

# Publications

## Understanding the Legal Aspects of Precision Farming Data

### Related Attorneys

Thomas H. Fusonie

Christopher A. LaRocco

### Related Services

Data Strategy, Privacy and Security

### Related Industries

Agriculture

### CLIENT ALERT | 5.14.2021

Farmers are rapidly adopting precision farming techniques because they generate a treasure trove of valuable data to help guide farmers on how to optimize their farming. With this explosion of new data, and nationwide news stories about data breaches and new privacy laws, questions have arisen regarding whether a farmer may face any legal liabilities based on how precision farming data is handled and stored. This brief article highlights the legal issues related to precision farming data, including an explanation of why farmers should not be concerned by the recent surge in data privacy and protection laws, and a primer on key things farmers should understand before signing an agreement with a precision farming vendor (e.g., cloud provider).

Data is at the heart of precision farming. Crop yields, soil conditions, humidity, temperature, crop or soil treatments, animal health, feeding, and tracking, and drone footage are just some of precision farming's central data components. This granular data paints a complete picture of a farm's overall status, which was unobtainable just a few years ago.

Farmers reap the benefits of this data by leveraging it to, among other things, reduce costs, perform more targeted treatments, reduce waste, and monitor animal health. In the most sophisticated precision farming frameworks, farmers can use IOT (internet of things) connected devices to automatically address issues as they arise. For instance, sensors may monitor soil conditions and determine that water levels are low in a particular area of the farm. The precision farming system would then communicate with an IOT-connected sprinkler system to water that particular zone.

However, as technology has advanced in all sectors, including farming, so has government regulation. These laws have focused on the regulation and protection of data. For instance, currently at least 20 states have introduced general data privacy laws and every state has passed a data protection law in one form or another.

While the increase in regulation might instinctively turn some farmers off on the idea of engaging in precision farming, fortunately, the existing and proposed laws in this space largely do not apply to the

data collected through precision farming. Those laws regulate the collection and use of “personal” data (i.e., data which can be used to reasonably identify an individual), yet the data collected in precision farming is typically non-personal data. Therefore, despite an exponential increase in the regulation of the collection and use of data, the data involved in precision farming is still largely unregulated.

While the data which is collected via precision farming may not be subject to data protection and privacy laws, there are still a number of issues related to this data for precision-farmers to consider. These issues and questions deal primarily with the technology license and/or cloud service agreements which facilitate precision farming. Technology licensing and cloud service agreements are notoriously complex and one-sided for the service provider. Before signing any agreement with a precision farming technology vendor, farmers should carefully consider their rights and obligations under the proposed contract and push back where necessary. At minimum, before signing any agreement the farmer should be able to answer the following questions:

### **What are the parties’ respective rights to the data?**

Precision farming data has great value. Not only to the farmer, but also to the precision farming vendors and competitors. For example, data showing crop yields based on a particular treatment might have value to a competing farmer trying to cultivate that same crop. Precision farming vendors might have the same interest in the data, not necessarily to cultivate the crops themselves, but to pool your farm’s data with other clients’ and then aggregate and sell that data to others – such as companies developing the treatments applied.

Because this data is so valuable, it is vital that ownership and, if applicable, licensing rights to the data are clearly defined in any precision farming agreement. The obvious preference would be for the farmer to own all data collected as part of the precision farming. However, vendors will often attempt to obtain rights or a license to use the data beyond the purposes of the agreement. Thus, for example, a farmer should aim to limit a cloud services vendor’s processing of their data to only that which is necessary to carry out the service (i.e., storage of the data) and to prohibit the sale or licensing of the data to third parties. Without performing due diligence at the onset of the contractual negotiations, farmers may be forfeiting their rights to the data or potential compensation related to the data (e.g., a licensee fee for use of the data).

### **Where is the data stored and how is it secured?**

Given the value of precision farming data, farmers should be able to understand where the data is stored and the procedural and technical safeguards in place to ensure the data is secure from external security threats. For cloud service agreements, the easy answer is that the data is stored in the cloud and typically secured by industry-standard data security protections, but other arrangements might not be as obvious. For instance, some service providers might choose to store the data off-premises at their data warehouse while others might store the data locally on a hard drive at the farm. Likewise, less established vendors may have rudimentary data protections while more established vendors will almost certainly have tested and sophisticated data security programs. In a farmer’s contract with its vendor, he or she should negotiate to include a representation and warranty from the vendor that it will store and secure the data in accordance with industry-accepted procedural and technical safeguards. While 100% security is not always possible, understanding where the data is stored, selecting an established vendor, and receiving a warranty from

the vendor of adequate data security protections can minimize risk and impact of a breach.

The American Farm Bureau Federation has collaborated with a number of ag tech vendors to establish its model "Privacy and Security Principles for Farm Data". These non-binding principles present a model standard for ag tech vendors to abide by when contracting with farmers. Among the principles are that: (1) farmers should own and control the precision farming data; (2) farmers should be given notice of all data which the vendor collects and how that data is used; (3) farmers should have the ability to prevent or opt out of the sale of data to non-affiliated third parties; and (4) the ag tech vendor should protect the data with reasonable data security protections. These principles are a great starting point when contracting with an ag tech vendor. To view all of the model principles and for a list of ag tech vendors that have agreed to abide by those principles visit: <https://www.fb.org/issues/innovation/data-privacy/privacy-and-security-principles-for-farm-data>.

Precision farming will continue to grow and, consequently, the value of the data collected as part of precision farming will grow with it. Despite the lack of existing regulations, farmers considering engaging in precision farming should still study precision farming agreements before executing them. Failure to do so could result in unnecessary exposure and missed opportunities for revenue.