All Data, Big and Small:
Agricultural Data and Risk Management on the Farm
Minnesota Crop Insurance Conference
September 12, 2019

Dr. Shannon L. Ferrell
Professor, Agricultural Law
OSU Dept. of Agricultural Economics
@shanferrell

Dr. Terry Griffin
Associate Professor, Cropping Systems Economist
KSU Dept. of Agricultural Economics
@SpacePlowboy

With grateful acknowledgement to:

Dr. Marvin Stone
Professor Emeritus,
Oklahoma State University

Ryan Jenlink, Esq.
Wick Phillips Gould & Martin, LLP

Kevin Thedford
P&K Equipment, Inc.
Enid, Oklahoma

Ryan Johnson
Farmers Grain Company
Pond Creek, Oklahoma

Matthew Steinert
Steinert Farms
Covington, Oklahoma
Definition time:
“Small Data”
Definition time: “Small Data”

Data collected from an individual farming unit
Precision ag tech adoption rates by farm size (2010)

Source: Schimmelpfennig, 2016

Precision ag tech adoption on Kansas Farms (through 2017)

Source: Griffin & Yeager, 2018
Data value is in the eye of the beholder

Source: http://www.extremetech.com/extreme/131810-google-microsoft-team-up-to-bring-super-wi-fi-to-rural-usa
Valuation of precision ag data:
The Ballad of Captain Binary Beard

How much to get yer data back?
How much fer me to not post it?

Valuation of precision ag data

• When the monitor goes down, does harvest stop?
• If the combine’s on fire, do you save the drive?
Data quality

• Data is great, but...
  – Calibration of sensors is crucial
  – So is data cleaning
  – Data ≠ truth

Definition time: “Big Data”
Definition time: “Big Data”

Definition time: “Sharpie Data”
Definition time: "Big Data"

Datasets requiring advanced techniques for collection, management, and analysis due to the data’s

- Volume
- Velocity
- Variety
- Veracity

<table>
<thead>
<tr>
<th>Data</th>
<th>Primary Use</th>
<th>Secondary Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yield monitor data</td>
<td>Documenting yields</td>
<td>GxExM analyses</td>
</tr>
<tr>
<td></td>
<td>On-farm trials</td>
<td></td>
</tr>
<tr>
<td>Soil sample data</td>
<td>Fertilizer decisions</td>
<td>Regional compliance</td>
</tr>
<tr>
<td>Scouting</td>
<td>Spray decisions</td>
<td>Regional analytics</td>
</tr>
<tr>
<td>TMDLs</td>
<td>Erosion control</td>
<td>Environmental stewardship</td>
</tr>
<tr>
<td></td>
<td>Soil health</td>
<td></td>
</tr>
</tbody>
</table>

Need 1 field  Need many fields
How much are you sharing?  
Ohio State Digital Ag Program participants

92% Share data with at least 1 person  66% Share data with at least 2 people  34% Share data with 3+ people

Source: Fulton, 2019

So who’s using agricultural Big Data?

• Everybody*
• Commodities brokers & hedge funds
• Lending institutions
• Input suppliers
• Equipment manufacturers
• *gasp* Insurance companies
What could possibly go wrong?

What could possibly go wrong?
What could possibly go wrong?

Have you ever seen a telemarketer get their lungs ripped out through the phone? Well, you're about to.

What could possibly go wrong?
It’s like déjà vu all over again...

The technology curve

- **Technology Trigger**
  - R&D

- **Peak of Inflated Expectations**
  - Startup companies first round of venture capital funding

- **Trough of Disillusionment**
  - First-generation products, high price, lots of customization needed

- **Slope of Enlightenment**
  - Second/third rounds of venture capital funding

- **Plateau of Productivity**
  - Third-generation products, out of the box, product suites

- **On the Rise**
  - Early adopters investigate

- **At the Peak**
  - Activity beyond early adopters
  - Supplier consolidation and failures
  - Second/third rounds of venture capital funding

- **Sliding Into the Trough**
  - Negative press begins
  - Less than 5 percent of the potential audience has adopted fully

- **Climbing the Slope**
  - Methodologies and best practices developing

- **Entering the Plateau**
  - High-growth adoption phase starts: 20% to 30% of the potential audience has adopted the innovation
The technology curve

Principles of information security: “the CIA”

- Confidentiality
- Integrity
- Availability
Threats to confidentiality

- Intentional theft through apps
- Publishing of confidential information
- Foreign access to remote sensing data

Source: DHS, 2018

FaceApp (coming soon – FarmApp?)

FaceApp: Is The Russian

And where are those servers based? Mostly America, not Russia. Of course, given the developer company is based in St. Petersburg, the faces will be viewed and processed in Russia. The data in those Amazon data centers could be mirrored back to computers in Russia. It’s unclear how much access FaceApp employees have to those images, and Forbes hadn’t received a comment from the company at the time of publication about just what it does with uploaded faces.

So while Russian intelligence or police agencies could demand FaceApp hand over data if they believed it was lawful, they’d have a considerably harder time getting that information from Amazon in the U.S.
Threats to integrity

• Intentional falsification to disrupt or smear an industry

• Introduction of rogue data to cause automated system malfunction or erroneous decisions

• Thwarting machine learning

Source: DHS, 2018
Threats to availability

- Disrupting equipment availability
- Disruption of navigation systems
- Disruption of communications networks

Source: DHS, 2018
Center for Internet Security
Critical Security Controls

• Only allow authorized web browsers and carefully monitor what scripts they authorize.
• Secure network ports and only allow remote desktop access through VPNs or other encrypted pipelines
• Inventory and control hardware assets (especially with a change of personnel)

Source: DHS, 2018

Center for Internet Security
Critical Security Controls

• Inventory and control software assets; delete software that shouldn’t be there
• Establish levels of access for authorized users
• Separate operational technology systems (tractors, implements) from business operations networks

Source: DHS, 2018
• Maintain equipment to minimize opportunity for data loss

• Establish a plan for collecting backup data and for using backup data in the event of a data loss

• Understand who is using your data, what data they get, and how they are using it.

Source: DHS, 2018

Source: https://www.google.com/trends/
Owning information

Data is intangible and irreplaceable:
- “non-rival”
- “Excludable” and/or “non-excludable”

Copies of digital data are identical to the original.
Value lies in its use, not in the possession.

Data tombs are common (and worthless).
Anonymity does not exist with big data.
Ownership framework

• First: what does it mean to “own” something?
  – Right to POSSESS*
  – Right to USE
  – Right to ENJOY
  – Right to EXCLUDE OTHERS FROM*
  – Right to TRANSFER
  – Right to CONSUME or DESTROY*

• Better question: What are the rights and responsibilities of the parties with respect to the data?

Framework for intangible property

• Intellectual property
  — Trademark
  — Patent
  – Copyright
  – Trade secret

• Where does farm data fit, if at all?
Why copyright© doesn’t work for ag data ownership

Simply collecting and transmitting data can have an impact...
Why trade secret MIGHT work for ag data ownership

• Note: Trade secret a function of STATE law

• Uniform Trade Secret Act (UTSA) §1
  – Information that:
    – derives independent economic value, actual or potential, from not being generally known… and
    – is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Efforts to maintain secrecy

“…the owner [must] take[] reasonable steps to ensure that the information does not become generally known.”

Source: Smith, Lars. RFID and Other Embedded Technologies: Who Owns the Data? 22(4) SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL 724 (2006); citing Restatement (Third) of Unfair Competition, §39 cmt. f.
Efforts to Maintain Secrecy
What if my data is constantly uploaded?

• Disclosed information “can retain its status as a trade secret if it remains secret from others to whom it has potential economic value.”

• “The precautions required of the trade secret owner may increase with increasing dissemination.”

Sources:
Restatement (Third) of Unfair Competition, §39 Comment (f),(g).

When it comes to data agreements

READ
Ya got served, dawg!

- FOIA requests
- Legal process
- Official-looking stuff

Disclosure under legal process
“I have this subpoena here...”

- Disclosure prohibited unless subpoenaed or otherwise compelled by legal process
- Give the Disclosing Party as much notice as possible (to contest process)
- Receiving Party must use best efforts to cooperate with the Disclosing Party; and
- Receiving Party may disclose only information which, in the written opinion of its legal counsel, it is **required** to disclose
Privacy and Security Principles for Farm Data
Originally adopted November 13, 2014

AGCO
Ag Connections, Inc.
Agrible, Inc.*
AgSense
AgWorks
Ag Leader Technology
American Farm Bureau Federation
American Soybean Association
Beck’s Hybrids*
CNH Industrial
Conservis*
Crop IMS
CropMetrics
Dow AgroSciences LLC
DuPont Pioneer
Farm Dog
Farmobile LLC*
Granular*
Grower Information Services Cooperative
GROWMARK, Inc.*
Independent Data Management LLC*

John Deere
Mapshots, Inc.
National Association of Wheat Growers
National Barley Growers Association
National Corn Growers Association
National Cotton Council
National Farmers Union
National Potato Council
National Sorghum Producers
North American Equipment Dealers Association
OnFarm
Raven Industries
Reinke Manufacturing Co., INC.
Syngenta
The Climate Corporation – a division of Monsanto
USA Rice Federation
Valley Irrigation
ZedX Inc.

Policies are swell, but...

• (Mostly) unenforceable at law
• Unilateral in nature
• Bilateral agreements would be nice, but
  – Significant disparities in bargaining power
  – Opportunity to assent
  – Adhesion / unconscionability
So who owns what?

• Farmer vs. service provider
• Farmer vs. data host
• Farmer vs. data processor
• Farmer vs. landowner

Landowner / tenant issues

• Review leases for:
  – Definition of farm data
  – Provision establishing who owns farm data
  – Provision defining what happens to farm data at the end of the lease

Source: Todd Janzen
You can’t unring a bell

Future policy directions

- Increased wireless broadband infrastructure
- Statutory rules for data ownership, storage & disclosure? (HIPAA for data?)
- Doctrine for data whose value is in the aggregate vs. standing alone?
Educational opportunities

- Helping producers see value of data / analytics
- Creating data collection & management plans
- Understanding risks & opportunities of sharing
- Creating / evaluating data sharing agreements

Fortune cookie wisdom

- Sharing requires trust
- Trust requires transparency and confidence(iality)
- If you know what you don’t know, you need a consultant
- If you don’t know what you don’t know, you need a counselor
Epilogue: How do we deal with disturbances in the Force?

*Star Wars: The Last Jedi, Russian Trolls, and the Disintegration of Discourse*

A new study finds half of the negative tweets about the film were "likely politically motivated or not even human."

*No, half of The Last Jedi haters were not Russian trolls*

Commentary: Numerous reports say The Last Jedi negativity was influenced by Russian bots and trolls, but the reality is far different.

**Many thanks!**

Shannon L. Ferrell
Oklahoma State University Dept. of Agricultural Economics
532 Agricultural Hall
Stillwater, OK 74078
shannon.l.ferrell@okstate.edu @shanferrell

That's a lower-case “L”