Harvesting Data: Separating the Wheat from the Chaff

Date: 07-19-2018

By: Satya Narayan

The use of sensor technology and hi-tech systems in precision agriculture has resulted in large quantities of data about farm conditions, operations, and yields in the possession of agricultural technology providers. Agricultural technology providers or “ATPs” are constantly developing new software algorithms to organize and analyze ag data collected from different farmers to create meaningful information that farmers can then apply to, and improve, their farming practices. The organization and analysis of large data sets to produce meaningful information, commonly referred to as “big data analytics,” has made it possible for farmers to adjust fertilizer, seed types, irrigation and other factors for different sections of a field. This information can then be used to offset differences in soil types and moisture allowing a farmer to optimize yields across an entire field. In other applications, John Deere has been able to forecast farmers’ demands for spare parts by analyzing machine data from individual combines and incorporating this information with land area and usage data. Big data analytics has even been used to predict and identify sick cattle more accurately than a cattle operator’s evaluation of physical signs of sickness in cattle. Indeed, the American Farm Bureau Federation, has acknowledged the potential impact of big data analytics in agriculture, saying that big data can do for agriculture what the Green Revolution and biotechnology did for agriculture.

While big data analytics has resulted in improvements in farming, some farmers and farm advocates are concerned that, unless restrictions are imposed on the ATP’s use and disclosure of ag data, ATPs might share ag data in a manner disadvantageous to farmers. The American Farm Bureau Organization has voiced concerns on behalf of farmers that ATPs might use ag data to manipulate commodities markets since ATPs have real-time data on how much grain is being harvested from tens of thousands of fields. There is also concern that ATPs might sell ag data to third parties and that this ag data may be used for marketing and sale of the third parties’ products and services without compensating farmers. Such a sale may have a compounded harm to farmers if third party product and service providers use the ag data to increase the price of products and services based on estimated farm production. Ag data that includes farm research and practices may also provide an advantage to competing farmers, inform environmental and animal welfare lobbies, or increase leverage for landowners. As a first step towards dealing with these concerns, a coalition of certain farm organizations, including the American Farm Bureau Organization, and certain ATPs, have agreed to a set of non-binding “Privacy and Security Principles for Farm Data” or what is now known as the “Core Principles,” that they hope will be adopted by other ATPs. However, farmers may find little solace since, as of February 2018, just nine of the original 30 agribusinesses have followed through on their pledge to implement the Core Principles for transparency in the collection of farmers’ data.

Related Article: New Data Privacy Law in California Impacts Large and Small Companies

The complete text of the Core Principles is available here on the American Farm Bureau Organization’s website. It reads very much like privacy and security principles for personally identifiable information, by requiring that the ATPs must provide farmers notice that ag data is collected, how the ag data will be disclosed and used, the types of third parties to which the
ATP will disclose such data, and the choices the ATP offers the farmer for limiting its use and disclosure. Among other things, the Core Principles require that an ATP’s collection, access, and use of ag data should be granted only with the farmer’s affirmative and explicit consent and that the ATP will not change the customer’s contract without his or her agreement. The American Farm Bureau Organization has also created a certification process and accompanying seal to indicate companies that comply with the Core Principles as well as a website that identifies certified companies and indicates their transparency grade.

While on the face of it, adopting the Privacy and Security Principles for Farm Data seem non-controversial and good business practice for ATPs to help build customer trust, their application, without an understanding of the legal landscape and the difficulties in practical business implementation, is ill-advised. For instance, the different types of “ag data,” which may include agronomic data, machine usage data, land data, personally identifiable information, and even associated weather data, are not created equal from a legal perspective in terms of assigning legal ownership to each type of ag data, or in their designation and treatment as business confidential information or as a trade secret, or in their designation and treatment as personally identifiable information (which is subject to the higher standard of privacy reserved for such information).

The foregoing notwithstanding, personally identifiable information may be a hidden issue in many ag data sets. For example, all 50 states and the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation that requires private entities to notify individuals about security breaches involving personally identifiable information. In addressing a data breach, an ATP may be focused on the exposure of trade secrets in the data sets and may not even think to consider the myriad of state laws that determine what constitutes a breach and when or if individuals must be notified. Recently, the European General Data Protection Regulation or “GDPR” starkly illustrated the importance of protecting this type of information by authorizing fines up to the greater of 20 million Euros or 4% of the annual global revenue of the prior fiscal year. As a result, ATPs should seriously consider the territorial scope of their business practices, both in the locations that the ATP is established and the location of the customers they serve. While an ATP can find comfort that the GDPR only applies to natural persons and not legal persons like corporations, an ATP may find that when providing services to a corporation, they cannot avoid processing data of natural persons as well. The difficulty in creating an assessment of privacy risks is multifold. First, the label for personally identifiable information varies from “personally identifiable information” in the United States to “personal data” in Europe. ATPs will likely find that although there are multiple definitions of what constitutes personally identifiable data in the United States, the European definition of personal data is much broader than the United States counterpart. An example of this difference is IP addresses, which may not be considered personally identifiable information in the United States as some courts have indicated that such information identifies a device rather than an individual. This is in direct contrast to the language of the GDPR which explicitly references online identifiers like IP addresses. The gulf between these terms further expands when a farmer considers that, while Europe has a relatively uniform regime for protection of personal data under the GDPR, the United States has a segmented regime where regulation and enforcement is dependent on a number of factors. These factors include the field of data, the enforcement body tasked with enforcement, and other factors. Depending on the type of services an ATP provides, an ATP may find itself subject to some mixture of the Graham-Leach-Bliley Act, the Federal Trade Commission Section 5 unfair and deceptive acts in or affecting commerce, and state privacy regulation.
**Related Article:** [Are You Prepared for the General Data Protection Regulation ("GDPR")?](#)

ATPs should consult with legal counsel familiar with technology and data related contracts, to assist them with drafting an appropriate definition for “ag data” and appropriate contract clauses that help build customer trust but also do not create contractual representations of the ATP that would exceed a customer’s rights granted by applicable law. Furthermore, ATPs adopting these principles should also consult with legal counsel about the frequency and nature of contract modifications that is necessitated by the rapidly evolving nature of technology and the workflow process of complying with a contractual obligation to obtain customers’ consent to contract modifications.