INTELLECTUAL PROPERTY ISSUES IN CANADIAN AGRICULTURE

Keystone Agricultural Producers/
Pro Bono Students Canada

INTRODUCTION

The intention of this document is to provide a broad overview of topics related to protection of data collected from farming equipment and precision farming services. This document will discuss different types of data collected; relevant privacy legislation in Canada and internationally; copyright protection for databases; contractual protections; and trade secrets. Ideally, this manuscript will offer a broad overview of several topics pertaining to information collected as a result of agricultural technologies, and provide avenues for further research.

PBSC University of Manitoba volunteers would like to thank James Battershill (General Manager, Keystone Agricultural Producers) and Robert A. Watchman (Partner, Pitblado Law LLP) for their supervision and guidance on this project.

Please note: this document does not contain legal advice. Pro Bono Students Canada is a student organization. This document was prepared with the assistance of PBSC University of Manitoba law student volunteers. PBSC students are not lawyers and they are not authorized to provide legal advice. This document contains general discussion of certain legal and related issues only. If you require legal advice, please consult with a lawyer.

COLLECTION OF DATA

Brianna Bogucki

What is precision farming?

Precision farming is designed to maximize the yield of crops, both within single fields and between different fields. Generally precision farming has both temporal (time) and special (location) components. This combination of components that vary between and within individual fields can make optimizing crop yield while minimizing the resources used a difficult proposition. To maximize yield, a farmer must know a) which conditions remain stable during a given growing season b) which conditions vary throughout the growing season and c) why some sections of their field might be struggling while other areas flourish.[1]

How is data collected?

One way for a farmer to get a bird's eye view of their fields (and the condition of the crops growing there) is through the use of satellite- and aircraft-based remote sensors.[2] These sensors can measure wavelengths of light reflected from the fields. Certain wavelengths indicate crop health, while others indicate areas where the crop may struggle. Another advantage to satellite- and aircraft-based imaging is that it is quick; a farmer can survey their entire property in minutes, while driving through it and collecting similar data could take hours.[3] Probably the greatest advantage to satellite- and aircraft-based imaging is the accuracy and consistency of data collection. Consistent, regular data from a satellite or UAV is easier to analyze than what a farmer remembers from memory or jots down on a note pad from a visual field check. Ultimately, the majority of the data's value lies in its consistent and accurate aggregation, and subsequent analysis.

In order to maximize the yield-to-resource ratio, both differences in crop yield over time and location must be measured. Arguably, the main technology that has come to affect precision farming is the creation of Geographic Information Systems (GIS) and Global Positioning Systems (GPS), which allow producers to identify their exact position in their field, and the relative positions of topographical features that might impact plant growth due to elements such as elevation, slope, and water drainage.[4] Some GPS systems allow positions of vehicles within a field within 2 cm accuracy.[5] Additionally, automated steering systems (including assisted steering systems where the GPS shows the driver where to go; automated steering systems that automatically steer the vehicle, allowing the producer to focus on other equipment while their hands are off the wheel; and intelligent guidance systems that provide steering patterns based on the characteristics of a particular field) help improve accuracy of planting, application of fertilizer and pesticides, and harvesting.[6] Yield monitors also allow mapping of yields as a whole when coupled with GPS receivers.[7]

---

[1] David Herring, "Precision Farming" (29 January 2001), *NASA Earth Observatory* (blog), online: <http://earthobservatory.nasa.gov/Features/PrecisionFarming/>

[2] Ibid.

[3] Ibid.

[4] Thomas C.Kaspar et al., "Relationship Between Six Years of Corn Yields and Terrain Attirbutes" (2003) 4 Precision Agriculture at 87.

[5] CEMA aisbl – European Agricultural Machinery, "Precision Farming: Key Technologies & Concepts" (n.d.), *CEMA* (blog), online: <http://cema-agri.org/page/precision-farming-key-technologies-concepts>

[6] Ibid.

[7] Tom Goddard, "What Is Precision Farming?" (17 October 2001), *Alberta Agriculture and Forestry* (blog), online: <http://www1.agric.gov.ab.ca/$department/deptdocs.nsf/all/sag1951>

In addition to relatively stable topographical factors, other factors such as pests, disease, incorrect application of resources, and the amount of precipitation in a given growing season can also affect the yield of a field.[8] In order to combat these transient factors, variable systems such as variable rate fertilizers and pesticide sprayers may be used in conjunction with mapping tools that allow producers to note specific areas that require spraying or fertilization, and target those areas rather than spraying a whole field.[9] This can be done through variable rate technology (VRT)[10] that can vary the rate of application.

Another important component in precision farming are various sensors. These sensors can evaluate crop moisture, nutrients, salinity, and a host of other factors, and can often be integrated into a precision farming system to allow sensors to communicate with applicators (ex. a tractor and a farm office). This allows for the development of a database of data, the analysis of which can be conducted through sophisticated computer systems to precisely analyse what should have been done, what was actually done, and the results. This analysis can give farmers more accurate pictures of what the crops actually need to maximize yield (and which sections of the field need what, and how much), rather than speculating on what the field as a whole might need.[11] These effects can be especially significant in areas where fertilizer use and irrigation need to be strictly controlled.[12]

The consequence of having so much data collected is that it requires significant computing power to store and analyse it. Companies such as John Deere can collect data into customer accounts, allowing customers to access the information later through an online web portal. John Deere has provided a document that specifies what kinds of data they collect, when and how it is collected, and how the company will use the data to generate results useful to the producer. More information on what kind of data (including machine data, production data, and industry-specific data) is collected can be found online.[13] Essentially, however, it means that the data collected by John Deere equipment is held on the John Deere website, a site owned and operated by John Deere.

What are the concerns with how and by whom data is collected/compiled?

The main concerns stemming from the collection of this vast data is what it will be used for, and by whom. Who owns the data collected, the farmer that collected the data, or the company that mandated its collection? Can the company sell the producer's data to third parties?[14] When farmers produce data specifically for companies, are they entitled to feedback based on the results of the findings?

Privacy concerns surround the collection and use of data, particularly when one company collects the data, and then subsequently forwards it to a second, different company for analysis. It would be advisable for anyone who uses equipment capable of generating GPS data to consent to the collection of that data, regardless of which company the data is being sent to for analysis. Afterwards, a separate release should be signed in order to transfer/disclose the collected data to the company performing the analysis.

---

[8] *Supra* note 4 at 87.
[9] *Supra* note 7.
[10] *Supra* note 5.
[11] *Supra* note 1.
[12] *Ibid.*
[13] https://www.deere.ca/privacy_and_data/docs/DataTypeInventory.pdf
[14] Lisa Heacox, "Ensuring Data Privacy in Agriculture" (16 February 2016), *PrecisionAg* (blog), online: <http://www.precisionag.com/data/ensuring-data-privacy-in-agriculture/>

In addition to obtaining initial consent from data producers, access procedures should be implemented to control or restrict the viewing and use of collected data. Consideration should also be given to what happens when an individual refuses to consent to data being collected, or provides consent but then later withdraws it. This should be contemplated in the agreement between the company producing the data and the company analyzing it.

Legal counsel, producers, large companies, and legislators are equally confused about the implications that precision farming data will have on the agriculture industries, and no answers are for certain. However, the most likely areas of law that will impact the future of agricultural data are privacy law, contract law, and possibly copyright law, with each offering different protections and weaknesses.[15]

[15] *Ibid.*

PRIVACY BASICS: PERSONAL INFORMATION AND LEGISLATION

Danielle Otto

What is the Personal Information Protection and Electronic Documents Act?

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is federal law that came into full force in 2004.[16] PIPEDA governs the collection, use, disclosure, and storage of personal information by private sector organizations.[17] The law requires that all organizations collecting personal information have a Privacy Officer on staff to monitor how this information is being used—that consent is being obtained at all stages (though some exceptions to the requirement of consent are set out in the Act), and that collection, use, and disclosure are kept within reasonable limits.[18]

In addition to mandating the existence of Privacy Officers, PIPEDA also gives individuals the right to know what information organizations have about them, and to file a complaint with the Office of the Privacy Commissioner (a federal ombudsperson),[19] in instances of suspected non-compliance with PIPEDA. Decisions of the Privacy Commissioner can be reviewed in Federal Court, and rare cases, appealed to the Supreme Court of Canada.[20]

Although some provinces have chosen to adopt their own legislative frameworks, PIPEDA is the private sector privacy legislation that applies in Manitoba.[21]

What is 'personal information'?

The definition of personal information under PIPEDA is very broad. Personal information is any information about an identifiable individual. This could be anything from the content of conversations,[22] to the location information collected from a smartphone.[23] The collection of statistics—raw numerical data— is not included in the definition, but it may nonetheless qualify if the information can be used in combination with another source to identify a specific person.[24]

For instance, the data collected from the GPS in a car, such as distance travelled, and braking speed is not *per se* personal information. But if you're driving a company car, and your employer knows that you are the individual generating that data – then it is personal information, and is subject to the safeguards in PIPEDA.

Why does it matter whether the information is personal?

[16] Office of the Privacy Commissioner, "Fact Sheet: Complying with the Personal Information Protection and Electronic Documents Act", (2014), online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_16_e.asp>.
[17] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Part 1 s2-4
[18] *Ibid* Note 17, ss. 5-7
[19] *Ibid* Note 17
[20] See for example Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, [2013] 3 SCR 733, 2013 SCC 62 (CanLII)
[21] Government of Manitoba, "FIPPA for the Public | FIPPA", (2016), online: <http://www.gov.mb.ca/chc/fippa/public_portal_home.html>. It should be noted that PIPEDA only applies to the extent that an organization is carrying out commercial activity, and does not apply to provincially-regulated employees.
[22] Morgan v. Alta Flights (Charters) Inc. 2005 FC 421, 2005 CarswellNet 2675
[23] PIPEDA Report of Findings #2014-008
[24] Order P12-01 – Information & Privacy Commissioner for BC, Schindler Elevator Company at para. 58

Subject to specific exemptions—for journalistic, research, or legal[25] purposes, PIPEDA prohibits organizations from collecting, using, or disclosing personal information without consent and knowledge. PIPEDA also requires that when consent is given, organizations restrict their use and disclosure to the original purpose for which the individual consented. Therefore, it is important to read and understand contracts for purchase and sale in order to establish the limits of the consent that has been, or will be, granted by executing the contract.

To use the precision farming example, if a producer gives consent to John Deere to collect and use their data for the purpose of creating a yield map that will assist in decision-making, it would violate the provisions of PIPEDA for John Deere to sell the resulting yield data to Monsanto, without specifically seeking consent for that activity. The producer WOULD have recourse for this violation.

They could inquire with the company's privacy officer to find out how information was used, file a complaint with the Office of the Privacy Commissioner—which would examine the evidence to determine if a violation occurred, and issue recommendations for how the company can better comply with its PIPEDA obligations in the future.

Ultimately the producer could seek review of the Privacy Commissioner's decision in Federal Court, and that may prevent any unauthorized disclosure in the future.

Is precision agriculture covered by PIPEDA?

It might not be. However, that question is yet to be specifically decided.

Certainly, agricultural tech companies would fall within the definition of an 'organization', and thus they could be required to comply with PIPEDA. But in the context of precision agriculture, the difficulty is illustrating that the information falls within the definition of 'personal'

GPS data is sometimes recognized as personal, even though it's not in itself about a person. This was established by a decision of the of Privacy Commissioner under PIPEDA in 2006.[26] The commissioner found that the GPS data collected from company vehicles is personal information, and thus the employer (an elevator company) couldn't use it for discipline purposes without the employee's knowledge. This was true, despite the fact that the actual information being collected was the speed, location, and acceleration of a vehicle that was company-owned.[27] The commissioner cautioned the elevator company against "function creep",[28] that is, implementing the technology for business efficiency reasons, but over time, moving toward using it for employee discipline, and other purposes it did not make known to employees.

The information was personal because the employer could use other information it already had to link it with an identifiable individual. This bodes well for producers, because it means that the numerical data collected from yield mapping, auto-steering, and other GPS-based precision agriculture technologies, is arguably personal—whether or not it relates to the producer as a person. As well, the commissioner's warning against function creep is potentially

---

[25] *Supra* note 17 ss. 5-7, s. 7
[26] PIPEDA Case Summary No. 351, Re, 2006 CarswellNat 5577
[27] *Ibid* note 26, at 5
[28] *Ibid* note 26, at 2

to the producer's benefit, especially in a circumstance where they consented to limited collection, and use, but find their yield data has been sold to a third-party.

However, a 2012 case, filed under British Columbia's PIPEDA-equivalent legislation, had very similar facts as the one decided in 2006, but resulted in the opposite outcome. That case applied a newer, and much narrower definition of 'personal information' from the Federal Court of Appeal. Where previously, it had only mattered that the information be 'about'[29] and identifiable individual, the new interpretation says that personal information isn't just any information that can be linked to someone, but only information that is of a truly personal nature the individual can reasonably expect to be kept private, in order to advance goals like maintaining dignity.[30]

It was ultimately found that the GPS data did not fall within the employee's "zone of privacy" thus it could be collected and used after employees were notified, but consent was not explicitly required.[31]

This ruling presents a problem for a farmer who is hoping to argue that their precision agriculture data should fall under PIPEDA's umbrella. It's easy to see that things like health information, and individual whereabouts come within the sphere. But this narrowing of the definition of personal, means that even when there is clear connection to specific individual, the information may not be private enough to justify PIPEDA safeguards. Just as vehicle speeds and acceleration may not qualify, companies could argue the land elevations, and the weight of grain harvested does not come within the "zone of privacy".

And even if the precision agriculture data was deemed to be sufficiently private to be included in PIPEDA, producers face an addition barrier: namely the requirement that the information be about identifiable individual.

Numerical GPS data from a variety of non-farming contexts has been covered by PIPEDA. The cases on smartphone use, and company vehicles clearly show that. But in all of those instances, it is very clear who exactly is generating the data. This may not be the case when machinery is used by a group of individuals farming together, or the piece of equipment in question is owned by an incorporated farm. It may be impossible to establish any link between an identifiable individual—because it wouldn't necessarily be known who was driving the tractor or combine when a particular piece of data created.

Call-centre employees have successfully argued that the recordings of their work calls are personal information despite being created by a corporation[32], but that situation is significantly more clear-cut than the kind of information precision agriculture generates. For a single producer, who farms alone, there may be less of a difficulty in asserting that he is the 'identifiable individual' that PIPEDA requires, but for many producers this won't be the case.

What's the bottom line?

PIPEDA, if it were applied to precision agriculture, would offer producers significant protection for their information. In fact, American legal commentary has recommended that PIPEDA should be used as model for creating privacy legislation that specifically addresses

[29] See Dagg *v*. Canada (Minister of Finance), [1997] 2 S.C.R. 403
[30] See The Information Commissioner of Canada v. NAV CANADA 2006 FCA 157 at para. 52-53
[31] Order P12-01 – Information & Privacy Commissioner for BC, Schindler Elevator Company at para. 184
[32] PIPEDA Case Summary #220 2003 CarswellNet 5818

precision agriculture, because of the way it limits the collection, use, and disclosure of information at all stages; and also because producers would then have access to privacy liaison in each of the companies they deal with.[33]

But it is unclear from the cases that have been decided so far, that PIPEDA applies to precision agriculture. The legislation doesn't specifically anticipate the problems associated with this technology, and so the point can be argued either way.

[33] Jacob Strobel, "Agriculture Precision Farming: Who Owns the Property of Information?" 19:2 (2014) Drake J. Agric. L., 250-251.

OTHER LEGISLATION PERTAINING TO DATA COLLECTION AND PRIVACY

Jane Harrington

What do privacy laws in other jurisdictions look like?

The big issue with farm data collection pertains to the ability to define the type of data that is collected. Precision farming equipment can collect two types of data: personal and aggregated. The laws surrounding personal data collection are for the most part, established and clear in most jurisdictions. In Canada, PIPEDA covers the protection of personal information. Many other jurisdictions have similar Acts.[34]

What is "big data"? The automotive industry model.

Precision farming equipment is capable of collecting "aggregated" or anonymous data. This data, although it may provide much information, is in theory, incapable of identifying individuals. This data is sometimes referred to as "big data" and there has been much interest in this data from a variety of industry. For example, in the automotive industry, essentially all vehicles created post 2010 are "connected", meaning they relay information wirelessly to the automaker, which has the potential to be sold to third parties. The connected automotive industry is expanding and it is predicted that by 2020 it will exceed 14.5 billion dollars.[35] The automotive industry offers a good analogy to the farm equipment industry. It is promising to see that the automotive industry has taken proactive steps to protect the privacy of its customers. On a basic level, consumers are concerned about where the data is going. Maybe more insidious, financing companies have appreciated the usefulness of obtaining car data to inform their lending decision making.[36] In September 2015, the United States congress reported the *Driver Privacy Act* 2015 for consideration of the Senate: [37]

> (Sec. 2) Declares that any data in an event data recorder required to be installed in a passenger motor vehicle (as provided for under Department of Transportation [DOT] regulations concerning the collection, storage, and retrievability of onboard motor vehicle crash event data) is the property of the owner or lessee of the vehicle in which the recorder is installed, regardless of when the vehicle was manufactured.
>
> Prohibits a person, other than the owner or lessee of the motor vehicle, from accessing data recorded or transmitted by such a recorder unless:

---

[34] For a list of privacy laws from different jurisdictions, see DLA Piper, "Data Protection Laws of the World" (2016), *Data Protection Laws of the World* (website), online: <https://www.dlapiperdataprotection.com/#handbook/world-map-section>. eBook also available for download.

[35] Christopher Wolf, "The Auto Industry Is Serious About Connected Car Privacy" (25 March 2015), *Chronicle of Data Protection: Privacy & Information Security News and Trends* (website), online: <http://www.hldataprotection.com/2015/03/articles/consumer-privacy/the-auto-industry-is-serious-about-connected-car-privacy/>

[36] John A. Rothchild, "Losing Control: Who Owns Your Devices Now That They Are Connected to the Internet? An Introduction to the Internet of Things" (Presentation delivered at the ABA Business law Spring Meeting, San Fransisco, California, 17 April 2015) [online PDF]: <http://www.americanbar.org/content/dam/aba/events/business_law/2015/04/spring/losing-control-201504.authcheckdam.pdf>

[37] U.S., bill, S, *Driver Privay Act of 2015* 114th Cong, 2015, S. 766, reported without amendment. Retrieved from: <https://www.congress.gov/bill/114th-congress/senate-bill/766>

- a court or other judicial or administrative authority authorizes the retrieval of such data subject to admissibility of evidence standards;
- an owner or lessee consents to such retrieval for any purpose, including vehicle diagnosis, service, or repair;
- the data is retrieved pursuant to certain authorized investigations or inspections of the National Transportation Safety Board or DOT;
- the data is retrieved to determine the appropriate emergency medical response to a motor vehicle crash; or
- the data is retrieved for traffic safety research, and the owner's or lessee's personally identifiable information and the vehicle identification number are not disclosed.

Is farmer privacy being accounted for in the agriculture industry like driver privacy is being accounted for in the automotive industry?

Within the precision farming equipment industry, no act similar to the *Driver Privacy Act* has yet been introduced. The American Farm Bureau has taken some steps towards protecting farmer privacy. In May 2015 they prepared *Privacy and Security Principles for Farm Data* (PSPFD).[38] These are some key points from the agreement:

> ***Ownership:*** We believe farmers own information generated on their farming operations. However, 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 (Agriculture Technology Provider) etc. The 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.
>
> ***Transparency and Consistency:*** ATPs shall notify farmers about the purposes for which they collect and use farm data. They should provide information about how farmers can contact the ATP with any inquiries or complaints, the types of third parties to which they disclose the data and the choices the ATP offers for limiting its use and disclosure.
>
> ***Terms and Definitions:*** Farmers should know with whom they are contracting if the ATP contract involves sharing with third parties, partners, business partners, ATP partners, or affiliates. ATPs should clearly explain the following definitions in a consistent manner in all of their respective agreements: (1) farm data; (2) third party; (3) partner; (4) business partner; (5) ATP partners; (6) affiliate; (7) data account holder; (8) original customer data. If these definitions are not used, ATPs should define each alternative term in the contract and privacy policy. ATPs should strive to use clear language for their terms, conditions and agreements.

The document was signed by over 20 companies who manufacture or sell equipment or services that have the capacity to collect farming data, including John Deere, CropMetrics, Farmobile LLC, and OnFarm. However, it was signed on a voluntary basis and doesn’t refer to any specific law. With respect to personal data, the US has adopted data breach notification laws in 47 states. In California, anyone who collects data through their products must include an

[38] American Farm Bureau, “Privacy and Security Principles for Farm Data” (5 March 2015), *The Voice of Agriculture: American Farm Bureau Association* (website), online: <http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf>

opt-out option in their contract. More information on the *Privacy and Security Principles for Farm Data* will be discussed in the 'Contract Law Basics' section of this document.

The U.S. Federal Trade Commission has initiated legal action against companies that experienced data breaches. In ***FTC v. Wyndham*** the U.S. Federal Court of Appeal ruled in favour of the FTC, finding that data security failures led to three data breaches at Wyndham hotels in less than two years. According to the complaint, those failures resulted in millions of dollars of fraudulent charges on consumers' credit and debit cards – and the transfer of hundreds of thousands of consumers' account information to a website registered in Russia.[39]

How is producer privacy being dealt with internationally?

The United States, with its large agriculture industry, seems to be taking the lead on the matter of privacy and data collection from "connected" equipment. In Australia, the *Privacy Amendment Act* 2012 was introduced to amend the previous *Privacy Act* 1988, however it does not specifically mention precision agriculture.[40]

John Deere Canada appears to give their customers an option to opt-out of the transmittance of their data however, Lance Formwalt, a lawyer with Seigfried Bingham, presented a webinar in which he states that although companies may have this opt-out option it's important to pay attention to the exceptions.[41] It's in the best interest of the companies to acquire aggregated data even if they don't have immediate plans to sell it. As technology increases, the potential effects that aggregated data have, are limitless.

Here in Canada it's essential for farmers to read carefully through their contracts as this is a new area of privacy law that has yet to be addressed by legislature.

[39] Lesley Fair, "Third Circuit Rules in FTC v. Wyndham Case" (25 August 2015), *Federal Trade Commission: Protecting America's Consumers* (blog), online: <https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case>
[40] Jonathan Brandon, "Australia's Data Privacy Laws Come into Force as Providers Struggle with Data Management" (12 March 2014), *Business Cloud News* (blog), online: <http://www.businesscloudnews.com/2014/03/12/australias-privacy-laws-come-into-force-as-csps-struggle-with-data-management/>
[41] Lance Formwalt, "Webinar: Data Privacy and Protection: What Dealers Need to Know to Avoid Risk" (Webinar published online 24 April 2015) [video]: <http://www.precisionfarmingdealer.com/webinar-data-privacy-2015>

COPYRIGHT PROTECTION FOR DATABASES

Ashley Kaufmann

Are databases (and the information stored on them) protected by copyright legislation?

The *Copyright Act* of Canada defines compilation in the following way:

> (a) a work resulting from the selection or arrangement of literary, dramatic, musical or artistic works or of parts thereof, or
>
> (b) a work resulting from the selection or arrangement of data;[42]

In addition to the *Copyright Act*, the *North American Free Trade Agreement*[43] and the World Trade Organization *Agreement On Trade-Related Aspects Of Intellectual Property Rights* (TRIPS)[44] set out a test of originally used to determine if a database can be protected by copyright. TRIPS states:

> Article 10
> *Computer Programs and Compilations of Data*
> 1. Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).
> 2. Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.[45]

NAFTA, which binds Canada, the U.S. and Mexico, states the following:

> Article 1705: Copyright
> 1. Each Party shall protect the works covered by Article 2 of the Beme Convention, including any other works that embody original expression within the meaning of that Convention. In particular:
>
> (a) all types of computer programs are literary works within the meaning of the Berne Convention and each Party shall protect them as such; and
>
> (b) compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations, shall be protected as such.
>
> The protection a Party provides under subparagraph (b) shall not extend to the data

[42] Copyright Act (R.S.C., 1985, c. C-42)
[43] North American Free Trade Agreement Between the Government of Canada, the Government of the United Mexican States and the Government of the United States of America (NAFTA), [1994] (accessed November 1, 2015).
[44] World Trade Organization, “Trade-Related Aspects of Intellectual Property Rights”, [1994] (accessed November 1, 2015).
[45] *Ibid*.

or material itself, or prejudice any copyright subsisting in that data or material.[46]

Based on the Copyright Act of Canada, as well as NAFTA and TRIPS, in order for a claim of copyright over a database to succeed, the compilation must constitute an intellectual creation. In order to qualify as an intellectual creation a compilation must embody an original expression and must involve a process of creative selection or arrangement. While the description in statute remains quite vague, Canadian courts, as well courts in other jurisdictions, have further clarified the creativity requirement for database copyright.

What does case law say about interpreting the above statutes?

There have been several notable cases that have prompted Canadian courts to clarify the law set out in statute surrounding copyright of compilations. The case of ***Tele-Direct (Publications) Inc. v. American Business Information Inc***[47]***.***, which concerned a publication of the Yellow Pages, addressed the issue of copyright over a compilation of data. In ***Tele-Direct***, the plaintiff did not claim copyright over the raw data it received from the telephone provider, however did claim copyright in respect to the organization of the information, which it received from the telephone provider in a disorganized state, and in respect to the collection of additional data. In this case, the Federal Court of Appeal stated in very clear language that the informational content and organizational scheme of the Yellow Pages, cannot be protected by copyright law in Canada.

Slumber-Magic Adjustable Bed Co. v. Sleep-King Adjustable Bed Co establishes the principles to be applied in determining whether copyright exists in a compilation[48]***.***, This case concerned a sales brochure comprised of parts of competitors brochures. In ***Slumber-Magic*** the British Columbia Supreme Court referred to the British Case of ***Ladbroke (Football), Ltd. v. William Hill (Football), Ltd.***[49]:

> So long as work, taste and discretion have entered into the composition, that originality is established. In the case of compilation, the originality requisite to copyright is a matter of degree depending on the amount of skill, judgment or labour that has been involved in making the compilation.[50]

Additionally, in ***Ladbroke*** the House of Lords stated:

> Where copyright is claimed in a compilation it is not the correct approach to dissect the work in fragments and, if the fragments are not entitled to copyright, then deduce that the whole compilation is not so entitled; rather, the court should canvass the degree of industry, skill or judgment which has gone into the overall arrangement[51].

In ***Tele-Direct*** the Federal Court of Appeal referred to ***Feist Publications Inc. v. Rural Telephone Service Co.***[52]***,*** a landmark case heard by the United States Supreme Court:

[46] NAFTA, *supra* note 43.
[47] *Tele-Direct (Publications) Inc. v. American Business Information Inc*. (1997), [1998] 2 F.C. 22, 37 B.L.R. (2d) 101
[48] *Slumber-Magic Adjustable Bed Co. v. Sleep-King Adjustable Bed Co*. (1984), [1985] 1 W.W.R. 112, 3 C.P.R. (3d) 81 (B.C. S.C.)
[49] *Ladbroke (Football) Ltd. v. William Hill (Football) Ltd.* (1964), [1980] R.P.C. 539, [1964] 1 All E.R. 465, [1964] 1 W.L.R. 273 (U.K. H.L.)
[50] *Supra* note 47, at para 5.
[51] *Ibid*.
[52] *Feist Publications Inc. v. Rural Telephone Service Co.* (1991), 111 S. Ct. 1282 (U.S. Kan.)

> [...] As mentioned, originality is not a stringent standard; it does not require that facts be presented in an innovative or surprising way. It is equally true, however, that the selection and arrangement of facts cannot be so mechanical or routine as to require no creativity whatsoever. The standard of originality is low, but it does exist [...] [at 1296][53]

In summary, the Canadian courts have established that compilations of material produced by others may be protected by copyright. However, in order for a compilation to be protected, the arrangement of the elements taken from other sources must be the product of some form of creativity, including thought, selection, and work.

How is this relevant to the Canadian farming industry?

A report on precision agriculture by the US National Academy of Sciences states: "If ownership cannot be or is not protected, there may be a chilling effect on the willingness of individuals to provide field and farm data to aggregate databases, whether publicly or privately established."[54]

Based on both existing statute and findings of Canadian courts, one may conclude that if a supplier of precision farming equipment or a regional group were to compile data from individual farmers' equipment, it would be possible to claim copyright for a database of information if the material was organized in a way that satisfies the requirement for an original intellectual creation. If one succeeded in claiming copyright over these databases, a supplier or group may be able to charge others for their use or share the information with third-parties, providing there are no other barriers in place. One such barrier is a confidentiality or non-disclosure agreement.

The most common effort to keep data private in the precision technology industry is through the use of contracts with farmers, including confidentiality agreements[55]. Companies, including John Deere, have included these confidentiality agreements to satisfy farmers' concerns about misappropriation of data collected through precision farming.

The following confidentiality clause is included in John Deere's terms and conditions for purchase orders:

> 26. CONFIDENTIALITY. This Order and any material transmitted herewith may contain information confidential or proprietary to Buyer, its subsidiaries or affiliates and such information is not to be used by Seller other than the purpose for which it was transmitted to Seller. *Seller shall hold such information in strictest confidence and not disclose such information to third parties without the prior, written consent of Buyer*. Seller will execute a confidentiality and non-disclosure agreement as required by Buyer.[56] [Emphasis added]

While the above clause mentions that the Seller is not to disclose Buyer information to third parties, it is important to note that these agreements do not guarantee confidentiality in every

---

[53] *Supra* note 47 at para 34.
[54] Committee on Assessing Crop Yield: Site-Specific Farming, Information Systems, and Research Opportunities, National Research Council, Precision Agriculture in the 21st Century: Geospatial and Information Technologies in Crop Management [1997] (National Academy Press: Washington D.C,) at 109.
[55] Jacob Strobel, "Agriculture Precision Farming: Who Owns The Property Of Information? Is It The Farmer, The Company Who Helps Consults The Farmer On How To Use The Information Best, Or The Mechanical Company Who Built The Technology Itself?" (2014), 19:2 Drake J of Ag. Law 247-248.
[56] "John Deere Purchasing Terms And Conditions**"** [2007], (Accessed January 20, 2016) https://jdsn.deere.com/wps/wcm/connect/71fad4004d1bd535930dbba912093b63/purchasing_terms_and_conditions_can_eng.pdf?MOD=AJPERES

situation due to their vagueness. As a result, some argue that confidentiality agreements are "insufficient for property data rights with respect to precision agriculture."[57]

[57] *Supra* note 55 at 248.

CONTRACT LAW BASICS:
FARMERS AND AGRICULTURE TECHNOLOGY PROVIDERS (ATPs)

Madison Urschatz

What information does the contracts between ATPs and farmers contain?

Contracts between Agriculture Technology Providers (ATPs) and farmers dictate how farm data will be managed.

The contract will identify:
- Who owns the farm data;
- Whether the ATP can collect, access or control the farm data;
- If the ATP is collecting farm data, how the data will be used; and
- Whether the ATP can sell or disclose farmer data to 3rd parties.

Therefore, the contracts between ATPs and farmers are very important.

Contracts may be consented to digitally or through manual signing, and often appear as Terms of Use.

What is *Privacy and Security Principles For Farm Data* (PSPFD)?

The *Privacy and Security Principles for Farm Data* is a set of principles that outlines how ATPs will contract with farmers. While the principles are not legally binding, the organizations listed in the section below have agreed to the following principles:[58]

> ***Education***: Grower education is valuable to ensure clarity between all parties and stakeholders. Grower organizations and industry should work to develop programs, which help to create educated customers who understand their rights and responsibilities. ATPs should strive to draft contracts using simple, easy to understand language.
>
> ***Ownership:*** We believe farmers own information generated on their farming operations. However, 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. The 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.
>
> ***Collection, Access and Control***: An ATP's collection, access and use of farm data should be granted only with the affirmative and explicit consent of the farmer. This will be by contract agreements, whether signed or digital.

[58] *Supra* note 38.

Notice: Farmers must be notified that their data is being collected and about how the farm data will be disclosed and used. This notice must be provided in an easily located and readily accessible format.

Transparency and Consistency: ATPs shall notify farmers about the purposes for which they collect and use farm data. They should provide information about how farmers can contact the ATP with any inquiries or complaints, the types of third parties to which they disclose the data and the choices the ATP offers for limiting its use and disclosure.
An ATP's principles, policies and practices should be transparent and fully consistent with the terms and conditions in their legal contracts. An ATP will not change the customer's contract without his or her agreement.

Choice: 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. If multiple options are offered, farmers should be able to choose some, all, or none of the options offered. ATPs should provide farmers with a clear understanding of what services and features may or may not be enabled when they make certain choices.

***Portability*:** Within the context of the agreement and retention policy, farmers should be able to retrieve their data for storage or use in other systems, with the exception of the data that has been made anonymous or aggregated and is no longer specifically identifiable. Non-anonymized or non- aggregated data should be easy for farmers to receive their data back at their discretion.

Terms and Definitions: Farmers should know with whom they are contracting if the ATP contract involves sharing with third parties, partners, business partners, ATP partners, or affiliates. ATPs should clearly explain the following definitions in a consistent manner in all of their respective agreements: (1) farm data; (2) third party; (3) partner; (4) business partner; (5) ATP partners; (6) affiliate; (7) data account holder; (8) original customer data. If these definitions are not used, ATPs should define each alternative term in the contract and privacy policy. ATPs should strive to use clear language for their terms, conditions and agreements.

Disclosure, Use and Sale Limitation: 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.

Data Retention and Availability: Each ATP should 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. The ATP should include a requirement that farmers have access to the data that an ATP holds during that data retention period. ATPs should document personally identifiable data retention and availability policies and disposal procedures, and specify requirements of data under policies and procedures.

***Contract Termination*:** Farmers should be allowed to discontinue a service or halt the collection of data at any time subject to appropriate ongoing obligations. Procedures for termination of services should be clearly defined in the contract.

***Unlawful or Anti-Competitive Activities*:** ATPs should not use the data for unlawful or anti- competitive activities, such as a prohibition on the use of farm data by the ATP to speculate in commodity markets.

***Liability & Security Safeguards*:** The ATP should clearly define terms of liability. Farm data should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure. Policies for notification and response in the event of a breach should be established.

Who has agreed to the PSPFD?[59]

Organization	Machine Brands Using Technology
AGCO	Challenger Fendt GSI Massey Ferguson Valtra
Ag Connections, Inc.	
AgSense	
AgWorks	
Ag Leader Technology	
American Farm Bureau Federation	
American Soybean Association	
Beck's Hybrids	
CNH Industrial	Case IH New Holland Agriculture New Holland Construction Rocky Mountain Equipment
Crop IMS	
CropMetrics	
Dow AgroSciences LLC	
DuPont Pioneer	
Farmoblie LLC	
Granular	
Grower Information Services Cooperative	
GROWMARK, Inc.	
Independent Data Management LLC	
John Deere	John Deere
Mapshots, Inc.	
National Association of Wheat Growers	
National Barley Growers Association	
National Cotton Council	
National Farmers Union	
National Sorghum Producers	

[59] *Supra* note 38.

North American Equipment Dealers Association	
OnFarm	
Raven Industries	Seedmaster
Syngenta	
The Climate Corporation – a division of Monstanto	
USA Rice Federation	
Valley Irrigation	
ZedX Inc.	

Are the contracts enforceable if I didn't read them?

Terms of use must be adequately communicated to customers to be enforceable. There are three ways terms of use are brought to a user's attention:[60]

1. **Click-Wrap**
    - A user agrees to the terms of the contract by clicking a button stating they "agree" or "accept."
    - Generally, click agreements have been found to be an effective method of providing notice under Canadian law.[61]

2. **Click-Wrap with Links to Terms**
    - A user agrees to the terms of the contract by clicking "agree" or "accept," however instead of displaying the agreement on that webpage, the user is provided an opportunity to open the terms of use on separate page.

3. **Browse-Wrap**
    - The agreement is placed on the website and users express their consent by continuing to use the website. So by simply using the site or service the customer is agreeing to the terms of use. This can appear as a tab stating "legal" or "privacy" on the bottom of a webpage.
    - While some US courts have found browse-wrap agreements are not binding due to insufficient notice,[62] Canadian courts have found browse-wrap agreements binding.[63]

Therefore, even if an individual does not read the terms of use, the terms are still likely to be enforceable if there are click-wrap or browse-wrap agreements in place.

Note:

- If an organization has agreed to the PSPFD they will only collect and access farm data with the affirmative and explicit consent of the farmer. Therefore, farmers are agreeing to click-wrap or click-wrap with link to terms, not browse-wrap.

[60] Nathan Schissel and Jade Buchanan, "Are Your e-Commerce Terms and Conditions Enforceable?" (19 August, 2015), *Technology Law Advisor* (blog), online: <http://technologylawadvisor.com/are-your-e-commerce-terms-and-conditions-enforceable/>
[61] See *Douez v. Facebook, Inc*., 2014 BCSC 953.
[62] See *Nguyen v. Barnes & Noble, Inc*., 763 F. 3d 1171 (9th.Cir. 2014).
[63] See *Century 21 Canada Limited Partnership v. Rogers Communications Inc.*, 2011 BCSC 1196 [*Century 21*].

In what circumstances were contracts deemed unenforceable?

Obscure Terms of Use That Are Hard to Find

- If terms of use are particularly hard to find the agreement may be deemed unenforceable.[64]
- Placing the terms of use on the footer of the website has been found acceptable and enforceable.[65]

Note:

- If an organization has agreed to the PSPFD they have committed to easily accessible policies.

Reserving the Right to Change the Agreement at Any Time

- If a party can unilaterally amend the contract at any time, the courts may find that the agreement does not constitute a contract and would not be legally binding.[66]

Note:

- If an organization has agreed to the PSPFD they will not change a customer's contract without notifying the customer and obtaining their consent.

What does this look like from a farmer's point of view? A John Deere Example

Example

The following information provides a look into how an ATP coveys their data policies to a farmer.

John Deere complies with *PSPFD*.

Accessibility of Policies

John Deere's policies are easily accessible. A link to their privacy and data policies is located on their homepage.

[64] See *In re Zappos.com, Inc., Customer Data Security Breach Litigation* 2012 U.S. Dist. LEXIS 181087 (D. Nev., Dec. 19, 2012) [*re Zappos*].
[65] See *Dell Computer Corp. v. Union des consommateurs*, 2007 SCC 34, para 238.
[66] See *re Zappos*, supra note 5; *Roling v. E*Trade Securities LLC*, 2010 WL 4916401 (N.D. Cal. Nov. 22, 2010); and *Harris v. Blockbuster Inc.,* 2009 WL 1011732 (N.D. Tex. April 15, 2009).

The direct links to their policies are:

http://www.deere.com/privacy_and_data/privacy_and_data_canada_en.page
https://www.deere.com/privacy_and_data/policies_statements/en_CA/data_principles/business_data_commitment.page

Their privacy policy includes:

- Types of Information & Data Collected by John Deere;
- How John Deere Collects Information & Data;
- How John Deere uses Information & Data (the "Purposes");
- Why Information & Data are Disclosed by John Deere;
- The Choices the Farmer has to Limit Information Provided;
- How the Farmer Will be Notified if there are Changes to this Statement; and
- How to Contact John Deere.

Explicit Consent to Collection

There is a "Data Usage Agreement" that is displayed on the "MyJohnDeere" Operations Center when a new user signs in. It must either be accepted or declined.

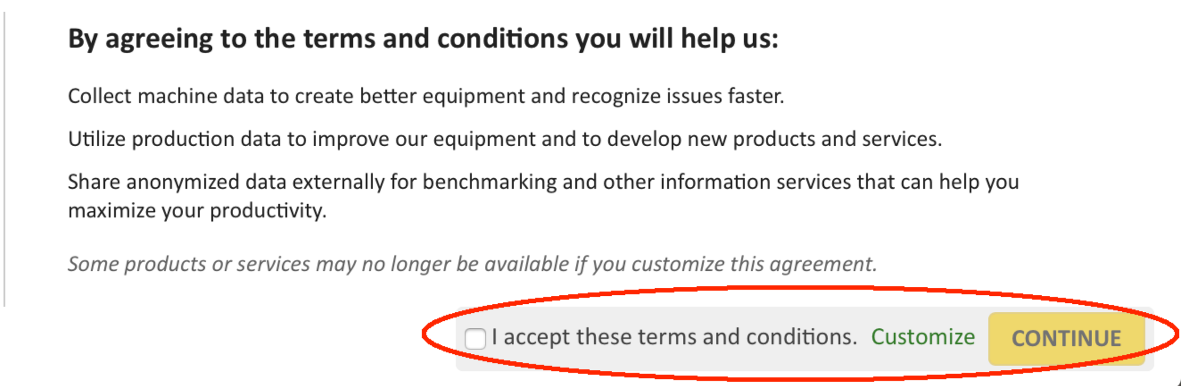
MyJohnDeere is the name of John Deere's application program interface (API). Each agriculture technology provider will have their own API, or will contract out the services to independent companies. For example, Seedmaster uses API provided by Raven Industries.

If a user "accepts" the terms and conditions, they are accepting the policies linked to in the bottom right corner, the same policies available on the homepage. This contract is a click-wrap agreement with link to terms.

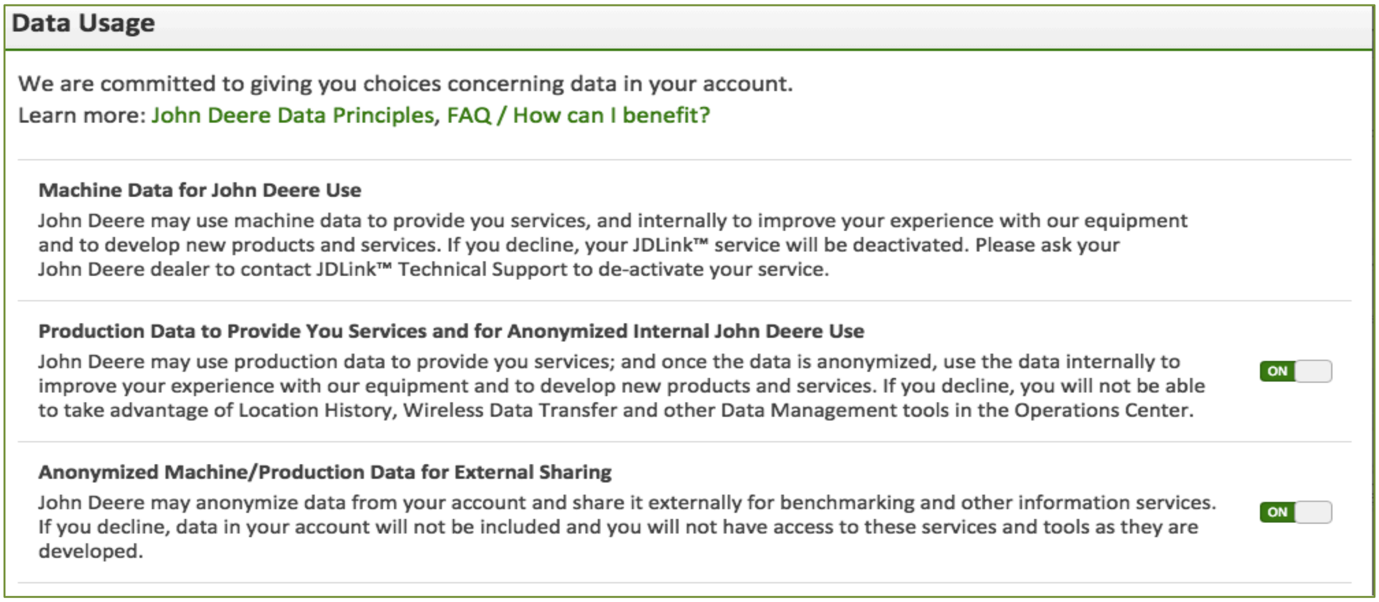
There is also an option to customize the data collection terms, as discussed below.

Customizing Options

If a farmer hits the "Customize" button they will be taken to a page that clearly explains how the data will be used and provides an "on/off" option for whether they consent to their data being used in this way:[67]

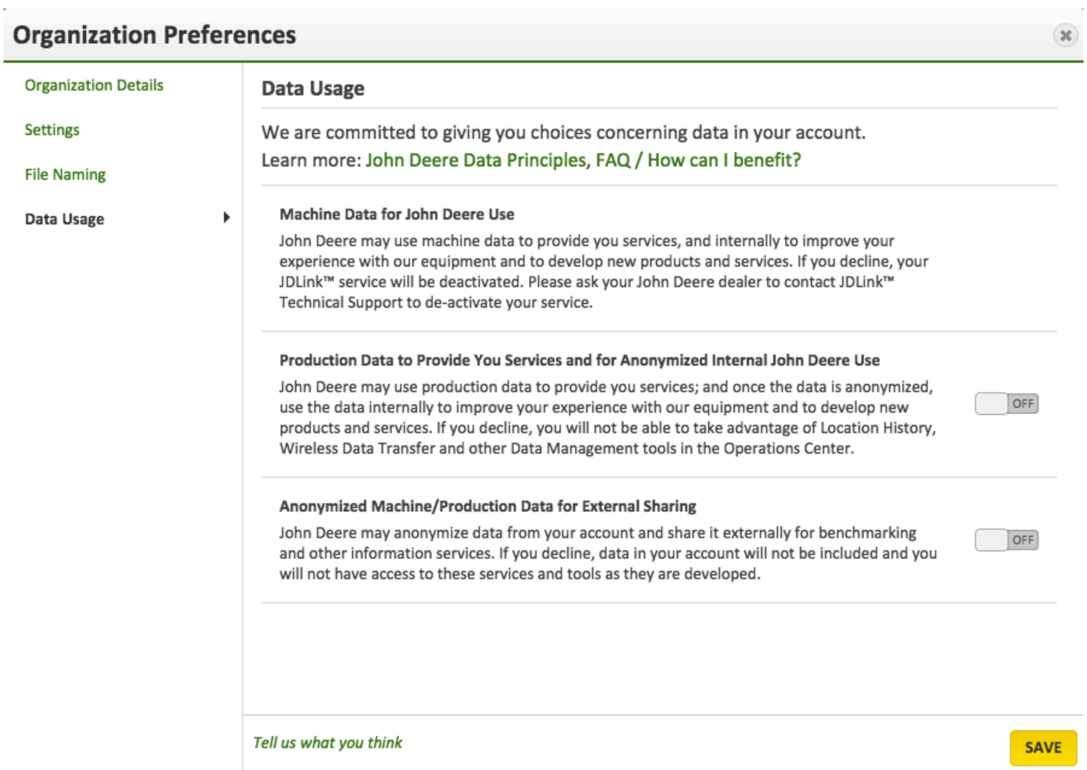


[67] Images from John Deere, "Data Usage" (accessed 21 March 2016), *MyJohnDeere* (website pop-up), online: <https://myjohndeere.deere.com/>



Changing Preferences

A farmer may change their preferences at any time by accessing the "Organization Preferences" tab from their MyJohnDeere Operations Center and clicking "Data Usage."[68]



68 *Ibid.*

Official Contracts

Official contracts can be accessed at:
https://www.deere.com/privacy_and_data/agreements/agreements.page

Section 3.3: Data Collection, states that the policies located on their website www.johndeere.com are synonymous with those in the contract, and restates those policies.

TRADE SECRETS: DO THEY APPLY?

Stacey Dunn

Can trade secrets be used to prevent the equipment companies from selling the data collected off agriculture equipment?

Data collected through GPS, yield monitors and other technical agricultural equipment to US companies can predict crop yields in a certain area. Sale of this data (by the "supplier") can result in the purchaser (the "farmer") to be undercut in the market and adversely affect grain prices in Canada.

Trade secrets are information that is un-disclosed (secret), non-trivial information that is not a part of a skill set. They can be created in 3 ways in order to protect information, (1) through contract, (2) fiduciary relationships and (3) a tort of breach of confidence.

Creating trade secrets through contracts:

Trade secrets created through contract, known as a confidentiality agreement or non-disclosure agreement can create a trade secret. If a party to the contract discloses the information, they would be in breach of contract and could be sued for damages. This requires all aspects of a valid contract including offer, acceptance, consideration and public policy considerations.

Trade secrets created through fiduciary relationships:

There are two situations where a fiduciary relationship arises. The first is automatic where the onus is on an alleged fiduciary to prove why a fiduciary relationship should not be established. This is the case for relationships such as a solicitor/client, doctor/patient or agent/principle. An automatic fiduciary duty does not arise between a supplier and a consumer. The second category is on a case by case basis. The test to determine where a fiduciary duty can arise was set out by ***Frame v Smith***[69] and reiterated by the Supreme Court of Canada (SCC) in ***International Corona Resources Ltd. v LAC Minerals Ltd***:

(i) The fiduciary [i.e. the supplier] has power or discretion
(ii) The [supplier] can exercise that power or discretion unilaterally so as to affect the beneficiary's [the farmer] legal or practical interests, and
(iii) The [farmer] is particularly vulnerable or dependent upon the fiduciary[70]

In this case, a fiduciary relationship does not arise as at least one element of the test is not met. The supplier has power and discretion over the data that it has collected. It may be argued that they are exercising that power unilaterally to affect the farmer's practical interests by affecting the market however the relationship between selling the data and the change in market price is not direct and would be difficult to prove to the court on the balance of probabilities. Where the test really fails is that the farmer is not in a vulnerable or dependent state with

[69] *Frame v Smith*, [1987] 2 SCR 99, 9 RFL (3d) 225.
[70] *International Corona Resources Ltd. v LAC Minerals Ltd.* (1989), [1989] 2 S.C.R. 574 [*LAC Minerals*].

the supplier. The farmer has the choice to purchase equipment from many different companies or to not use the technology that is capable of collecting specific yield data.

In addition, the SCC stated in ***LAC Mineral*** that in a commercial context the parties should protect themselves by contract as opposed to a presumed fiduciary duty.[71] This is because in arm's length commercial transactions, each party has ample opportunities to negotiate their own rights and obligations.[72] In this case, the farmer signs a contract allowing use of the collected data however they are in a position to attempt to negotiate that contract or to buy equipment from suppliers that do not allow the collect or sale of the data collected. Since the right to the data collected is covered by contract, a fiduciary duty will not protect that information.

Trade secrets and breach of confidence:

The tort of breach of confidence can protect trade secrets that protect confidential information when 3 elements are met:

(i) The information must be confidential
(ii) The information must be communicated "in circumstances importing an obligation of confidence"[73]
(iii) The information was used without authorization and to the detriment of the party communicating it[74]

This test was adopted by the SCC in ***LAC Mineral***.[75] In this case, even if you could determine that the data collected by farming equipment is confidential, a tort of breach of confidence still does not apply as the information is not communicated to the supplier (by the farmer) under confidential circumstances. In many cases the farmer may not be aware that the information is being distributed to 3rd parties, but there is no reasonable expectation of privacy with data collected from machinery unless explicitly communicated to the purchaser. In this case, that would not be communicated to the purchaser because the sales contract includes consent to communicate that information. Therefore, the third element required to prove the tort is not met. The information is not communicated without authorization as the sales contracts have agreements that the data could be sold or used by 3rd parties, even though this is to the detriment of the farmer.

The bottom line: can the concept of trade secrets be used to protect information?

The information being communicated or sold to 3rd parties **typically cannot** be protected by trade secrets. A sales contract where the farmer consents to the information being used or sold precludes the protection of the information by trade secrets. In the absence of consent from the farmer in a sales contract, the information could not be protected through a fiduciary relationship or the tort of breach of confidence.

---

[71] *Ibid.*
[72] Kennedy, J., "*Equity in a Commercial Context*", in P.D. Finn, ed., *Equity and Commercial Relationships* (The Law Book Co., 1987); *Weinberger v Kendrick* (1982) 34 Fed Rules Serve (2d) 450.
[73] *Coco v. A.N. Clark (Engineers) Ltd.*, [1969] R.P.C. 41 (Ch.) at p 47.
[74] *Ibid*.
[75] *LAC Minerals supra* note 2 at para 10.

The information could not be protected through a fiduciary relationship as the farmer is not vulnerable to or dependent on the supplier. The data could not be protected through a tort of breach of confidence as the information is not communicated in circumstances that indicate a level of confidentiality. However, in the absence of consent from the farmer, the information could be protected as a trade secret through a non-disclosure contract with the supplier.

CONCLUSION

Overall, the current landscape of agricultural information collection appears to be concentrated on issues of privacy and contract law, rather than copyright law. Because this technology (and the resulting concerns) are relatively new, there is little litigation from which to develop an opinion on what facets of data collection, processing, and possession will be significant in the battle to maintain privacy. The main concern is to ensure that larger companies and third party groups do not take control over data collected by producers and use it against them to the advantage of the large corporations/third parties. Unfortunately, until a case is brought for litigation by the courts, we can only speculate about what potential issues might arise.