Key Data Ownership, Privacy and Protection Issues and Strategies for the International Precision Agriculture Industry

Joan K. Archer, Ph.D., J.D.
Cordero A. Delgadillo, J.D.

Husch Blackwell LLP
4801 Main Street, Suite 1000
Kansas City, MO 64112-2551

A paper from the Proceedings of the
13th International Conference on Precision Agriculture
July 31 – August 4, 2016
St. Louis, Missouri, USA

***Abstract*.** Precision agriculture companies seek to leverage technology to process greater volumes of data, greater varieties of data, and at a velocity unfathomable to most. The promises of boundless benefits are coupled with risks associated with data ownership, stewardship and privacy. This paper presents some risks related to the management of farm data, in general, as well as those unique to operating in the international arena. Examples of U.S. and international laws related to data protection also are provided. Finally, best practices in drafting agreements that can assist in managing risks relevant to those companies that presently operate or plan to expand their business to areas outside the United States are examined.

***Keywords*.** Data ownership, stewardship, privacy, security, cybersecurity, farm data, precision ag, cybersecurity liability, contract.

Introduction

Modern agriculture faces a variety of challenges. Farmers today must understand the complex ecosystems of their farms. They also must be tech savvy because most farm machinery now includes a data collection component. Precision agriculture ("Precision Ag") companies seek to harvest data and put it to use, employing various business models for their services, such as charging for use of certain data tools, commoditizing data as a valuable asset. The rise of data-based agriculture services brings with it many issues related to data stewardship, which includes data ownership, privacy, and protection. Although the aspect of data ownership has been at the forefront of debates, many precision ag companies are less aware of the crucial laws and regulations that govern data privacy and protection.

In this paper, we introduce points of risk related to farm data stewardship, expanding on concepts and definitions related data stewardship, and highlighting the vulnerabilities inherent in the networks which data transverses.

Then, we explore agricultural technology challenges, identifying those challenges related to data stewardship, and examine initiatives championed by the agriculture industry sector ("FA Sector"), such as the American Farm Bureau Federation's ("AFBF") privacy and data security initiative, that seek to clarify data stewardship issues. We also highlight examples of relevant U.S. and international laws related to data stewardship.

Next, we provide examples of ways to mitigate data stewardship risks through good contract drafting, highlighting certain best practices, including strategies to avoid points of exposure related to international commercial contracts.

Finally, we conclude with a brief comparison case study regarding the disparities in the laws of the United States, China (PRC), the European Union, and Brazil related to data breach obligations. This discussion is designed to alert precision ag companies to certain complexities associated with developing an international precision ag business.

Points of risk related to farm data stewardship

Potential risks to farm data have garnered national attention, underscoring the importance of data stewardship. On March 31, 2016, the Federal Bureau of Investigation's Cyber Division and the US Department of Agriculture jointly released a Private Industry Notification, *Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector,* which predicts that cyber criminals and hacktivists will increasingly target farm data.[1]

In order to appreciate and reduce risks related to farm data, precision ag businesses, commonly referred to as agricultural technology providers ("APTs"), must understand farm data and the concepts of data stewardship.

[1]Private Industry Notification (2016). Smart farming may increase cyber targeting against US food and agriculture sector. Federal Bureau of Investigation, Cyber Division. https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf . Accessed 25 May 2016.

Farm data – what is it?

Generally, ATPs should consider data in the abstract to include any combination of elements, resulting in encoded information. So, data may encode information yet remain unintelligible to humans. Farm Data or farm-level data is similarly broad, including the overlapping classes of information below that highlight the complex web of data:

Personal information

Personal information includes any data element(s) that enable identification of an individual, such as the name and address or an individual.

Financial information

Financial information includes any payment data or related information, such as bank account information retained for processing payments and insurance information.

Operational information

Operational information includes a variety of information related to the farm, such as employee data, usage data related to inputs such as fertilizer, and other mapping, sensor and related data created or needed to operate. This includes raw data (e.g., unprocessed subparts of information), field data (e.g., data recorded automatically or by ATPs in the field), and experimental data (e.g., data that has been transformed to enable analysis, such as data visualizations).

Data stewardship – what is it?

For purposes of this paper, data stewardship refers to the select issues below:

Data ownership

Although the current trend is that farmers own the data, the concept of "ownership" is not as simple as it appears. And, in some circumstances, it may not be required or fair for the ATPs to simply forego ownership rights. An illustrative example of the complexities of data ownership are data licenses, which if properly prepared can allow ATPs broad rights to use, transform, and monetize the data yet allow for the ownership interest to remain with the data subject (e.g., farmer).

Data ownership issues are critical and challenging. For example, many agribusinesses utilize contract farming yet often times the contract farmers do not own the land but rather farm through a lease arrangement, collective or other special economic development programs – who owns the land, who owns the data, who has the authority to license the data derived from such land?[2]

---

[2] *See* Faria, J. A. E., Tavares, A., & Sanders, G. (2015). Legal guide on contract farming. UNIDROIT, FAO, IFAD. http://www.fao.org/3/a-i4756e.pdf. Accessed 25 May 2016.

Data security/protection

Data security/protection includes procedures and principles related to maintaining data such that it is reasonably secure from unauthorized access or acquisition. Examples of reasonable data security practices include conducting security risk assessments, remediating vulnerabilities, providing security training for employees, creating and implementing policies, including access and use policies, enforcing policies, conducting security audits and implementing best practices for archiving system logs for purposes of investigation and internal policy compliance.

Data privacy

Similar to data security in some respects yet different, data privacy is the process and principles that relate to collecting, using, and retaining data in a manner that is consistent with privacy laws, such as providing notice of data practices. ATPs collect not only confidential farm-related data, but also certain financial and other personally identifying information that may be subject to legal restrictions. To avoid risk of liability, ATPs should implement systems and periodically audit those systems to ensure that actual privacy protection practices are consistent with customer-facing statements and that the laws of the relevant jurisdictions are followed. With data stewardship and farm-level data defined, ATPs should appreciate the complexities of how such data flows between parties and seek to manage the specific points of risk.

Specific points of risk

With the complex web of Farm Data in mind, areas of risk become apparent. All data risks can be linked to five fundamental characteristics of risks related to the Internet: 1) geography (a country's governing laws); 2) physical Infrastructure (the vast network of public cables and private hardware); 3) logic layer (the protocols that automatically transmit and route data packets to the addressed location); 4) cyber personas (identifiers such as IP addresses and usernames); and 5) people (individuals, not always easily linked to cyber personas). The five characteristics above create many risks. A few are explored below.

Like other types of data, farm-level data is subject to ever-expanding hardware vulnerabilities (i.e., physical infrastructure risks). For example, in 2016 Nils Rodday, now working for IBM, demonstrated security vulnerabilities in the radio communications and Bluetooth version used within a commercial-grade unmanned aerial vehicle ("UAV"), which cost roughly $40,000.00. For just $40, Rodday was able to execute a man-in-the-middle attack, which allowed him to intercept data, alter data, and alter GPS waypoints to summon the UAV from a distance of nearly 2km.[3]

Beyond hardware vulnerabilities, Farm Data is also at risk from human error and rogue employees, which are widely viewed as the most substantial point of vulnerability (i.e., people risks). Whether through stupidity, ignorance or vengeance, humans are the cause of

[3]*See generally* RSA Conference Speakers (2016). Nils Rodday. EMC Corporation. http://www.rsaconference.com/speakers/nils-rodday. Accessed 25 May 2016.

much unauthorized access and use of data, and employees with credentials that allow for administrative access to big data information systems are high-value targets.

Ultimately, the specific points of risk are too many to list, and this paper focuses on those risks that can be addressed by good contract drafting. Thus, ATPs should seek to understand the nature of the contract and the farm data flows between parties to ensure that contractual *limitations of liability* and *indemnifications* are appropriately addressed. Such crucial contract clauses are covered in more depth later in this paper. The following issues, however, should also be considered by ATPs seeking to eliminate specific points of risk:

- **Definitions** – data, sensitive data, "anonymized" information according to what standard?
- **Standard of care** – what level of precautions must be taken, by whom and when, and are you liable for actions of independent contractors?
- **Breach procedures** – identify the contact persons, notice timelines and procedures, expenses, investigation coordination obligations, which party covers expense of different tasks?
- **Oversight** – audit rights, assessments, monitoring?
- **Return, delete, destroy** – when and how must data be retained or relinquished?
- **Administrative controls** – internal policies, restricted access, and logging?
- **Employee devices** – internal policies banning, allowing, or limiting use to minimize risk?
- **Cyber Insurance** – is it required, how much, what is excluded?

With an understanding of farm data, data stewardship, and points of risk related to farm data, we now explore and analyze FA Sector initiatives that seek to clarify data stewardship issues and highlight specific laws related to data stewardship.

Analysis of FA Sector initiatives and highlights of data stewardship laws

All businesses must balance risk and reward when grappling with data stewardship. In the context of precision ag, technological advancements introduce risk by creating an immense influx of valuable (and sometimes valueless and even risky) data. Aggravating the inherent risks of data stewardship in the FA Sector, trust barriers have stalled adoption of certain technologies, prompting palpable discussions amongst the FA Sector.[4]

Thankfully for ATPs, discussions amongst those in the FA Sector have sprouted several initiatives aimed at alleviating risks and increasing the adoption of precision agriculture technologies. Three such initiatives are provided below. Whether the initiatives are adequate is also discussed. Regardless of adequacy, however, such initiatives are certainly useful developments in the FA Sector for highlighting the importance of data stewardship.

[4]*See, e.g.,* Ag Gateway's Committee on Data Privacy & Security (2014). AgGateway Corporation. http://www.aggateway.org/WorkingGroups/Committees/DataPrivacySecurity.aspx . Accessed 25 May 2016.

Initiative 1: Privacy and Security Principles for Farm Data (the "Farm Data Principles")[5]

The Farm Data Principles is an agreement between influential farm organizations and ATPs that was championed by the American Farm Bureau Federation ("AFBF") in early 2014.[6] As of April 1, 2016, the Farm Data Principles had 37 signatories.[7] Essentially, the Farm Data Principles is an affirmation of belief (or promise) by the signatory ATPs that their business relationships should operate and data should be collected, used and managed in accordance with the Farm Data Principles. These Principles set expectations regarding a diverse set of interrelated data issues, including: 1) education; 2) ownership; 3) collection, access and control; 4) notice; 5) transparency and consistency; 6) choice; 7) portability; 8) terms and definitions; 9) disclosure, use and sale limitation; 10) data retention and availability; 11) contract termination; 12) unlawful or anti-competitive activities; 13) liability & security safeguards. In reality, these data issues are complex. If ATPs rely on a mere 3-page agreement without adequately altering contractual provision and conducting audits to ensure best practices are implemented, it is likely that such promises will be an invitation to litigation rather than a safeguard against exposure risks.[8]

AFBF attempted to create a tool to help address these risks. It created the Transparency Tool, which is a voluntary certification process that builds upon the Farm Data Principles. The Transparency Tool was funded by a consortium of farm industry groups, commodity organizations and ATPs to promote *transparency, simplicity,* and *trust* related to contracts between ATPs and their customers.[9] Crucially, the Transparency Tool does not to proscribe particular practices upon ATPs. An enduring accomplishment, the Transparency Tool has moved the understanding of relevant contractual data issues forward. Yet, true to its namesake, the Transparency Tool provides a disclaimer that states:

> ***Disclaimer:*** *The Ag Data Transparency Evaluator (ADTE) is an online tool provided to assist farmers with making decisions regarding data transfer, usage, and sharing with ag technology providers (ATPs).* ***The information provided on this website is not a legally binding contract and does not replace the terms of any agreements you may have with an applicable ATP.***

---

[5]American Farm Bureau Federation (2016) Privacy and security principles for farm data. American Farm Bureau Federation. http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf. Accessed 25 May 2016.

[6]Hurst, B. (2015). Big Data and Agriculture: Innovation and Implications. (2015). American Farm Bureau Federation. http://agriculture.house.gov/uploadedfiles/10.28.15_hurst_testimony.pdf. Accessed 25 May 2016.

[7]*See* fn7.

[8]*See, e.g.,* Federal Trade Commission (2016). Protecting consumer privacy press releases. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. Accessed 25 May 2016.
("When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information.").

[9]Ag Data Transparency Evaluator. American Farm Bureau Federation. http://www.fb.org/agdatatransparent/. Accessed 25 May 2016.; AgGateway (2014). Data privacy and use whitepaper (draft). AgGateway. http://s3.amazonaws.com/aggateway_public/AgGatewayWeb/WorkingGroups/Committees/DataPrivacySecurityCommittee/Data%20Privacy%20and%20Use%20Whitepaper%20v3.5.pdf. Accessed 25 May 2016
(providing uniform definitions that enable consistent review under the Transparency Tool).

Thus, this Tool, though perhaps helpful, may not be the panacea that many companies hope it will be. Actions must match the representations made during the course of use of the Tool. Policies, procedures and audits should also be used to maintain compliance with the Farm Data Principles.

Initiative 2: Agriculture Data Coalition ("ADC")[10]

The stated mission of ADC is to create a neutral, independent, farmer-centric data repository where farmers can securely store and control the information collected by technology tools. The ADC promises that the repository is "privacy-ensured." To be fair, the repository may have adequate safeguards related to privacy; but to be certain, guaranteeing privacy is a difficult position to take because it is an ongoing and complex task that requires operational flexibility to keep up with evolving data security threats.[11]

In sum, the takeaway is clear. The FA Sector's private initiatives are great starting points, but should not be substituted for independent technical and legal analysis with regard to critical data rights. Support for the proposition that tailored legal analysis is vital can be traced to the FA Sector's goal to "[t]ailor risk-based, performance-based protection measures to the sector's physical and cyber assets, personnel, and customer products," to enhance the security and resilience of U.S. critical infrastructure.[12] The 2015 Food and Agriculture Sector-Specific Plan ("FA SSP") lends further support with its mission that "the FA Sector is to protect against a disruption anywhere in the food system that would pose a serious threat to public health, safety, welfare, or to the national economy."[13] The FA SSP identified four (4) significant risks to the FA Sector, including cybersecurity.[14] Thus, data stewardship issues require companies to address security risks in their entirety – passwords and antivirus software are not enough.

Comparative case study of U.S. and international data stewardship laws

Data stewardship laws arise from a variety of sources, such as rules and regulations promulgated by administrative agencies like the U.S. Federal Trade Commission ("**FTC**"), as well as laws codified by central bodies of government, such as Congress. Courts also provide controlling precedents through their legal opinions issued in connection with litigation. Generally, all data stewardship legal regimes are principle driven, and in recent years many countries principles align with the Fair Information Practices Principles ("FIPPs")[15]:

---

[10]Agricultural Data Coalition (2016). Agriculture data: Putting farmers in the driver's seat. Agricultural Data Coalition. http://agdatacoalition.org/. Accessed 25 May 2016.
[11]*See* Committee on Agriculture (2015). Big data and agriculture: Innovation and implications. U.S. House of Representatives. http://agriculture.house.gov/uploadedfiles/10.28.15_hearing_transcript.pdf. Accessed 25 May 2016 (discussing the difficulties of defining farm data for regulatory purposes related to ensuring privacy and the rapid development of the cyber threat landscape that complicates efforts to secure farm data).
[12]Critical Infrastructure Partnership Advisory Council (2011). Annual report. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/cipac/cipac-annual-2011.pdf. Accessed 25 May 2016.
[13]Jackson, L., Bornstein, J., Detlefsen, C., Gordon, R., Durkovich, C. (2015). Food and agriculture sector-specific plan. FDA, USDA, Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf. Accessed 25 May 2016.
[14]Id.
[15]National Strategy for Trusted Identities in Cyberspace. Appendix A-Fair information practice principles. NIST. http://www.nist.gov/nstic/NSTIC-FIPPs.pdf. Accessed 25 May 2016.

- **Transparency** – notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information ("PII").

- **Individual Participation** – involve individuals in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII.

- **Purpose Specification** – articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

- **Data Minimization** – only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

- **Use Limitation** – should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

- **Data Quality and Integrity** – ensure that PII is accurate, relevant, timely, and complete.

- **Security** – protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- **Accountability and Auditing** – be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Although the FIPPs are not universally applied in all countries, they are referenced above to illuminate the global policymaking trends related to data stewardship. Below are relevant laws selected to provide a comparative analysis of laws related to data stewardship in the United States, China, the European Union, and Brazil.

United States

US laws govern data within specific sectors, such as healthcare[16] and financial services,[17] which are often enforced by the corresponding regulatory agency, such as the Office of Civil Rights for healthcare data violations. Because U.S. laws do not establish an overarching governance model for all data collected by businesses, however, those companies outside a specific regulatory regime, including most precision ag companies, are regulated under consumer protection laws, and the rules and regulations employed in the healthcare and financial services industries likely will become models for others as well, including agriculture. Regulators typically enforce data stewardship principles against businesses under consumer protection laws that prohibit unfair and deceptive business practices (even in the context of B2B because businesses are equally protected as consumers).[18] For

[16] 42 U.S.C. § 1301 (1997). The Health Insurance Portability and Accountability Act ("HIPAA").
[17] 15 U.S.C. §6801 (2011). The Financial Services Modernization Act. ("Gramm-Leach-Bliley" or "GLB")
[18] *See, e.g.,* 15 U.S.C. § 45 (2006). Federal Trade Commission Act.

example, the FTC has brought over fifty (50) enforcement actions related to data stewardship that amount to what some refer to as court-made law regarding the question of what constitutes reasonable security – the elusive threshold for businesses seeking to avoid enforcement actions.[19]

Further complicating US data stewardship laws, most states use different definitions of personal information and require disparate obligations related to information, such as requirements for data security[20] and different standards when determining whether data breach notification obligations, have been triggered – some states provide a 'risk of harm' exception while other states require notification upon any unauthorized access and acquisition. Notably, the laws that apply depend on the residence of the data subject (usually consumers). Thus, ATPs with a single place of business could be subject to multiple state laws, so long as a single customer resides there. Penalties for violating data stewardship related laws typically include long-term oversight, reporting requirements, fines, and disgorgement of profits.[21]

The highlights of laws regarding the three countries below were selected because the potential effect of emerging laws and because such countries are identified as regions for growth in precision ag.

China (PRC/Mainland)

Privacy is enshrined in Chinese law and is associated with the right to dignity. Although this right is somewhat different than US concepts of privacy, it is nevertheless protected through general concepts of civil and tort law.[22]

Similar in some respects to the US, China does not have a comprehensive law related to issues of data stewardship. In 2012, however, the Standing Committee of the National People's Congress laid the foundation for rapid developments of additional administrative rules and regulations related to data stewardship by outlining eleven principles in its *Decision on Strengthening Online Information Protection* (the "Decision").[23]

In 2013, the Ministry of Industry and Information Technology ("MIIT"), the functional "regulator" of internet-related personal data, implementing aspects of the Decision,

---

[19]*See* Sloan, P. and Delgadillo, C. (2015). FTC enforcement of data security. http://www.huschblackwell.com/~/media/files/businessinsights/businessinsights/2015/05/whitw%20paper%20ftc%20enforcement%20of%20data%20security/whitepaper_ftcenforcementofdaftcenforce.pdf. Accessed 25 May 2016.
(Summarizing and providing lessons from over 50 FTC enforcement proceedings).

[20]*See, e.g.,* Cal. Civil Code §1798.81.5 (requiring businesses implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification, or disclosure).

[21]See FN 16

[22]De Hert, P. and Papakonstantinou, V. (2015). The data protection regime in China. European Parliament, Directorate-General for Internal Policies. http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf. Accessed 25 May 2016.

[23]11th National People's Congress (2012). Decision of the National People's Congress on strengthening the network information protection. http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm. Accessed 25 May 2016.

announced the *Telecom and Internet Users' Personal Data Protection Regulations* (the "Regulations"). The regulations detail data security requirements, such as personnel training[24] and security audits/remediation,[25] and also provide privacy protections for consumers, such as the requirement that companies post a privacy policy.[26]

Importantly, these Regulations apply to nearly all companies that solicit or do business in China and operate online. A particularly unique obligation, though also found in Brazil, is that companies must stop collection and use of personal information, **and delete** such information after service has concluded.[27] Another issue, again not unique to China, is the quick-expanding definition of personal information.[28]

Overall, China has a poor track record related to data stewardship, especially with respect to consumers; yet in recent years, interest has increased and so has enforcement. Enforcement happens through the courts as no other central enforcement authority has emerged. Enforcement actions are rare compared to other countries and are primarily focused on the illegal sale of personal information rather than unreasonably data security practices. Nonetheless, prudent ATPs targeting to enter China will stay abreast with developments.

European Union ("EU")

The EU has a strong reputation for regulating and enforcing data stewardship issues. The European Commission has adopted a Data Protection Directive that individual member states implement through local legislation that differs in practice across the EU. Due to perceived overreaching by US intelligence agencies, however, the EU is currently in a state of flux – at least in terms of international data transfers of EU data to the United States. Thankfully, clarity seemingly may be just around the corner.

The EU Parliament recently adopted the General Data Protection Regulation ("GDPR") that will harmonize much of the disparities under the current regime. The GDPR took effect on May 24, 2016. Businesses were given two years to align their practices with the GDPR. The impact of the GDPR will resonate beyond the EU, as enforcement mechanisms are strengthened and jurisdiction is expanded. The definition of personal information expanded and the level of consent required has been heightened – no more opting out of data policies, data subjects must opt in to certain data practices. Troubling for companies that plan to derive value from customer data is the fact that the GDPR enhances a customer's rights to demand that data be deleted and destroyed. Whether doing business in the EU or elsewhere, these data stewardship laws are ignored at an organization's peril.

---

[24]Ministry of Industry and Information Technology (2013). Telecom and Internet users' personal data protection, Art. 15.
[25]Id at Art. 16.
[26]Id at Art. 8.
[27]Id at Art. 9.
[28]*See* State Administration of Industry and Commerce (2015). Measures for punishments against infringements on consumer rights and interests (superseding definition of personal information that includes new data categories, including gender, occupation, date of birth, and consumption habits). Geospatial data is also considered PI.

Brazil

Much like the US, Brazil does not have a comprehensive data stewardship law, and instead regulates certain industries with specific laws.[29] Since January 2015, however, Brazil has been working on a comprehensive bill, but it has not garnered support from the business community as it is perceived to overburden business with compliance requirements.

Brazil's constitution protects privacy and allows for compensatory damages due to violations.[30] Brazil's Consumer Code also provides rights to citizen's whose personal information is kept in a consumer database, such as requiring the database owner to make requested corrections within five (5) business days.[31] The 2014 Civil Rights Framework for the Internet also provides protections, such as invalidating contracts[32] that do not adhere to data stewardship requirements, such as obtaining consent by providing consumers separate, prominent clauses that detail data collection, use, storage, and processing of personal information. Brazil, like most other countries, has data retention laws that mandate that certain data be maintained by companies for a predefined number of years.

Data stewardship contract clauses and international considerations

Generally, contracts are the most realistic method for mitigating risks, and in the context of data stewardship, this general rule applies. ATPs should remain resilient and update standard contracts as their business operations, agricultural technologies, and relevant laws change. Business practices also should be aligned with contracts and written policy statements.

Data stewardship contract clauses

The two provisions provided below relate to how the parties apportion risk between one another. The first is an *indemnification* clause and the second is a *limitation of liability* clause. These provisions are more essential than novel – that is to say, these provisions are common in most commercial contracts. In the context of transaction where data is cornerstone, counsel for ATPs should consider modifying the 'boilerplate' to provide robust protection for the specific risks related to the types of data and methods of collection.

Indemnification

An indemnification clause provides information related to which party to the contract will defend certain claims that arise as a result of the parties' agreement. For example, an ATP may choose provide certain indemnifications related to its products or services as a business proposition because the ATP has a comfortable level of assurance that the likelihood of such claims arising is low. Typically, an indemnification clause is negotiated when both parties are equally sophisticated, and it will be modified according to the specifics of the agreement and bargaining power of the parties.

---

[29] *See, e.g.,* National Congress of Brazil (2001). Financial institutions confidentiality act (105/2001); National Congress of Brazil (2011). Credit information law (12.414/2011).
[30] The Federal Constitution of Brazil, Art. 5, X (1988).
[31] National Congress of Brazil (1990). Consumer protection code, Art. 43 para 3.
[32] Marco Civil da Internet, Art. 8

Please note that indemnification clauses may not be enforceable in all states or countries. Certain conduct also can invalidate an indemnification provision. Also, please consider dictating the specifics of how the indemnification will function in an attached exhibit, identifying who controls the defense in the event of litigation and other procedures regarding communication and related obligations.

Sample indemnification clause (drafted for farmer/customer benefit):[33]

"[AGRICULTURAL TECHNOLOGY PROVIDER] WILL DEFEND, INDEMNIFY AND HOLD HARMLESS [AGRIBUSINESS], [AND AGRIBUSINESS' [PARENT COMPANY] AND [ITS/THEIR] SUBSIDIARIES, AFFILIATES, AND [ITS/THEIR] RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUCCESSORS AND PERMITTED ASSIGNS] (INDIVIDUALLY, A "QUALIFYING INDEMNITEE") FROM AND AGAINST ALL LOSSES, DAMAGES, LIABILITIES, DEFICIENCIES, ACTIONS, JUDGMENTS, INTEREST, AWARDS, PENALTIES, FINES, COSTS OR EXPENSES OF WHATEVER KIND, INCLUDING REASONABLE ATTORNEYS' FEES, THE COST OF ENFORCING ANY RIGHT TO INDEMNIFICATION HEREUNDER AND THE COST OF PURSUING ANY INSURANCE PROVIDERS, ARISING OUT OF OR RESULTING FROM ANY THIRD-PARTY CLAIM AGAINST ANY QUALIFYING INDEMNITEE ARISING OUT OF OR RESULTING FROM [AGRICULTURAL TECHNOLOGY PROVIDER'S] FAILURE TO COMPLY WITH ANY OF ITS OBLIGATIONS UNDER [INSERT APPROPRIATE SECTION NUMBER(S), FOCUSING ON PROVISIONS RELATED TO DATA STEWARDSHIP, PARTICULARLY DATA SECURITY].

Limitation of liability

A limitation of liability clause provides information related to the parties' agreement regarding under what circumstances liability will be limited. For example, an ATP that provided an indemnification clause for the benefit of its farmer or customer may also include a limitation of liability clause, placing a monetary cap on recoverable damages, and excluding certain categories of damages.

Please note that a limitation of liability clause may not be enforceable in all jurisdictions. For example, some jurisdictions may invalidate a limitation of liability provision on the grounds that it imposes an unreasonable limitation on damages.

Sample limitation of liability clause (drafted for agricultural technology provider)

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL [AGRICULTURAL TECHNOLOGY PROVIDER] [OR ITS AFFILIATES,] [OR ANY OF [ITS/ THEIR] RESPECTIVE LICENSORS] [OR SERVICE PROVIDERS,] HAVE ANY LIABILITY ARISING FROM OR RELATED TO YOUR USE OF OR INABILITY TO USE THE [ATP TOOL/APPLICATION] [OR THE [CONTENT] AND SERVICES FOR:]

[33]The text contained in [brackets] within this section does not constitute legal advice or otherwise create an attorney-client relationship. The examples provided either are notes and instructions or optional text examples that should be modified by legal counsel to reflect the particular parties and circumstances of the relevant agreement. Please consult your attorney.

(a) PERSONAL INJURY, PROPERTY DAMAGE, LOST PROFITS, COST OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF GOODWILL, BUSINESS INTERRUPTION, COMPUTER FAILURE OR MALFUNCTION OR ANY OTHER CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL OR PUNITIVE DAMAGES

(b) DIRECT DAMAGES IN AMOUNTS THAT IN THE AGGREGATE EXCEED THE AMOUNT ACTUALLY PAID BY YOU FOR THE [ATP TOOL/APPLICATION.]

THE FOREGOING LIMITATIONS WILL APPLY WHETHER SUCH DAMAGES ARISE OUT OF BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE OR COMPANY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF THE APPLICABLE JURISDICTION DOES NOT ALLOW CERTAIN LIMITATIONS OF LIABILITY, THOSE LIMITATIONS ALLOWABLE WILL APPLY.

Although managing risks with good contract drafting is important, it is not alone sufficient to manage applicable risks. Thus, other contract provisions, as well as best practices should be considered and deployed, including those specific to international contracting.

International considerations for contracting

ATPs that contact with parties in different countries can create unanticipated issues that can have a dramatic, and sometimes unwanted, effect for all involved. Consequently, it is imperative to be aware of certain rules and avoid the common pitfalls presented below.

United Nations Convention on Contracts for the International Sale of Goods

The UN Convention on Contracts for the International Sale of Goods ("**CISG**") is a model law. Model laws seek to strike a balance between parties and serve as blueprint for jurisdictions that have yet to grapple with certain issues. The CISG was developed to lower barriers for international trade by eliminating uncertainties that arise from using unfamiliar domestic laws. The CISG is in the form of a treaty and as of December 29, 2015, it has been adopted by eighty-four (84) Contracting States, including the United States, Mexico, Canada, Germany, China (PRC), the Russian Federation, Ukraine, and Brazil.

Scope of Application – when does it apply to ATPs?

Despite the fact that parties seldom mention CISG and instead select domestic laws to govern agreements, Article 1 of the CISG provides that the Convention will automatically apply to contracts for the sale of goods between parties in different Contracting States. Crucially, "goods" under the convention may be construed broadly to favor the application of the CISG to a mixed contract – that is a contract that contemplates a mixed use of hardware and software components. Thus, ATPs should be aware of how to avoid and invoked the CISG.

Many international parties have selected laws of their domestic domicile, yet tribunals repeatedly apply the CISG because ratified treaties are incorporated into the domestic laws

of a Contracting State. An example can be found in the *Agricultural products and cereals case.* There, the Foreign Trade Court of the Serbian Chamber of Commerce determined that the CISG applied to a Serbian and Bosnia and Herzegovina agricultural products and grains debt dispute where the parties contract provided that Serbian law should govern.[34] The rationale provided by the tribunal was that for disputes arising from the sale of international goods, Serbian's controlling law is that of the CISG because in April 1992 Serbia signed the Convention essentially incorporating the CISG into Serbian law.

Derogation of Convention

Although application of the CISG is favored and the CISG is considered among the most successful and utilized Conventions, it does not always achieve its goal of reducing uncertainty. International tribunals may not follow the majority rules interpreting the CISG.[35] Fortunately, the CISG values party autonomy, and Art. 6 parties may exclude, in whole or part, the application of the CISG.

ATPs with their legal counsel should make such application and derogation (deviation) determinations ahead of time and make such intentions clear. If parties fail to exclude the CISG (which *may* not be a prudent decision), the differences in the controlling contract regime, may adversely affect the parties because the CISG codifies rules that are often much different that of US law.

To exclude the Convention, the contract must be explicit:

"THE PARTIES HEREBY AGREE THAT THE UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS WILL NOT APPLY TO THIS CONTRACT [AS TO SECTIONS [list section]]. [INSERT APPLICABLE CHOICE OF LAW CLAUSE]."

Ultimately, this section is about legal certainty which, although difficult to achieve, is more likely if good contract drafting practices are followed.

Conclusion

Data stewardship, including data ownership, privacy and security, involves balancing risks against rewards. Notably, data stewardship laws and related enforcement actions are on the rise in the U.S. and internationally, as are private lawsuits. Prudent ATPs will develop best practices related to all aspects of data stewardship – that is, companies should not solely rely on good contract drafting. Yet, contracts are a crucial (and practical) start to any data protection scheme. They must be carefully drafted, especially if data will flow across borders. Thus, to limit the risk of substantially diminishing the value of data as an asset, companies must implement best practices and take into account the complexities of the international arena.

---

[34] *Serbia v. Bosnia & Herzegovina (2010).* Foreign Trade Court of Arbitration. http://cisgw3.law.pace.edu/cases/100506sb.html. Accessed (*Agricultural products and cereals case*).

[35] *See, e.g., Industrias Magromer Cueros y Pieles S.A. v. Sociedad Agrícola Sacor Ltda (2008).* Supreme Court of Chile. http://cisgw3.law.pace.edu/cases/080922ch.html. Accessed 25 May 2016 (Rejecting the CISG as applicable to international sale of goods when parties have not mentioned).

References

15 U.S.C. § 45 (2006). Federal Trade Commission Act.

15 U.S.C. §6801 (2011). The Financial Services Modernization Act.

42 U.S.C. § 1301 (1997). The Health Insurance Portability and Accountability Act.

Ag Data Transparency Evaluator. American Farm Bureau Federation. http://www.fb.org/agdatatransparent/. Accessed 25 May 2016.; AgGateway (2014). Data privacy and use whitepaper (draft). AgGateway. http://s3.amazonaws.com/aggateway_public/AgGatewayWeb/WorkingGroups/Committees/DataPrivacySecurityCommittee/Data%20Privacy%20and%20Use%20Whitepaper%20v3.5.pdf. Accessed 25 May 2016

Ag Gateway's Committee on Data Privacy & Security (2014). AgGateway Corporation. http://www.aggateway.org/WorkingGroups/Committees/DataPrivacySecurity.aspx Accessed 25 May 2016.

Agricultural Data Coalition (2016). Agriculture data: Putting farmers in the driver's seat. Agricultural Data Coalition. http://agdatacoalition.org/. Accessed 25 May 2016.

American Farm Bureau Federation (2016) Privacy and security principles for farm data. American Farm Bureau Federation. http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf. Accessed 25 May 2016.

Cal. Civil Code §1798.81.5.

Committee on Agriculture (2015). Big data and agriculture: Innovation and implications. U.S. House of Representatives. http://agriculture.house.gov/uploadedfiles/10.28.15_hearing_transcript.pdf. Accessed 25 May 2016

Critical Infrastructure Partnership Advisory Council (2011). Annual report. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/cipac/cipac-annual-2011.pdf. Accessed 25 May 2016.

De Hert, P. and Papakonstantinou, V. (2015). The data protection regime in China. European Parliament, Directorate-General for Internal Policies. http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf. Accessed 25 May 2016.

Faria, J. A. E., Tavares, A., & Sanders, G. (2015). Legal guide on contract farming. UNIDROIT, FAO, IFAD. http://www.fao.org/3/a-i4756e.pdf. Accessed 25 May 2016.
The Federal Constitution of Brazil, Art. 5, X (1988).

Federal Trade Commission (2016). Protecting consumer privacy press releases. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. Accessed 25 May 2016.

Guang Dong Light Headgear Factory Co v. ACI International, 521 F. Supp. 2d 1153 (2007).

Hurst, B. (2015). Big Data and Agriculture: Innovation and Implications. (2015). American Farm Bureau Federation. http://agriculture.house.gov/uploadedfiles/10.28.15_hurst_testimony.pdf. Accessed 25 May 2016.

Industrias Magromer Cueros y Pieles S.A. v. Sociedad Agrícola Sacor Ltda (2008). Supreme Court of Chile. http://cisgw3.law.pace.edu/cases/080922ch.html. Accessed 25 May 2016.

Jackson, L., Bornstein, J., Detlefsen, C., Gordon, R., Durkovich, C. (2015). Food and agriculture sector-specific plan. FDA, USDA, Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf. Accessed 25 May 2016.

Marco Civil da Internet, Art. 8.

Ministry of Industry and Information Technology (2013). Telecom and Internet users' personal data protection, Art. 8, 9, 15, 16.

National Congress of Brazil (1990). Consumer protection code, Art. 43 para 3.

National Congress of Brazil (2001). Financial institutions confidentiality act (105/2001).

National Congress of Brazil (2011). Credit information law (12.414/2011).

11th National People's Congress (2012). Decision of the National People's Congress on strengthening the network information protection. http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm. Accessed 25 May 2016.

National Strategy for Trusted Identities in Cyberspace. Appendix A-Fair information practice principles. NIST. http://www.nist.gov/nstic/NSTIC-FIPPs.pdf. Accessed 25 May 2016.

RSA Conference Speakers (2016). Nils Rodday. EMC Corporation. http://www.rsaconference.com/speakers/nils-rodday. Accessed 25 May 2016.

Serbia v. Bosnia & Herzegovina (2010). Foreign Trade Court of Arbitration. http://cisgw3.law.pace.edu/cases/100506sb.html.

Sloan, P. and Delgadillo, C. (2015). FTC enforcement of data security. http://www.huschblackwell.com/~/media/files/businessinsights/businessinsights/2015/05/whitw%20paper%20ftc%20enforcement%20of%20data%20security/whitepaper_ftcenforcementofdaftcenforce.pdf. Accessed 25 May 2016.

State Administration of Industry and Commerce (2015). Measures for punishments against infringements on consumer rights and interests.