Understanding Data Privacy and How It Impacts Precision Agriculture

Natalia S. Kruse, Attorney
Husch Blackwell
nationwide reach | global capabilities

17 offices
700 attorneys
global experience
result focused
Internet of Things

• One estimate indicates IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025.

• By 2020, it is estimated that there will be 40 billion “Things” and 10 billion traditional devices connected to the internet.
Internet of Things

- *Internet of things (IoT):* infrastructure of interconnected objects, people, systems and information resources, together with intelligent services to allow them to process information of the physical and the virtual world and react.
- *IoT Device:* digital entity which bridges between real-world physical entities and the other digital entities of an IoT system.
Smart Contracts

- A self-executing contract.
- Combination of a rules based software program that is aligned with the IoT System used to carry out the agreed-to services, or an individual or series of transactions.
- Terms and obligations of the transaction are agreed upon and pre-programmed into the smart contract.
- The IoT system monitors the inputs and commercial conditions and the External Utility(s) trigger actions when certain conditions exist.
- Can incorporate “smart” features like price comparisons for automatic price negotiations, and predictive analytics to forecast inventory needs based upon current or historic demand trends.
Artificial Intelligence

• 120 AI Predictions for 2019, *Forbes*: “There is no shortage of angst when it comes to the impact of AI on jobs, especially within the agricultural industry. However, the future of precision agriculture and the key to growing a better crop will rely on AI… *Farms across the world are moving to fill the labor gap—not replace jobs—with AI technology*”

• Machine Learning
  • Automated machine adjustments
  • Disease or pest identification
  • Irrigation and water management
Legal Considerations

- Is product subject to hacking?
- How are you protecting the data?
- Who is responsible in the event of a breach?
- Are you handling sensitive data?
- Who owns the data?
- What are the potential repercussions if there is a breach?

- How to secure the device and data on the network?
- How to protect individual privacy?
- How to preserve the ability to use collected data and potentially generate a valuable asset?
  - Development of end user agreements and privacy policies.
  - IoT Device Manufacturers will now become data merchants.
What Entities are Covered by the CCPA?

For profit legal entity

<table>
<thead>
<tr>
<th>$25,000,000</th>
<th>50,000</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have annual gross revenues in excess of $25,000,000</td>
<td>Alone or in combination, annually buy, receive for the business’s commercial purpose, sell, or share for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices</td>
<td>Derive 50% or more of its annual revenue from selling consumers’ personal information</td>
</tr>
</tbody>
</table>

**Or:** An entity that controls or is controlled by a business and that shares common branding with the business.
Does entity need to have physical presence in California to be subject to CCPA?

No
# Personal Information

Defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

<table>
<thead>
<tr>
<th>Names</th>
<th>Alias</th>
<th>Postal address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique personal identifier</td>
<td>Online identifier</td>
<td>IP address</td>
</tr>
<tr>
<td>Email address</td>
<td>Account name</td>
<td>SSN</td>
</tr>
<tr>
<td>Driver’s license #</td>
<td>Passport #</td>
<td>Education information</td>
</tr>
<tr>
<td>Purchasing/consuming history</td>
<td>Biometric information</td>
<td>Browsing/search history</td>
</tr>
<tr>
<td>Geolocation data</td>
<td>Employment-related information (for now)</td>
<td>Credit card/debit card #</td>
</tr>
<tr>
<td>Information re consumer’s interaction with web site, application, or advertisement</td>
<td>Audio, electronic, visual, thermal, or olfactory information</td>
<td>Records of products or services purchased, obtained or considered</td>
</tr>
<tr>
<td>Financial information</td>
<td>Medical information</td>
<td>Telephone #</td>
</tr>
</tbody>
</table>
Basic Rights Provided by CCPA

✓ **Disclosures** - Businesses must disclose what PI they collect and how that information is shared with third parties.

✓ **Right to Access** - Businesses must provide the specific pieces of PI the business has collected on the consumer for the 12-month period prior to the request.

✓ **Right to be Forgotten** - Businesses must respond to requests to delete PI.

✓ **Opt-out of Sales** - Businesses must provide an online mechanism to opt-out of PI being sold to third parties.
Enforcement

✓ **Private Right of Action**
  - Effective January 1, 2020
  - Limited to data breaches due to a failure to implement and maintain reasonable security procedures and practices
  - Statutory damages of between $100 and $750 “per consumer per incident”
  - Class actions

✓ **Attorney General’s Office**
  - Enforces privacy rights
  - Cannot enforce until publishes interpretive regulations (no later than July 1, 2020)
  - Can seek damages of $2,500 “per violation” or $7,500 for intentional violations
Where is the CCPA Headed?

- Goes into effect on January 1, 2020
- Amendments continue
- Other state legislation
## States that Considered Similar Legislation in 2019

<table>
<thead>
<tr>
<th>Hawaii</th>
<th>Illinois</th>
<th>Maryland</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Massachusetts</td>
<td>Mississippi</td>
</tr>
<tr>
<td></td>
<td>New Jersey</td>
<td>New Mexico</td>
</tr>
<tr>
<td></td>
<td>New Jersey</td>
<td>New York</td>
</tr>
<tr>
<td>Texas</td>
<td>Washington</td>
<td>Nevada</td>
</tr>
<tr>
<td></td>
<td>Pennsylvania</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rhode Island</td>
<td></td>
</tr>
</tbody>
</table>
Potential Federal Action

✓ Committee hearings
✓ Multiple draft bills floating around
✓ Fundamental issue is whether law would set floor or ceiling
Takeaways—Why Should We be Concerned?

• CCPARequirements are complex and still in flux
• Entities have to respond to consumer’s requests at their own expense
• Significant penalties for failing to comply with the requirements of the CCPA
Data Security Concerns

• Any device with connectivity can be hacked.
• IoT presents unique challenges as there are many points of access.
• Few IoT devices encrypt information prior to sending. Many allow for simple passwords.
• Lack of standards and protocols and maze of applicable state laws are problematic.
• Security should be top priority in development and contracting.
Compliance Tips

• Determine whether you have to comply
• Understand what kind of data you have and why
• Update data management processes
• Prepare for data access requests
• Update technology and invest in security from threats
• Establish a data breach notification policy
• Pay attention to developments in the law and industry
THANK YOU!

For More Information Contact:

Natalia Kruse

- Direct: 608-258-7126
- natalia.kruse@huschblackwell.com