Big Data Privacy Management Strategy:
A Tim Hortons Case Study

Maaz Saad
Faculty of Business & IT, Ontario Tech University
MBAI 5110G – Big Data Systems Design
Professor Carolyn McGregor
March 13, 2023

Table of Contents

1.1 Summary of Tim Hortons

Tim Hortons is a Canadian restaurant chain specializing in coffee, doughnuts, and other baked and fried goods (Canadian Encyclopedia). Tim Hortons is strongly associated with Canada's national identity and was founded in April 1964 in Hamilton, Ontario, by a former Toronto Maple Leaf's defenseman and a businessman from Montreal (Canadian Encyclopedia). Tim Hortons has grown to become the largest restaurant chain in Canada, operating 3,500+ stores as of February 2023, with a staggering 1,800 locations in Ontario, of which 163 are in Toronto (ScrapeHero). Over the decades, the company has had a few owners. In 1995, Wendy's bought Tim Hortons in a partnership that lasted until 2006 and is currently owned by a Brazilian firm, 3G Capital, as of 2014, that also happens to own Burger King (Canadian Encyclopedia).

Despite its incredible popularity and having established itself as an ethos among the Canadian population, Tim Hortons has had its fair share of controversies over the years (Canadian Encyclopedia). Some of these controversies have included their coffee cups not being recyclable, the company sourcing its pork products from pigs that were raised in confined gestation crates, hiring foreign workers when the unemployment rate in Canada was skyrocketing, cutting employee benefits after the minimum wage was increased, and being regularly criticized by health care professionals for the number of calories and sugar content in their products (Canadian Encyclopedia).

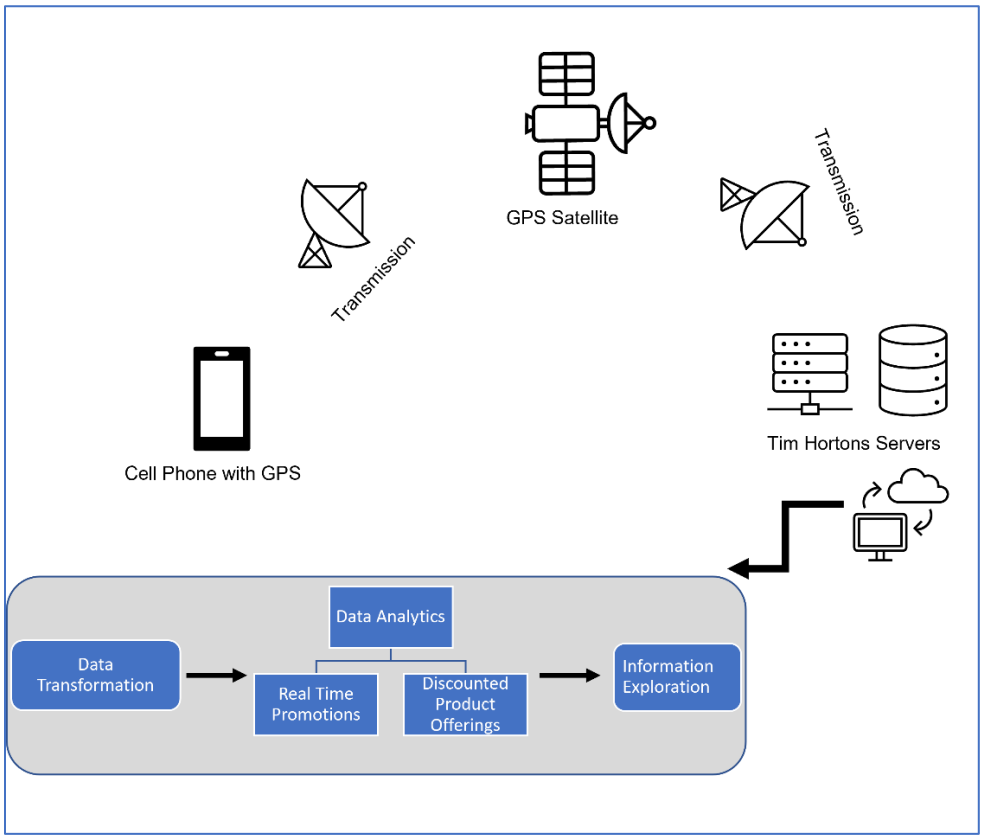
All these controversies seem minor compared to the one that is the basis of this report. Tim Hortons has violated the law by collecting vast amounts of location data from its customers without their explicit approval through the Tim Hortons mobile app (BNN Bloomberg). In this report, we will review Tim Hortons' breach of privacy laws, how and why it happened, and what we can learn from it to better structure our own privacy management strategy.

1.2 Tim Hortons Initial Business Objective

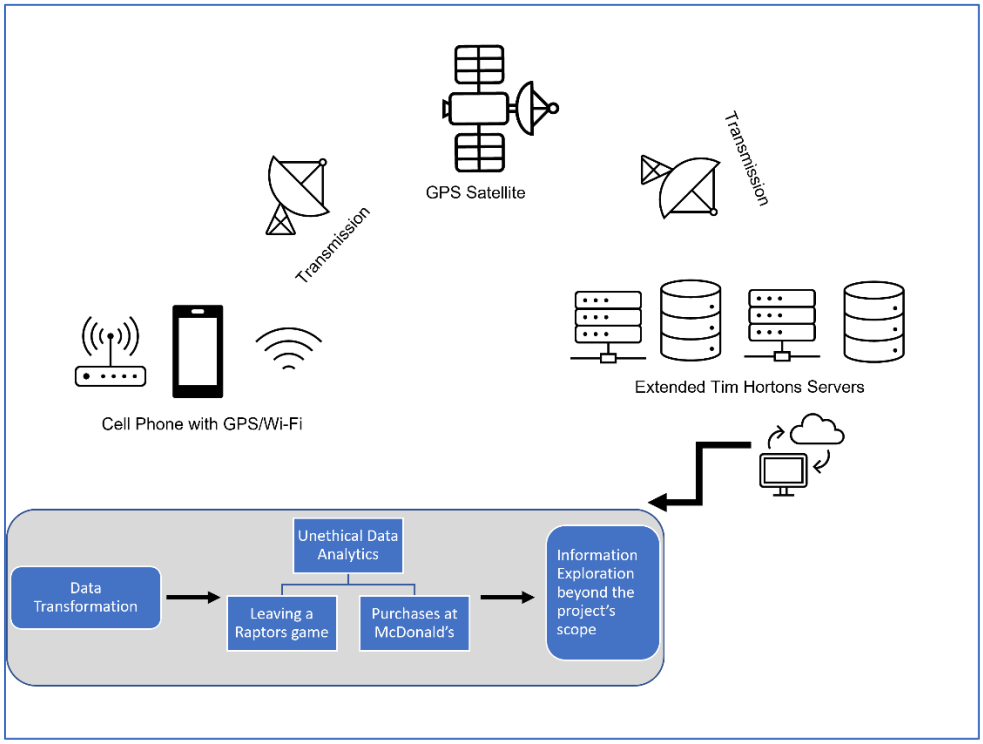
Tim Hortons updated its mobile app in May 2019 to collect location data from its users' phones (The Verge). According to Tim Hortons, the purpose of this data collection was to optimize their advertising strategy by tailoring ads to a person's specific interests and targeting promotions and offers depending on their location (The Verge). The goal of the organization was to show users' offers and discounted products when they were in the vicinity of a franchise, which the management hoped would lead to a potential increase in sales and an overall enhanced customer experience (The Verge).

Tim Hortons originally claimed that the mobile app could only record location history when the app was physically open on the user's phone, or so it led its customers to believe (The Verge). Tim Hortons planned to use the location data in an aggregated capacity to analyze user movement trends, such as when users switched to other coffee chains such as McDonald's or Starbucks, especially during the pandemic (BNN Bloomberg). Furthermore, Tim Hortons hired the services of an American geofencing firm, Radar, for the pattern analysis (The Verge). However, it seems as if none of these original objectives were met, and the analysis went in a completely illegal and immoral direction, which we will explore further in the next few sections.

2.1 Tim Hortons Initial Scope Architecture



2.2 Tim Hortons Extended Scope Architecture



3. Evidence of a Clear and Purposeful Plan

Tim Hortons had a simple and achievable goal when they started off with this project, which was to collect data from its customers and provide them with targeted ads. However, it seems as if the project went off the rails due to poor project management or weak decision-making. As mentioned, Tim Hortons' original plan was to conduct simple data analytics of a descriptive nature. Descriptive data analytics is the science of analyzing historical data to decipher patterns and get an understanding of what happened (MBAI 5110G - Week 8). Diagnostic data analytics is the second layer of analytics, where analysts dig deeper into the data to understand why patterns exist and try to reverse engineer the conditions under which a specific event took place (MBAI 5110G - Week 8). There is another layer of analytics that is applied to make predictions about the future, but in our opinion, Tim Hortons did not want to make actual predictions about the future, consumer trends, or buying patterns; they were more interested in the past events that had transpired to provide real-time offers to its customers. Therefore, we will only focus on the descriptive data analytics and take a gander at the sort of data that needs to be collected for such an analysis and what Tim Hortons ended up acquiring.

According to the Wired article that summarizes the findings of the Privacy Commissioner of Canada, the Tim Hortons app tracked the physical movements of its customers every few minutes. The app informed the customers that it would only track the location when the application was opened on the customer's phone (Wired). And in terms of descriptive analytics, this is the correct approach, as the system in the back-end only needs to know the real-time location to determine the person's current location and show them tailored ads.

However, the app went above and beyond and tracked the location of the customers even when it was not opened and ended up tracking data such as the location of a customer's workplace and home, their travel routes, if they entered or left a sports venue, among other events (Wired). Recording this type of data at a few-minute interval is definitely not needed for the type of analysis that Tim Horton set out to do (Wired). Worst of all, Tim Hortons scrapped this targeted advertising project but continued to collect the location data for another calendar year (Wired).

Unfortunately, the issue only got worse from here. The Office of the Privacy Commissioner reported that Tim Hortons partnership with the American geofencing firm, Radar, for the pattern analysis was extremely problematic (Wired). The contract between the two sides had such vague and ambiguous language that it could potentially allow Radar to sell 'de-identified' location data to whomever wishes to purchase a vast amount of data for their own intents and purposes (Wired). This issue at stake is that de-identified data can be re-identified, which poses a serious security risk and is a breach of a person's privacy beyond a reasonable doubt (Wired).

Considering this information, our team can say with certainty that Tim Hortons plan of data acquisition through data analytics was not well established, which evidently made the execution go in a completely obtuse direction. We believe that the management team at Tim Hortons responsible for this project was probably not skilled enough to develop a proper business plan and follow it while staying faithful to the privacy laws that they had definitely agreed to uphold as a business entity in Canada.

4. Ethical and Privacy Risks

In this section, we will present key points that clearly explain the ethical and privacy risks of collecting personal data without having a proper plan detailing how the data shall be used and the drawbacks of not having a data governance plan in place. Some of these risks are listed here:

- **Data Ownership**: It is an established fact that an individual has ownership of their personal data, and any data related to them is, by default, confidential (HBS). Collecting someone's personal information without their consent is simply illegal and a punishable offense in the eyes of the law. Therefore, it is imperative that our organization only collects personal information from our customers after receiving meaningful consent (HBS). Some ways of receiving this explicit consent are through the use of a written contract, asking a customer to agree to our company's terms and conditions in an online setting, and making it clear to the user through the use of pop-ups that their online activity will be recorded (HBS).
- **Transparency**: To take it one step further, if our organization can inform the customers what their information will be used for, it can help develop a sense of trust between the two parties. So, giving the users a sense of how their personal information will be collected, stored, and eventually analyzed is a step in the right direction (HBS). Most importantly, it is the customer's right to not have their online footprint recorded and therefore needs to be given the option to opt out (HBS).
- **Privacy**: After receiving the customer's consent to have their personal activity recorded, it is still necessary to remember that the information needs to be kept private and secure (HBS). In other words, our organization is responsible for ensuring the security of the data and implementing a plan to ensure that it does not fall into the wrong hands. One way to keep data secure is by using dual-authentication passwords and file encryption (HBS). Another way is by stripping all personal details about an individual, such as their name, phone number, and social insurance number, from the variables of interest (HBS). This is known as de-identification of data, and Tim Hortons tried to utilize this mechanism but was unable to do a decent job.
- **Intention & Discrimination**: Before collecting data, our organization should internally review its project plan to determine what it hopes to achieve from this project in the long run (HBS). They should have a sense of the project's goals and milestones and what type of data will help them achieve them (HBS). The reason this analysis is crucial is because it will help us only collect data that is bound to be useful, and this way we will not end up with a multitude of unnecessary data points (HBS). The point we would like to make is that our organization should strive to achieve our targets with the minimum viable amount of data as opposed to the maximum (HBS). On the other hand, our analysts need to pay special attention to biases in machine learning models (Sibenco). For example, if our organization collects data on religion, gender, or sexual orientation, it could be used to discriminate against certain groups of people. Therefore, our analysts need to be aware of these preconceived notions that analytics models might have and put in an effort to exclude these biased values from the final results, which might have an actual effect on a person's daily life.
- **Security and Accountability**: At the end of the day, our organization needs to hold itself accountable for the safety of the data that we collect and any security breaches that might happen on our watch. In the case of a data leak or misuse, we must inform

the concerned parties right away instead of trying to hide it (OECD). And look for ways to mitigate the risk as much as possible and have a plan in place for when such an event were to occur. Moreover, if the only way to guarantee the privacy of the customers was to suspend the project or terminate it, we must be ready to do so in order to maintain the trust that our customers have put in our organization (OECD). Tim Hortons failed to show any consideration to its customers until ordered by the court to do so; hence, another lesson we can learn from them.

5. Big Data Privacy Management Strategy

The Big Data pipeline for customer location data involves the following stages: data collection, data acquisition, data transmission, data storage, data processing, data analytics, data governance, and data visualization (MBAI 5110G - Week 7). In terms of implementing procedures for customer location data governance and oversight, it is necessary to implement them at every stage in the pipeline.

- **Design Stage**: Since this is the very first step, it is vital to establish a strong foundation for the security and privacy of our big data pipeline. At this stage, we should define the parameters of our project, including the type and amount of data that will be required and how this data will be obtained. Special consideration must be given to obtaining meaningful consent from the customer to use their personal data for our purposes. Additionally, at this stage, we must also note down the hardware and software requirements for this project, including any cloud space that might be needed for storage.
- **Development Stage**: This is the stage where coding experts start to clean up the raw data and prepare it for further analysis. It is important that these engineers can keep the data secure through the use of encryption techniques. The engineers should also take into consideration that the data is meant to be used only for the purposes laid out in the original project plan, and any deviations from that plan will not be tolerated.
- **Testing Stage**: Once the pipeline has been designed, it needs to be tested to ensure its rigidity against malicious attacks. It is wise to hire ethical hackers whose objective is to break into the data files and either corrupt them or transfer them to a third party. This could help develop protocols that can be implemented in case of a security breach, and our organization will know how to deal with such events if they were to happen.
- **Deployment Stage**: The deployment part is when the big data pipeline goes live and the customer data is recorded, stored, and transmitted. This is an extremely critical juncture in our project and therefore needs to be handled with the utmost significance. There needs to be guidelines that the engineers can refer to in order to ensure that procedures are running smoothly and, more importantly, to identify errors.
- **Post-Implementation Stage**: Once the big data pipeline has been deployed for some time and the analysts have started to generate insights from the data, it does not mean that the pipeline will continue to work flawlessly and does not require any oversight. A best practice would be to set up a team of engineers who can conduct regular audits on the system to ensure that all processes are running as designed and that there are no inaccuracies, malfunctions, or breaches.

In sections four and five, we have stated several procedures and methods that our organization can make use of to better secure the big data pipeline with respect to customer

location data. For the purposes of our privacy management strategy, we believe these recommendations can help our organization not make the same mistakes as Tim Hortons.

By following simple rules such as obtaining explicit consent from customers before accumulating their data, implementing secure data storage and transmission practices by setting up a chain of command and restricting access to the data only to the necessary personnel, de-identifying data in a way that it cannot be re-identified, conducting regular audits at every stage in the pipeline, keeping the customers updated of any privacy breaches, and most importantly, sticking to the project plan and using the data in an appropriate and ethical manner, our organization can set itself apart from the competition.

We believe that by incorporating these strict measures at every stage of the development, deployment, and post-deployment processes, we can ensure that data governance and privacy are at the forefront of our organization's objectives. Moreover, by creating a regulated environment, we drastically reduce our chances of ever engaging in unethical or unlawful data practices and will always be held in high regard by our customers.

6. Conclusion

In this report, we summarize Tim Hortons' illegal data collection of customers' location through their mobile devices and the reason behind such a blunder, which was poor data governance laws and weak internal regulation. Based on this, we provided a set of guidelines and rules for our organization to consider while designing and deploying their own big data pipeline that encompasses customer location data as well. We believe that by following this set of rules, we can create a privacy management strategy that, when adhered to, will not cause us any legal troubles.

References

5 principles of data ethics for business. (2021, March 16). Business Insights Blog. https://online.hbs.edu/blog/post/data-ethics

Bennett, S. (2019, June 1). Big data, privacy and information governance: Incorporating an ethical based assessment. *Sibenco Legal & Advisory*. https://www.sibenco.com/big-data-privacy-does-your-organisation-need-an-ethical-based-approach/

Bronskill, J. (n.d.). *Tim Hortons app collected vast amounts of sensitive data: Privacy watchdogs*. BNN. Retrieved March 13, 2023, from https://www.bnnbloomberg.ca/tim-hortons-app-collected-vast-amounts-of-sensitive-data-privacy-watchdogs-1.1773347

Good practice principles for data ethics in the public sector—Oecd. (n.d.). Retrieved March 13, 2023, from https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm

Number of tim hortons locations in canada in 2023. (n.d.). ScrapeHero. Retrieved March 13, 2023, from https://www.scrapehero.com/location-reports/Tim%20Hortons-Canada/

Robertson, A. (2022, June 2). *Canadian government slams Tim Hortons for using its app to spy on customers*. The Verge. https://www.theverge.com/2022/6/2/23151517/canada-privacy-commission-tim-hortons-app-data-location-tracking-investigation-results

Technica, J. B., Ars. (n.d.). Your tim hortons coffee app knew where you were at all times. *Wired*. Retrieved March 13, 2023, from https://arstechnica.com/tech-policy/2022/06/tim-hortons-coffee-app-broke-law-by-constantly-recording-users-movements/

Tim hortons | the canadian encyclopedia. (n.d.). Retrieved March 13, 2023, from https://www.thecanadianencyclopedia.ca/en/article/tim-hortons