ("FLAG").[335] FLAG acknowledges the significant role that contracts play in farmers' businesses, and provides educational resources to help farmers understand the rights and obligations of these agreements.[336] As another example, CrescoAg, LLC, is an independent company that provides farmers with neutral assistance in farm data management, including record keeping and "whole farm" research services.[337] In order to help farmers overcome the multitude of hurdles that they face, the industry will require more organizations like FLAG and CrescoAg to provide neutral and independent guidance for farmers. These

335. *See Topic: Contracts*, FARMERS' LEGAL ACTION GROUP, http://www.falginc.org/topic/contracts (last visited Mar. 16, 2015).

336. *Id.*

337. *About Us*, CRESCOAG, http://www.crescoag.com/about (last visited Mar. 16, 2015).

services will require educators from a variety of backgrounds, including computer scientists, environmental scientists, economists, and lawyers.

Education, of course, is a two-way street. The Agreement includes a provision requiring ATPs to "provide information about how farmers can contact the ATP with any inquiries or complaints."[338] This policy is equally as important as transparency. Without a method for redressing issues and potential contract violations, transparency is merely an ideal without teeth. As precision agriculture progresses, it may be prudent for ATPs to carve out an entire section of their service contracts dedicated to providing users with a clear method for contacting the ATP, and to also include channels on their internet websites, via email, and by telephone. As the Facebook Apps example illustrates, there are many instances in which altruistic service providers are unaware that they have a glitch in their system. By underscoring two-way communication between the ATP and the farmer, both parties can ensure that the service and technology is operating as both parties expect and desire.

VI. CONCLUSION

It is unclear whether the potential benefits of agricultural data collection will outweigh the risks, or whether adequate protections will be set in place before substantial data rights violations or ownership misappropriations can occur. In the meantime, farmers who currently utilize precision agriculture, or who are considering implementing these tools, should take steps to protect the privacy, security, and ownership of their data, and to think carefully before consenting to any data sharing agreement. In order to fully realize the benefits that precision agriculture has to offer, more educational services should be provided in order to help farmers overcome any issues or concerns they have with implementing these technologies. Farmers should not hesitate to consult objective, third party sources regarding any of these concerns, particularly when it comes to the legal implications of a particular ATP's service agreement.

As lawyers, we have the ability to serve as liaisons between the farming community and the complex world of contract law that stands in the way of the decision to utilize precision agriculture. The Agreement provides many useful principles that we can refer to when helping a client determine if a particular ATP's service agreement is in his or her best interest and the implications it may have for his or her rights. Keeping the ultimate goal of farm data aggregation in mind, we can be a part of the effort to allay farmers'

338. AM. FARM BUREAU FED'N, *supra* note 287.

apprehensions regarding this incredible tool while also holding ATPs to the highest standards of transparency, trust, and choice.

Like farming, an idea begins no differently than a seed. The way the field is plowed, the quality of the soil in which they will grow and the water and nutrients they are provided will make all the difference on their ability to thrive and grow. If handled with care and attention, a single seed or idea can flourish into an abundant harvest. The idea of precision agriculture has the potential to revolutionize modern farming and to resolve many issues plaguing the industry around the globe. However, if haphazardly sown without clear goals, rules, and objectives, this seed may sprout into a weed and foster more lament than prosperity. Precision agriculture alone does not pose a threat to modern agriculture. Rather, it is the way in which we bring this tool to the field that will determine whether precision agriculture will take us from famine to feast, or feast to famine.