BRAD LIPIC
JORDAN DURLESTER

Session Number 10, The Enterprise Data Marketplace: How to Successfully Play Both Offense & Defense

25 September 2020
The Enterprise Data Marketplace: How to Successfully Play Both Offense & Defense

SOA Predictive Analytics 4.0: Session 10

Brad Lipic, VP Global Data Strategy
Jordan Durlester, Executive Director Global Data Strategy

09.25.2020
Active participation in the Society of Actuaries is an important aspect of membership. While the positive contributions of professional societies and associations are well-recognized and encouraged, association activities are vulnerable to close antitrust scrutiny. By their very nature, associations bring together industry competitors and other market participants.

The United States antitrust laws aim to protect consumers by preserving the free economy and prohibiting anti-competitive business practices; they promote competition. There are both state and federal antitrust laws, although state antitrust laws closely follow federal law. The Sherman Act, is the primary U.S. antitrust law pertaining to association activities. The Sherman Act prohibits every contract, combination or conspiracy that places an unreasonable restraint on trade. There are, however, some activities that are illegal under all circumstances, such as price fixing, market allocation and collusive bidding.

There is no safe harbor under the antitrust law for professional association activities. Therefore, association meeting participants should refrain from discussing any activity that could potentially be construed as having an anti-competitive effect. Discussions relating to product or service pricing, market allocations, membership restrictions, product standardization or other conditions on trade could arguably be perceived as a restraint on trade and may expose the SOA and its members to antitrust enforcement procedures.

While participating in all SOA in person meetings, webinars, teleconferences or side discussions, you should avoid discussing competitively sensitive information with competitors and follow these guidelines:

- Do not discuss prices for services or products or anything else that might affect prices
- Do not discuss what you or other entities plan to do in a particular geographic or product markets or with particular customers.
- Do not speak on behalf of the SOA or any of its committees unless specifically authorized to do so.
- Do leave a meeting where any anticompetitive pricing or market allocation discussion occurs.
- Do alert SOA staff and/or legal counsel to any concerning discussions
- Do consult with legal counsel before raising any matter or making a statement that may involve competitively sensitive information.

Adherence to these guidelines involves not only avoidance of antitrust violations, but avoidance of behavior which might be so construed. These guidelines only provide an overview of prohibited activities. SOA legal counsel reviews meeting agenda and materials as deemed appropriate and any discussion that departs from the formal agenda should be scrutinized carefully. Antitrust compliance is everyone’s responsibility; however, please seek legal counsel if you have any questions or concerns.
Presentation Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of the Society of Actuaries, its cosponsors or its committees. The Society of Actuaries does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented. Attendees should note that the sessions are audio-recorded and may be published in various media, including print, audio and video formats without further notice.
Agenda

01 Definition and Importance of an Enterprise Data Marketplace

02 Key Defensive Tactics

03 Key Offensive Tactics

04 Balance of Defensive and Offensive
What is an Enterprise Data Marketplace?

“Our company mission is to organize the world's information and make it universally accessible and useful” – Google

“Our organization’s data marketplace organizes our enterprise’s information and makes it universally accessible and useful” – Your Organization?

What Do We Have? What’s It All About? Can I Check It Out?
A Presentation of Two Halves

Establish a Defense

Enable an Offense
Establishing a Defense

What is a Defensive Tactic?

- Saving your colleagues from themselves
- T’s Crossed and I’s dotted
- Checking all the doors to make sure they’re locked
Enabling an Offense

What is an Offensive Tactic?

✓ Push not Pull
✓ Progressive, Forward-Thinking
✓ Creation of New Value
Key Defensive Tactics
Key Defensive Tactics

Audit Controls

Data Privacy By Design

Compliance Controls in a Changing Legislative Atmosphere
In the News: Data Breaches

According to Forbes, in 2019, the average total cost of a data breach in the U.S. is $8.19 million.

Google received the biggest fine so far in 2020 under GDPR – €50 million ($56.6 million)

British Airways faces record £183m fine for data breach

Marriott Faces $123 Million Fine For 2018 Mega-Breach
Privacy by Design:
A Framework Developed by Ann Cavoukian

Privacy is to be taken into account as it relates to design and operation throughout the whole of IT systems, networked infrastructure, and business practices

1. Proactive not reactive; preventative not remedial
   Take action in advance of the event, not after-the-fact

2. Privacy as the default setting
   Responsibility is on IT system design; not the individual

3. Privacy embedded into design
   Core and integral; not an add-on with potential diminished utility

4. Full functionality – positive-sum, not zero-sum
   Win-win in for all legitimate business purposes; not a trade-off between privacy and security

5. End-to-end security – full lifecycle protection
   Data onboarding through destruction and all steps in-between are to be included

6. Visibility and transparency – keep it open
   Ensure the system is subject to ongoing compliance and validation to stakeholders

7. Respect for user privacy – keep it user-centric
   Empower the user with strong privacy defaults and end-user options
Two key components to ensure data (i) governance/control and (ii) value maximization

<table>
<thead>
<tr>
<th>Data Organization:</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Data-Driven Initiatives Identified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy Impact &amp; Data Plan:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value Maximization:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explore new data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Isolated Virtual Server:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analytics Sandbox:</th>
</tr>
</thead>
<tbody>
<tr>
<td>De-Identified Data</td>
</tr>
</tbody>
</table>
Regulations Driving Change Around the Globe

- **GDPR**
  - General Data Protection Regulation
  - European Union

- **Cyber Security Law**
  - China

- **Cross-Border Privacy Rules (CBPR)**

- **APPI**
  - Act on the Protection of Personal Information
  - Japan

- **POPI**
  - Protection of Personal Information Act
  - South Africa

- **Shine the Light**
  - California’s Consumer Privacy Act

- **Asia-Pacific Economic Cooperation’s (APEC)**
# A Few Protection Methods

<table>
<thead>
<tr>
<th>Data Protection</th>
<th>Anonymization</th>
<th>Differential Privacy</th>
<th>Tokenization</th>
<th>Psuedonymization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Webster</strong></td>
<td>Remove identifying information from something so that the original cannot be known</td>
<td>(None) Method that seeks to maximize accuracy while minimizing the ability to identify the identity of data subjects</td>
<td>Symbol representation, or distinguishing feature</td>
<td>Use of a fictitious name</td>
</tr>
<tr>
<td><strong>In-Data Practice</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Distinguishing Features</strong></td>
<td>One-way; permanently removes the personally identifiable information with no way of getting back to it</td>
<td>Adds random noise to the data while retaining meaningful aggregate statistics; can be applied to the “ride-along” data attributes</td>
<td>Can switch the data between the “masked token” and “in the clear” as it moves through workflows</td>
<td>Adds a field with a pseudonym associated with the identity; preferred method when needing to link data sources on the same individual identity</td>
</tr>
</tbody>
</table>
Key Offensive Tactics
Key Offensive Tactics

Catalog + Request Module

Use-Case Hunting (Top Down)

Prospective Data Scan (Bottom-up)
A Wide Variety of Information Is Being Accumulated and Used

**Basic Demographics**
- Age
- Gender
- Education
- Occupation
- Assets
- Salary
- House price
- Marital status
- Number of Children
- Benefit amount
- Where you live
- Car ownership
- Benefit amount
- Where you live
- Car ownership

**Socio-Economic**
- Social Media Usage
- Avocations
- Insurance purchasing
- Driving Behaviour
- Credit Behaviour
- Well-being
- Stress
- Depression
- Activity
- Diet
- Smoker Status
- Care provider
- Alcohol consumption
- Sleep
- Previous claims history

**Health and Biometrics**
- Investment choices
- BMI
- Blood pressure etc
- Disease history
- Family History
- Prescription History
- Heart Rate / HRV / etc
- Genetic Data
- ‘Omic Data

---

Industry Best Practices for Data Protection
Catalog

Ability to register and track data sources

Benefits
- Enhances the data onboarding process
- Provides visibility and single source of truth for data, sources and projects using them
- Opportunity to cross-leverage sources
- Identifies gaps for future data acquisitions
- Enables regulatory compliance efforts

Risks
- Potential security concern given catalog could be exposed
- Potential financial impact at different capability levels

Measures of Success
- # of sources
- % of sources in catalog
- Date range of data available
- Geographies available
- Attributes available by geo or demographic
- Where PII is located
- Time spent cataloging
Insurance Value Chain and Applications

- New rating factors
- Underwriting risk segmentation
- Propensity to buy
- Distributor quality management
- Competitive pricing strategy
- Agent assessment
- Underwriting triage
- Fraud / Non-disclosure protection
- Propensity to complete purchase
- Determine underwriting ratings
- Structured/Unstructured Data
- Multivariate experience analysis
- Cross-sell and up-sell
- Proactive lapse management
- Customer lifetime value
- Fraud / Non-disclosure protection
- Claim management
- Claim validation
- Claims triage

Level of Demand

- High
- Medium
- Low

Industry Best Practices for Data Protection
Top Down vs. Bottom Up
Use-Case Hunting vs Prospective Data Scan

Illustrative Business Questions

- Leads Generation Needs?
- Better In-Force Mgmt.?
- UW focus?
- Customer Engagement?
- Claims Mgmt?

Intermediary Enablers

Technology, Application Development, Process, Change Management

Data Sources

- Traditional U/W
- Traditional Policy
- Traditional Distribution
- Rx
- Financial
- Lifestyle
- Health and Disease States
- Wellness Data
- Social & IoT Data
- ...

Top Down: Business problems or process inefficiencies create the demand for specific data-driven projects and data acquisition.

Bottom Up: Brainstorm business problems that can be solved as new and interesting data sources emerge.
Balance
Balance: Defensive and Offensive

**Defensive**
- Audit Controls
- Data Privacy By Design
- Compliance Controls in a Changing Legislative Atmosphere

**Offensive**
- Catalog + Request Module
- Use Case Hunting
- Prospective Data Scan

What Do We Have?  What's It All About?  Can I Check It Out?