Maaz Saad

Dr. Theresa Miedema

MBAI 5200G

14 December 2022

Contracts as risk management tools

The use of data analytics in the insurance industry has gained momentum in recent years, as it allows insurance providers to better understand and predict customer behavior. Using the results of the prediction models, insurance companies can determine insurance premiums with improved accuracy. However, these insurance companies are not yet equipped to perform data analytics on their own and therefore need to hire the services of data analytics firms. To do so, it is necessary for insurance companies to enter into contracts with these service providers to manage risk and ensure smooth operations and collaboration between the two parties.

In Canada, an individual's personal information is protected by federal and provincial privacy laws (BLG). The Personal Information Protection and Electronic Documents Act (PIPEDA) lays out the rules and regulations for how organizations in the private sector may collect, use, and disclose personal information during the course of their business endeavors (BLG). The insurance providers must ensure that the data analytics companies are compliant with PIPEDA while utilizing personal information under the ownership of the insurance company.

In our case, Hogtown Automobile Insurance would like to learn about their customers' driving patterns in the hopes of streamlining their models that determine insurance premiums,

and therefore, will be entering into an agreement with YYZ Analytics. Our research team at Hogtown has been asked to draw up a memorandum that focuses on two key issues that can serve as a guide for the contract negotiations between Hogtown and YYZ Analytics. Additionally, our memo will provide valuable recommendations to the Hogtown team to better mitigate the risks involved in such a project.

To: Executive at Hogtown Automobile Insurance

From: Maaz Saad, Research Analyst

Date: December 14, 2022

Subject: Considerations for Contract Negotiations with YYZ Analytics

Part A: Identification of Two Risks

1. Risk of data breach or unauthorized access to customer data due to inadequate security measures in place at YYZ Analytics.
2. Risk of unauthorized or improper use of customer data, including derivative data, for purposes other than getting insights about customers' driving patterns.

Part B: An overview of the nature of the risks

1. Risk of data breach or unauthorized access to customer data due to inadequate security measures in place at YYZ Analytics.

Problem: As a provider of insurance, Hogtown collects sensitive personal information from its customers, including but not limited to age, income, driving durations, driving speeds, and other related data. When this data is outsourced to a third party, such as YYZ Analytics, there is a risk that it may be mishandled, accessed by unauthorized parties, or otherwise compromised. While

the data is safe on Hogtown's servers, but when it is transferred from Hogtown's servers to YYZ's servers, hackers might try to get access to it through YYZ's servers. This could result in a breach of the customers' personal information, which could damage Hogtown's reputation and potentially expose the company to legal liability.

Law: Under the Personal Information Protection and Electronic Documents Act (PIPEDA), the Accountability Principles state that an organization is responsible for the protection and security of personal information in its possession (BLG). To clarify, this means that it is Hogtown's responsibility to come to a contractual agreement with YYZ wherein personal information will be safe from malicious attacks. It is important to note that Canadian privacy commissioners have only provided a set of guidelines that companies should follow to comply with privacy laws while sharing data (BLG). There are no laws under PIPEDA that offer Hogtown legal protection in the case of data breaches at YYZ. Therefore, the burden falls on Hogtown to protect itself from potential lawsuits by signing an airtight contract with YYZ.

2. Risk of unauthorized or improper use of customer data, including derivative data, for purposes other than getting insights about customers' driving patterns.

Problem: The reason Hogtown is leveraging the services of YYZ Analytics is to learn the driving patterns of its customers, and this type of complex analysis is bound to generate derivative data. Derivative data is the term that is used to broadly define the pieces of documentation that will be generated from this analysis, such as cleaned-up data sets, visualizations, testing and training subsets, discarded data, and most importantly, the driving patterns and behaviors (Law). It is imperative that the data is only used for the purposes specified by Hogtown in their contract with YYZ. Lastly, Hogtown needs to ensure that YYZ Analytics

has the necessary expertise and skill set to perform the analysis to a certain standard and level of accuracy (BPISA).

Law: Under PIPEDA, organizations are required to obtain consent from individuals before collecting, using, or disclosing their personal information (BLG). This means that Hogtown needs to officially reach out to its customers to let them know that their data will be shared with a data analytics service provider and get their consent if they concur. According to the Safeguards Principles, Hogtown is responsible for safeguarding the data from loss, theft, unauthorized access, and modification, whether it occurs at Hogtown or at YYZ (BLG). Therefore, Hogtown must frame their contract with YYZ Analytics in a way that it does not breach these laws under PIPEDA. Lastly, it is crucial that Hogtown include clear and enforceable terms in the contract that outline the consequences for failing to deliver the analysis at the agreed-upon standard (BPISA).

Part C: Recommendations

- Hogtown must include a clause in their contract with YYZ that requires them to implement appropriate safety and security measures to prevent unauthorized disclosure of customer data, such as anonymization of personal customer data before it is sent over to YYZ Analytics (IAPP). As an example, the contract could include a confidentiality clause that states that only authorized personnel can gain access to Hogtown's customer data (IAPP). Additionally, staff can be trained in matters of data privacy or security before they start working on the data. By requiring YYZ Analytics to implement these measures, Hogtown can ensure that their customers' data is secure from cyber attacks and reduce the risk of reputational harm.
- Another way to reduce the risk of data breaches due to inadequate security protocols is to ensure that YYZ introduces safety measures such as encryption, secure storage, and regular

security audits (BLG). Similarly, Hogtown should also make it crystal clear in the contract that YYZ Analytics is obligated to inform them of any incidents involving unauthorized access to or disclosure of customer data within a certain time period (BPISA). And failure to do so could result in potential financial penalties. This way, Hogtown can get ahead of the story and look for ways to remedy the situation. Also, it would give Hogtown the chance to take control of the narrative, including breaking the news to their customers in a sensible manner.

- Hogtown should require YYZ Analytics to warrant that the derivate data produced from the analysis will be accurate, reliable, and based on recognizable statistical methods (BPISA). To achieve this, Hogtown should include a provision in the contract stating that they are allowed to get the derivate data reviewed by a third-party data analytics vendor. This is perhaps the most important part of the contract, as the analysis is the reason this conversation was started. By getting a guarantee that Hogtown will receive trustworthy analysis, they can remain rest assured that their financial commitments to this project will not be in vain.
- Hogtown should also consider adding an indemnification provision that would require YYZ Analytics to take the blame in the event of legal claims arising from the inappropriate or misuse of the derivate data (BPISA). Hogtown can preemptively lower the chances of this issue arising by building a compliance monitoring section into the contract that allows Hogtown to follow up with the YYZ's progress through weekly or biweekly meetings (BPISA). This way, Hogtown can save on legal fees and save face with their customers, which is of paramount importance to the company. And more importantly, they can claim to their customers and in a court of law that YYZ had agreed to only utilize the data for the

purpose of discerning driving behaviors, and that any other offshoots are a result of mismanagement and carelessness on YYZ's end.

I hope this gives you a sense of the direction that your preliminary conversation with YYZ Analytics should take. It is reasonable to assume that YYZ Analytics already has some of these measures and protocols in place. Anyhow, you now have a clear understanding of the risks that Hogtown faces and the types of contractual clauses that can be employed to mitigate these risks.

Please let us know if you would like any further information or clarification.

After careful consideration, we boiled down the risks that Hogtown faces to two simple statements and provided ample explanations of the problem and how it ties in with the greater legal landscape. Once the potential risks were properly explained, we provided recommendations that can be followed as the executives start to discuss and review drafts of the service contract with YYZ Analytics.

Works Cited

Making the Most of Your Data: Getting Data Analytics Contracts Right. https://iapp.org/news/a/making-the-most-of-your-data-getting-data-analytics-contracts-right/. Accessed 14 Dec. 2022.

"Privacy Commissioner Reports Provide Guidance for Outsourcing Agreements." BLG, https://www.blg.com/en/insights/2021/02/privacy-commissioner-reports-provide-guidance-for-outsourcing-agreements. Accessed 14 Dec. 2022.

"BEST PRACTICES FOR INFORMATION SHARING AGREEMENTS." Office of the Saskatchewan Information and Privacy Commissioner, SaskIPC, https://oipc.sk.ca/resources/resource-directory/best-practices-for-information-sharing-agreements/.

"Derivative Data Definition." Law Insider, https://www.lawinsider.com/dictionary/derivative-data. Accessed 14 Dec. 2022.

Sample Memo - Purdue OWL® - Purdue University. https://owl.purdue.edu/owl/subject_specific_writing/professional_technical_writing/memos/sample_memo.html. Accessed 14 Dec. 2022.