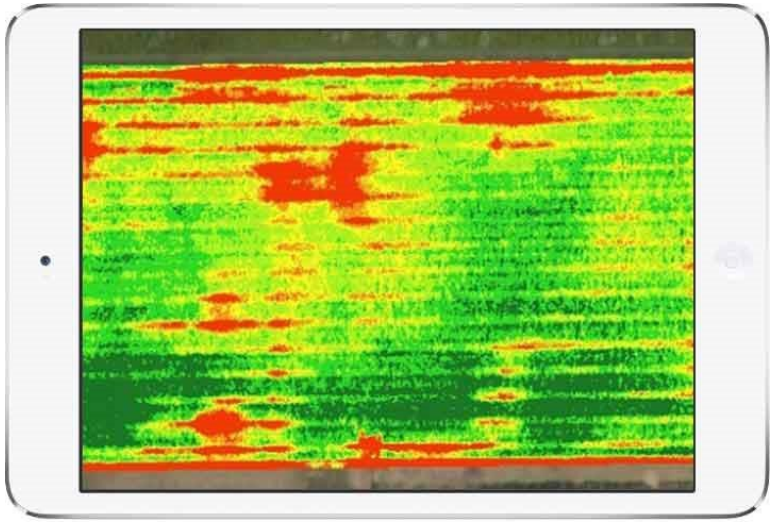
2016 Farmer Cooperatives Conference

Drones Take Flight: Privacy and Intellectual Property Issues

Jamie Nafziger

November 3, 2016

Yellow Striped Armyworm and Nitrogen – Can a Drone Help?



Key Legal Issues

- **Intellectual Property**
- **Privacy**

- **Agreements**
- **Regulations / Best Practices**
- **State and Federal Drone-Specific Laws**

Types of Farm Data

Grower's knowledge of land and conditions

Historical records of field, seed, inputs, etc. and performance

Information from sensors – drones

Grower's/landowner's personal information

- **Different legal protections/issues for each type**

Intellectual Property: Legal Standards

- **Is data collected from farms protectable intellectual property?**
- **Trade secret protection**
- **Uniform Trade Secrets Act (UTSA) defines trade secret as:**
  - **information, including a formula, pattern, compilation, program, device, method, technique, or process;**
  - **that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and**
  - **is the subject of efforts that are reasonable under the circumstances to maintain its secrecy**
- **Some farm data may qualify; info collected by drones may not**

Components of Precision Agriculture Ecosystem

- **Hardware**
  - Drones (UAS)
  - Sensors and cameras
  - Smart farm equipment
  - Communications systems
  - Mobile devices
  - Satellites
- **Software**
  - Apps
  - Cloud-based software
- **Talent**
  - Producers
  - Drone operators
  - Crop specialists
  - Applicators
- **Data**
  - Geolocation
  - Weather
  - Soil condition
  - Historical results
  - Databases of other variables

Intellectual Property: Practical Solutions

- **Agreements**
  - **Address different categories of data**
    - **Agreements between growers, software and hardware vendors, service providers, agronomists**
    - **Agreements between software and hardware providers**
  - **Who can use data?**
  - **What can they do with it?**
- **Ag Data Transparency Evaluator (American Farm Bureau Federation)**
- **Data repositories**

Legal Framework: Privacy

- **No federal comprehensive privacy law (instead specific areas: financial, health, etc.)**
- **State laws**
  - **Violations of reasonable expectation of privacy**
- **Federal Trade Commission**
  - **Deceptive or unfair acts**
  - **Individual person and his or her device**
  - **Collecting, using and sharing of personal information**
  - **Privacy policies – notice & consent**

Drone Privacy Law – Not Passed by House

- **Final bill passed in July 2016 did not contain these provisions**
  - **Commercial drone operators must disclose if collecting personal information about individual, including using facial recognition**
  - **Disclose how using personal information, including use for advertising or marketing**
  - **Disclose when personal information would be destroyed**
- **Final bill did contain**
  - **FAA shall convene industry to develop standards for remotely identifying operators and owners of UAS**

Reasonable Expectation of Privacy: Search & Seizure Analogy

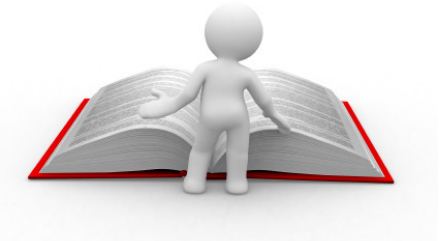
- ***Dow Chemical v. U.S.*** **(1986): aerial photographer hired by EPA photographed facility from 1,200, 3,000 and 12,000 feet – search constitutional – land open to view and observation does not trigger 4th Amendment protection – open area around facility more like an open field than curtilage of home**
- ***California v. Ciraolo*** **(1986): from small plane 1000 feet over fenced-in backyard, police photographed marijuana plants. Supreme Ct. – no reasonable expectation of privacy in things that can be seen from location where public has right to be**

Reasonable Expectation of Privacy: Search & Seizure Analogy

- ***Florida v. Riley*** **(1989): Police observed marijuana plants from helicopter at 400 feet looking through sides & roof of greenhouse left partially open – search constitutional**
- ***Kyllo v. U.S.*** **(2001): thermal imaging from outside home – search unconstitutional – device not in general public use/details of home previously unknowable**

Definitions of "personal information" or "personally identifiable information"

- **information from or about an individual consumer, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; (j) precise geolocation data of an individual or mobile device, including but not limited to GPS-based, WiFi-based, or cell-based location information; (k) an authentication credential, such as a username and password; or (l) any other communications or content stored on a consumer's mobile device.**
- **FTC consent decrees**



Farm Data

- **Elements of farm data that could be considered personal information**
  - **Grower and owner contact information**
  - **Geolocation of person or device**
  - **Image or video of person**
  - **Device identifiers**
  - **Credit card info**
  - **Financial information**

Privacy Challenge: Due Diligence on How Third Parties Use Personal Information

- **Software providers/hardware providers**
- **Database/repository providers**
- **Analytics providers**
- **App platforms**
- **Connections between apps**
- **Cookies and other trackers**
- **Ag service providers**

Privacy Challenge: Seamless Interactions

- **How to deliver privacy policy when drone will fly over or as drone flies over?**
- **Less interaction with screens and text makes delivering legal notices/making agreements with growers or people on land**

Help me Obi Wan Kenobi, you're my only hope; and by the way, if you speak with me, you understand and consent that your personal information, including your photo, name, and exact geolocation may be shared with the Galactic Empire. Nod if you are Obi Wan Kenobi and if you agree.

In the face of uncertainty…

- **Change law / new law**
- **Self-regulation**
- **Agreements**
  - **Who can access and use data?**
  - **What can they do with it?**
- **Disputes**

Change Law / New Law

- **Amend trade secret law to include data collected from farms? Proposed by witness in House Committee on Agriculture hearing October 28, 2015**
  http://agriculture.house.gov/uploadedfiles/10.28.15_ferrell_testimony.pdf
- **Over 45 states have considered or enacted drone legislation**
- **Concepts in Some Proposed/Enacted State Laws**
  - **Identification of drone owner or operator on device**
  - **Registration with state**
  - **Tenants need written permission from landowner to use UAS on property**
  - **Louisiana – farm data collected through UAS belongs to legal owner of property where collected (La. R.S. 3:41-47)**
  - **Texas – misdemeanor to capture, disclose, display, distribute "image" of individual or privately owned real property (narrow exceptions); Ch. 423 of Government Code**

Self-Regulation

- **American Farm Bureau Federation**
  - **Privacy and Security Principles for Farm Data (November 13, 2014; updated May 5, 2015)**
- **Open Ag Data Alliance (OADA)** http://openag.io/about-us/principals-use-cases/
- **AgGateway data privacy and use white paper** http://www.aggateway.org/WorkingGroups/Committees/DataPrivacySecurity.aspx

NTIA Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

- **National Telecommunications and Information Administration**
  - *https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf*
  - Updated in June when new FAA drone regulation released
- **Five voluntary best practices**

NTIA Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

1. **Inform others of your use of UAS**
   - **Reasonable effort to provide prior notice to individuals of general timeframe and area where UAS will be intentionally collecting data.**
   - **If UAS operator anticipates collection of covered data, operator should provide privacy policy for data.**
     - **Covered data: "information collected by a UAS that identifies a particular person. If data collected by UAS likely will not be linked to an individual's name or other personally identifiable information, or if the data is altered so that a specific person is not recognizable, it is not covered data."**
     - **Privacy policy should be in place no later than time of collection and made publicly available.**
       - **Purpose for which UAS will collect covered data**
       - **Kinds of covered data UAS will collect**
       - **Information regarding any data retention/de-identification practices**
       - **Examples of types of entities with whom covered data will be shared**
       - **How to submit privacy and security complaints/concerns**
       - **Information describing practices in responding to law enforcement requests**

NTIA Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

2. Show care when operating UAS or collecting and storing covered data

- **Without compelling need or consent of data subjects, avoid using UAS to intentionally collect covered data where operator knows data subject has reasonable expectation of privacy**
- **Avoid using UAS for purpose of persistent and continuous collection of covered data about individuals**
- **Make reasonable efforts to minimize UAS operations over or within private property without consent of property owner or without appropriate legal authority**
- **Make a reasonable effort to avoid knowingly retaining data longer than reasonably necessary to fulfill specified purposes**
- **Establish a process to receive privacy or security concerns for covered data**

NTIA Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

3. Limit Use and Sharing of Covered Data

- Receive consent if covered data is used for employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility
- Avoid using or sharing covered data for purpose not included in privacy policy covering UAS data
- Regarding publicly disclosed covered data, make reasonable effort to obfuscate or de-identify covered data prior to disclosure
- Make reasonable effort to avoid using or sharing covered data for marketing purposes

NTIA Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

4. **Secure Covered Data**
   - **Provide adequate program with administrative, technical, and physical safeguards appropriate to operator's size and complexity**
   - **Model security programs after NIST Cybersecurity Framework**
5. **Monitor and Comply with Evolving Federal, State, and Local UAS laws**

Conclusions

- **Both intellectual property and privacy issues regarding data collected by drones uncertain**
- **Due diligence required to answer producer questions about their data or required to draft privacy policies challenging in complex technology ecosystem**
- **For tech providers – getting grip on your data flows may become table stakes in precision ag**
- **Participation in standards development and legislative action likely helpful**
- **Focus on user agreements and training people in field to explain them is key**
- **Notice, privacy policies and following best practices reduce risk**

Thank You

Jamie Nafziger
Dorsey & Whitney LLP
Nafziger.jamie@dorsey.com
(612) 343-7922

Twitter: @JamieNafziger

Release the Drones: New Small UAS Regulations Now in Effect in the U.S.
https://www.dorsey.com/newsresources/publications/client-alerts/2016/09/drones-new-small-uas-regulations-in-us

Webinar Playback: An Exploration of the Commercial Use of Drones in Agribusiness and Infrastructure
https://www.dorsey.com/newsresources/events/event/2016/08/webinar-playback-drone-series_083116