

Teaching Case
**The Data and the Donut – Tim Hortons Mobile App and
Non-Consensual Collection of Private Information**

Brayden G. Royston and Prescott C. Ensign

Recommended Citation: Royston, B. G., & Ensign, P. C. (2026). Teaching Case: The Data and the Donut – Tim Hortons Mobile App and Non-Consensual Collection of Private Information. *Journal of Information Systems Education*, 37(4), 455-463. <https://doi.org/10.62273/MQEA6197>

Article Link: <https://jise.org/Volume37/n4/JISE2026v37n4pp455-463.html>

Received:	September 7, 2025
First Decision:	October 24, 2025
Accepted:	January 25, 2026
Published:	December 15, 2026

Find archived papers, submission instructions, terms of use, and much more at the JISE website:
<https://jise.org>

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Teaching Case

The Data and the Donut – Tim Hortons Mobile App and Non-Consensual Collection of Private Information

Brayden G. Royston

David R. Cheriton School of Computer Science

University of Waterloo

Waterloo, Ontario, Canada

braydengroyston@gmail.com

Prescott C. Ensign

Lazaridis School of Business & Economics

Wilfrid Laurier University

Waterloo, Ontario, Canada

ensign@wlu.ca

ABSTRACT

Canadians often hold a special place in their hearts for *Tim Hortons*, but what if Tim Hortons began collecting sensitive data without telling its customers? This is exactly what was revealed in the summer of 2022. Tim Hortons' mobile app collected data, including precise geolocation, from users who downloaded it to their smartphones without telling them about the tracking. When Tim Hortons released its updated mobile app, it promised customers a new way to interact with the coffee and restaurant chain while receiving promotions and coupons for their favorite menu items. Customers knew some data would be recorded – their order history and favorite menu items, to name a few – but they did not know the app was continuously tracking their geolocation data, even when closed. These data were then used by Tim Hortons to create targeted advertisements based on whether the user was walking, cycling, at home, or at work. Collecting data this way is illegal, and Tim Hortons eventually faced four class-action lawsuits and settled for roughly what might amount to C\$30 million. This payout would be in the form of free drinks and donuts to affected customers. The reader is left to consider whether this was enough compensation, and how Tim Hortons can prevent, or be prevented from, illegally capturing customer data in the future.

Keywords: Privacy, Ethics, Transparency, Application development

1. INTRODUCTION

It was the middle of July 2022, and *Tim Hortons* customers were out enjoying the beloved coffee shop's *Creamy Chills*, icy beverages that welcomed the hot summer weather. Those at Tim Hortons tasked with public relations, legal/regulatory compliance, and crisis management had other things on their minds. It turned out that one of its key customer engagement tools, the Tim Hortons mobile app, had been tracking the data of users to an unreasonable degree (Office of the Privacy Commissioner of Canada, 2022a). The

investigation found that “the app was gathering locations as frequently as every few minutes, whether or not the app was open – even if [customers] explicitly limited that collection through settings” (Fingas, 2022). Tim Hortons was not the first company to employ questionable practices in data collection strategies and probably would not be the last. So, what did this situation mean for Tim Hortons, and how did it relate to the world of consumer data privacy on a grander scale? This case study aims to help readers examine the ethical and legal implications of corporate data practices.

2. BACKGROUND

Figure 1 provides an image of a quintessential Canadian bricks-and-mortar Tim Hortons restaurant. Tim Hortons was a multinational fast-food restaurant chain with 5,350 restaurants in 15 countries as of July 2022 that had originally found its niche in coffee and donuts. The restaurant was created in 1964 in Hamilton, Ontario, Canada (Tim Hortons, n.d.-a). Jim Charade partnered with professional ice hockey player Tim Horton, and as the company evolved, its headquarters were eventually moved to Toronto, the capital and largest city in Ontario. Tim Hortons adapted as a business, and while its core had remained coffee and donuts, adapting its services and menu items as consumer preferences changed over time had been paramount to its evolution as a fast-food chain.



Figure 1. Typical Tim Hortons Restaurant With Drive Thru

3. THE MOBILE APP

Figure 2 portrays the Tim Hortons mobile app. Released in July 2017, after a lengthy process of development and refinements, the Tim Hortons app was a new means for customers to interact with Tim Hortons and vice versa. There was a two-way flow of communication, with customers showing Tim Hortons their buying habits and Tim Hortons enticing customers with deals. The app was a competitive response to an app released by Starbucks two years earlier, which provided similar functionality (Harris, 2017). Once downloaded, the smartphone app allowed customers to browse Tim Hortons’ menu, view coupons and specials, and order food before arriving at a Tim Hortons location (Tim Hortons, n.d.-b). Along with this, the app allowed customers to keep track of points, which previously could only be done with a physical *Tims Rewards* card, to eventually redeem for free beverages and food (Tim Hortons, n.d.-b). The refreshed app, released in May of 2019, did a bit more. In general, the mobile app gave customers a more personalized and smooth Tim Hortons experience, but unbeknown to customers who had downloaded the app, they were getting closer to Tim Hortons than they realized (Office of the Privacy Commissioner of Canada, 2022b).

“Tim Hortons clearly crossed the line by amassing a huge amount of highly sensitive information about its customers. Following people’s movements every few minutes of every day was clearly an inappropriate form of surveillance. This case once again highlights the harms that can result from poorly designed technologies as well as the need for strong privacy laws to protect the rights of Canadians.” – Daniel Therrien, Privacy Commissioner of Canada

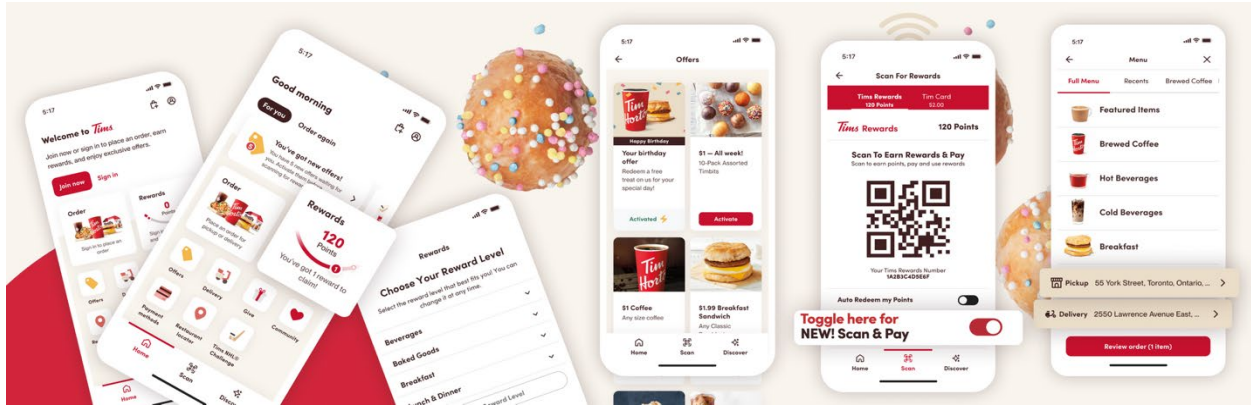


Figure 2. Tim Hortons Mobile App

Tim Hortons’ previous reward program had been successful, perhaps too much so. “Make seven trips to Tim Hortons to buy a coffee or baked good – and get a free coffee or baked good on your next visit. The large number of giveaways ate into revenues” (Gerlsbeck, 2020). José Cil, CEO of Restaurant Brands International (Tim Hortons’ parent company), stated that the Tims Rewards program was partly to blame for a US\$150 million sales drop the previous year. The reward program was revalued in line with others in the industry (e.g., McDonald’s or Starbucks) that pushed the dollar value of purchases over the frequency of purchases. Instead of seven visits to get an item, it was closer to 16 to 20 visits. Refer to Table 1 for a summary of key events described in this case study.

Date	Event
July 2017	Tim Hortons mobile app released.
May 2019	Tim Hortons refreshed mobile app released with new functionality.
June 2020	Office of the Privacy Commissioner of Canada announces investigation.
May 2022	Federal privacy commissioner investigation states the app unnecessarily collected vast amounts of data without obtaining adequate consent.
July 2022	Class action lawsuits emerge over privacy invasion.
February 2023	Québec court approves class action settlement.

Table 1. Timeline of Events

4. MOBILE APP DATA COLLECTION

Figure 3, taken from the Radar Labs website, indicates the services from Tim Hortons’ third-party geolocation provider. While the purpose of the Tim Hortons mobile app was to let customers order food ahead of time and track their rewards, a federal report found that the app had been tracking users’ movements and recording data as frequently as every few minutes (CBC, 2022). The app then stored these geolocation data, completely unbeknown to customers (Al Mallees, 2022). Tim Hortons could then use these data for a variety of tasks that utilized the user’s location (CBC, 2022). First, the app inferred where

the user lived and worked based on the amount of time and time of day that they would spend at specific locations. The purpose of having these pieces of information was originally to deliver targeted ad campaigns that contained content tailored to where people lived and worked, although Tim Hortons claimed that these ad campaigns were never actually executed.

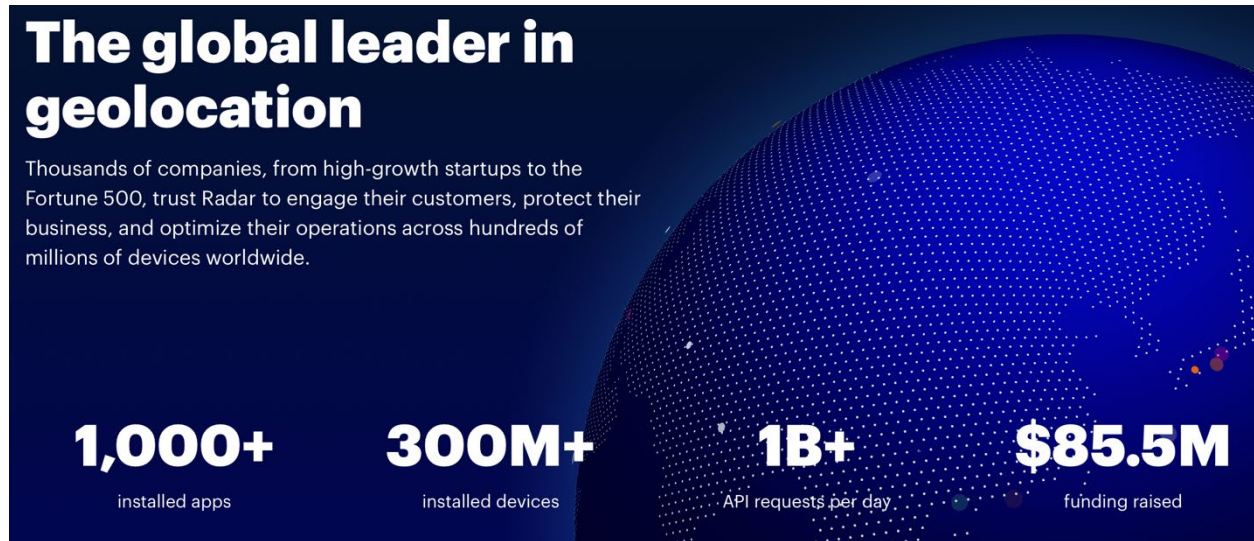


Figure 3. Screenshot From Radar Labs “About” Page

4.1 Legal Findings

The Tim Hortons mobile app used constants such as “user_entered_home.” Figure 4, with material from the OPCC (2022b), provides examples of the code to track user location arrival and departure events for home, work, non-Tim Hortons restaurant, etc. The constants represented events that occurred in the code, essentially displaying real-time data which a software engineer could use to reference a customer’s precise location as well as whether they were moving. The Office of the Privacy Commissioner of Canada (2022b) called this “granular location data” which recorded precise longitude and latitude coordinates as well as altitude (McLeod, 2020a). Such information could identify when a person’s smartphone that had downloaded the app “entered a Starbucks, Second Cup, McDonald’s, Pizza Pizza, A&W, KFC, or Subway” (Office of the Privacy Commissioner of Canada, 2022b). The fact that Tim Hortons collected data that led to such intimate insights, such as whether someone vacationed for a week, went out of town with their kids, waited for a bus, biked to a location, or even walked or ran to a location, caused consumers discomfort. Boshell (2019) states that data collection, as it was for Tim Hortons, was often done by a third party and often such data were de-identified or anonymized and then sold to another party.^[EN1] Such secondary markets were not covered by law, and data could be reattributed to an individual to profile them, their buying behavior, and activities/lifestyle (Boshell, 2019).

- USER_ENTERED_HOME; USER_EXITED_HOME;
- USER_ENTERED_OFFICE; USER_EXITED_OFFICE;
- USER_STARTED_TRAVELING; USER_STOPPED_TRAVELING;
- USER_ENTERED_GEOFENCE; USER_EXITED_GEOFENCE

Figure 4. Sample of Constants in the Tim Hortons Mobile App Source Code

4.2 User Consent Issues

The Tim Hortons mobile app did have a permission prompt. Figure 5, with material from OPCC (2022b), provides the prompt for the Apple and Android operating systems, but it did not make the customer aware that the app would be tracking geolocation data regardless of their response to this prompt.^[EN2] This action violated data privacy laws in Canada since the mobile app did not disclose that it was gathering these location data. Figure 6, with material from the Department of Justice (2025), illustrates the relevant Canadian privacy legislation referenced in this case study. Furthermore, the app continued to record granular location data even when it was closed. A company in Canada was required by federal law to be transparent and disclose to the customer whether and when it would be collecting data, and to disclose what any collected data would be used for. In addition, a company had 30 days from receiving a request to provide the user the data that it held that concerned them.

Android – “Allow Tim Hortons to access your location while you are using the app? We use your location to help you find nearby restaurants and provide you with more relevant marketing & offers.”

iOS – “We use your location to help you find nearby restaurants and provide you with more relevant marketing & offers.”

Figure 5. Consent to Access a Device’s Location Functionality

In PIPEDA (Personal Information Protection and Electronic Documents Act) 2020, section 8.1, the Government of Canada states the following regarding the collection of consumer data:

Organisations must be open and transparent about their practices and inform individuals about the information collected, used, and disclosed, as well as the purposes for such activities, among other requirements. One way that organisations meet this obligation is through a public-facing privacy policy...

Figure 6. Data Privacy Laws in Canada

Laws exist to ensure transparency between a company and the customer regarding all data collection. The fact that Tim Hortons did not abide by the law, regardless of whether it did so on purpose, resulted in the organization being propelled into a legal battle.

4.3 Data Deletion Measures

To compensate customers who were impacted, Tim Hortons proposed giving them an in-store credit for a “free hot beverage and a free baked good” (Edmiston, 2022). This settlement equated to approximately C\$29.7 million in value (Canadian Press, 2022), while total revenue for Tim Hortons in 2022 was C\$7.164 billion. Additionally, Tim Hortons committed to deleting geolocation information that it may have collected and that its direct, third-party service provider, Radar Labs Inc., would do likewise. Figure 7 relays information collected by the Office of the Privacy Commissioner of Canada (2022b). Although the compensation solution of providing a beverage and a baked good was on-brand and possibly an acceptable solution for some customers, questions lingered. Some questioned whether this award was monetarily appropriate given the sensitivity of the data, arguing that customers should have been compensated more. Tim Hortons was not forced to release what it and Radar Labs Inc. had fully planned to do with the geolocation data. What was the root cause of this situation, and what measures might Tim Hortons put in place to avoid something like this happening again?

Radar asserts our “business model is to sell software, not data.” OPCC (2022b) noted that Radar’s website claimed that it had installed the SDK on over 100 million devices, and that it processes over 100 billion locations per year. As of 2025, Radar received over 1 billion API requests per day and had over 300 million devices installed with its APIs and SDKs.^[EN3]

Radar asserts that “disclosure of de-identified or aggregated data, that such information is not in itself personal information regulated by any Canadian private sector privacy legislation (except the Québec Private Sector Act).”

OPCC (2022b) came to the finding that Tim Hortons did not meet its obligations under the PIPEDA... In our view, Tim Hortons did not collect or use personal information for appropriate purposes in the circumstances, as required under the Acts... While we did not conduct an in-depth review of Tim Hortons’ overarching Privacy Management Program, the nature of certain contraventions identified through our investigation is indicative of a broader lack of accountability.

Tim Hortons collected vast amounts of sensitive personal information for more than a year, without ever using it for the stated purpose; and attempted to obtain consent via permission requests that were materially different across mobile platforms, and inconsistent with the App’s actual operation.

Figure 7. Overview of Radar Labs’ Data Practices and the Office of the Privacy Commissioner of Canada’s Findings

5. THE BROADER LANDSCAPE OF DATA PRIVACY

The public stance towards data collection exuded more and more caution, and this was evident in the laws put in place around the globe (Barnett, 2022). This made measures taken to prevent data collection infringements more stringent than ever. But that did not mean enforcement was keeping pace. McLeod (2020b) was critical, noting that “the inescapable conclusion is that Canada’s data privacy law hasn’t kept pace with 21st century technology, and legal compliance is half-hearted at best.” When Google illegally tracked users’ location data (in a similar manner to Tim Hortons), it was hit with a fine of approximately US\$400 million. Table 2 shows penalties imposed for violations in data privacy. The European Union adopted a comprehensive, principles-based approach to data privacy, with individual consent serving as a cornerstone, whereas the United States adopted a sector-specific approach. The EU started from a prohibition on collecting data unless there was an established legal basis for doing so, whereas the US allowed free collection unless there were specific prohibitions against it. The EU could impose fines of up to 4% of an entity’s global revenue. Canada was moving toward a more comprehensive treatment. For example, Bill C-27 would have enacted greater consumer privacy protection by replacing and updating PIPEDA, creating a Personal Information and Data Protection Tribunal, addressing the design, development, and deployment of AI systems, and requiring risk identification and mitigation measures, but by mid-2025 Bill C-27 had not advanced.

Known incidents corroborated the concern that data practices such as those employed by Tim Hortons were not a one-off occurrence. Did Tim Hortons and other companies act in bad faith or simply follow industry practices to stay competitive? Was there a realization that the risk associated with operating unlawfully was present, and did organizations assess that risk and still choose to break laws for financial gain? There were significant deterrents for tech-enabled companies to contemplate data privacy issues, but it seemed these fines were just another expense budgeted. Within an organization such as Tim Hortons, there would typically be internal audits, compliance oversight, and individuals tasked with design ethics. It appeared that governance mechanisms were absent or had failed.

Company, Date	Fine, Company Revenue	Incident
Google, 2022	US\$400 million, US\$282 billion	Illegal location tracking.
Instagram, 2022	US\$403 million, \$US40 to 50 billion	Failure to protect children's privacy settings on its platform.
Meta, 2022	US\$255 million, US\$116 billion	Insufficient protection against data scraping.
Facebook, 2023	US\$1.2 billion, \$US135 billion	EU-US data transfers.
Meta (Facebook & Instagram), 2023	US\$385 million, US\$135 billion	Changing terms of service forced users to consent to personalized advertising as a condition of use.
Facebook, 2024	US\$260 million, US\$150 billion	"View As" flaw left users vulnerable to attackers.
Meta, 2024	US\$90 million, US\$165 billion	Failing to protect user passwords and reporting issues.
Equifax, 2019	US\$575 million, US\$5 billion	Database leak.
Amazon, 2021	US\$877 million, US\$500 billion	Data breach, failure to comply with data processing laws.
Didi Global, 2022	US\$1.19 billion, US\$20 billion	Violating data security laws, failing to protect personal information of users.
TikTok, 2025	US\$600 million, US\$10 billion	"...sent the personal data of Europeans to China illegally and wasn't transparent enough with users" (O'Regan, 2025).

Table 2. Data Privacy Violations and Fines

6. DATA PRIVACY FROM THE CUSTOMER LENS

Did customers worry about what data were tracked and what organizations did with collected data? For those with a smartphone, so much data (geolocations, IP addresses, names, emails, photos, videos, etc.) was generated, whether or not it was securely stored or in the public domain (Vigderman & Turner, 2024). Did customers even care if an app like that of Tim Hortons surveilled them? As Radar Labs' (n.d.) website states, "a user may send a location event to Radar in the background (assuming they have granted background location permissions) without opening the app." What governance did a person have over "their" data at this time, and was it wholly their responsibility to determine where and how these data were distributed? It may not have been reasonable for a person to be able to use technology like mobile phones and apps, both of which track vast amounts of personal data, and be fully educated on where such data were going and what those data were being used for. Customers' digital literacy was important as was the role of app stores as gatekeepers. The regulatory lag between the offense occurring, the OPCC identifying it, and then doing something about it was notable. In short, data privacy was a shared responsibility.

7. ACKNOWLEDGMENT

This work was made possible by the Social Sciences and Humanities Research Council of Canada.

8. ENDNOTES

- EN1. Radar Labs product “Geofencing Core Platform” pricing: <https://www.vendr.com/marketplace/radar-labs>. Radar Labs “Data Processing Addendum” was found at <https://radar.com/dpa> and its “Privacy Notice” at <https://radar.com/privacy#share>.
- EN2. Geolocation was the process of identifying the geographical location of an item or person. Geofencing created a virtual perimeter around a real-world area to trigger a response when a device entered or exited that zone. It was a way to monitor an asset or individual’s proximity to a defined area, which may be used to trigger an automated action or alert.
- EN3. An SDK was a software development kit, a set of tools in an installable bundle that helped developers create applications for a particular platform, operating system, or service. Such kits included resources like code libraries, compilers, debugging, documentation, and APIs. An API was an application programming interface, a set of rules and protocols that permitted different applications to communicate with each other. Further details on Radar Labs SDK may be found here <https://docs.radar.com/sdk/sdk> and details on its APIs here <https://docs.radar.com/api>.

9. REFERENCES

- Al Mallees, N. (2022, June 1). Tim Hortons App Tracked Too Much Personal Information Without Adequate Consent, Investigation Finds. *CBC News*. <https://www.cbc.ca/news/business/tim-hortons-app-report-1.6473584>
- Barnett, K. (2022, November 15). Google’s \$400m Penalty and Impact of the 5 Heftiest Data Privacy Fines on 2023 Ad Plans. *The Drum*. <https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans>
- Boshell, P. M. (2019, March 25). The Power of Place: Geolocation Tracking and Privacy. *Business Law Today*. <https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/>
- Canadian Press. (2022, July 29). Tim Hortons Offers Coffee and Doughnut as Proposed Settlement in Class Action Lawsuit. *CTV News*. <https://www.ctvnews.ca/business/article/tim-hortons-offers-coffee-and-doughnut-as-proposed-settlement-in-class-action-lawsuit/>
- CBC (2022, August 7). Ticketmaster Troubles; Tim Hortons Offers Treats to Settle Class-Action Suits: CBC’s Marketplace Cheat Sheet. *CBC News*. <https://www.cbc.ca/news/business/marketplace-cheat-sheet-1.6543265>
- Department of Justice. (2025). Personal Information Protection and Electronic Documents Act (S.C. 2000, c.5). *Government of Canada*. <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/>
- Edmiston, J. (2022, August 4). ‘Sweet Deal’ for Tims? Coffee-and-Doughnut Privacy Breach Settlement a Marketing Win, Says Expert. *Financial Post*. <https://financialpost.com/news/economy/a-sweet-deal-for-tims-coffee-and-doughnut-privacy-breach-settlement-a-marketing-win-expert>
- Fingas, J. (2022, June 2). “Tim Hortons App Tracked Donut Lovers’ Locations Without Consent: An Investigation Found the Canadian Restaurant Violated Users’ Privacy.” *Engadget*. <https://www.engadget.com/tim-hortons-app-location-tracking-investigation-200058746.html>
- Gerlsbeck, R. (2020, March 10). A Double-Double, and Don’t Forget the Data. *Smith School of Business, Queen’s University*. <https://web.archive.org/web/20201101113519/https://smith.queensu.ca/insight/content/a-double-double,-and-dont-forget-the-data.php>
- Harris, S. (2017, July 19). Tim Hortons Set to Launch Order App After Months of Delay and Controversy: Franchise Owners Launched a Protest in March to Block an Earlier Release of the App. *CBC News*. <https://www.cbc.ca/news/business/tim-hortons-mobile-order-and-pay-app-rbi-franchisee-1.4211247>
- McLeod, J. (2020a, August 21). Canada’s Privacy Laws Have ‘No Teeth’: What I Learned During an Eight-Month Investigation Into Tim Hortons’ Data Tracking. *Financial Post*. <https://financialpost.com/technology/canadas-privacy-laws-have-no-teeth-what-i-learned-during-an>

[eight-month-investigation-into-tim-hortons-data-tracking-efforts](#)

- McLeod, J. (2020b, July 16). Want the Personal Data Corporations Have on You? Good Luck, It's Not Nearly as Simple as It Sounds. *Financial Post*. <https://financialpost.com/technology/want-the-personal-data-corporations-have-on-you-good-luck-its-not-nearly-as-simple-as-it-sounds>
- Office of the Privacy Commissioner of Canada. (2022a, June 1). Tim Hortons App Violated Privacy Laws in Collection of 'Vast Amounts' of Sensitive Location Data. *Government of Canada*. https://web.archive.org/web/20220608150036/https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220601/
- Office of the Privacy Commissioner of Canada. (2022b, June 1). Joint Investigation Into Location Tracking by the Tim Hortons App. *Government of Canada*. <https://web.archive.org/web/20220608185607/https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-001/>
- O'Regan, E. (2025, May 2). TikTok Hit With €530M Fine After Illegally Sending Users' Data to China. *Politico*. <https://www.politico.eu/article/tiktok-hit-with-e530m-privacy-fine-ireland-china-data/>
- Radar Labs. (n.d.) FAQs. <https://docs.radar.com/faqs>
- Tim Hortons. (n.d.-a). About Us. *Tim Hortons*. <https://www.timhortons.ca/?lang=en>
- Tim Hortons. (n.d.-b). Mobile App FAQs: About the App. *TimHortons.com*. <https://www.timhortons.com/mobile-app-faq#AbouttheApp>
- Vigderman, A., & Turner, G. (2024). The Data Big Tech Companies Have on You. *Security.org*. <https://www.security.org/resources/data-tech-companies-have/>

AUTHOR BIOGRAPHIES

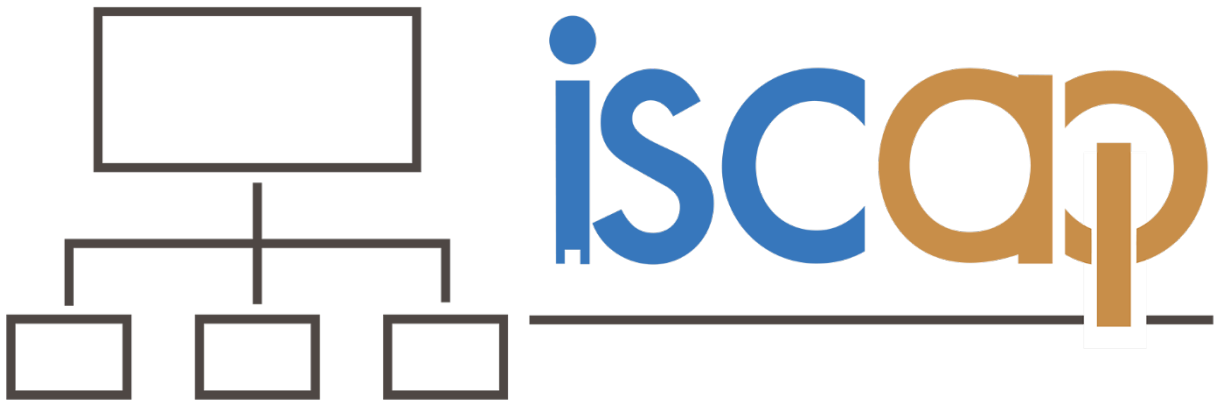
Brayden G. Royston is a software engineer at Apple in Seattle, Washington. He completed a Bachelor of Computer Science at the University of Waterloo and a Bachelor of Business Administration at Wilfrid Laurier University. He has held internships as a software engineer at Tesla, NimbleRX, Gadze Finance, TD Labs, Innovapost, and Hatch as an engineering consultant. He has served as VP of engineering at UW Blueprint, an organization that combines science and technology for social good; coach and competitor for Laurier's Case Team; program assistant at Shad Canada; technical project lead at UW Blockchain Club; mentor at Hack the North; tech executive at The GoldenHack; council representative at the UW mathematics society; and campus ambassador at Xlerate Lazaridis.



Prescott C. Ensign is a Professor in the Lazaridis School of Business & Economics at Wilfrid Laurier University. His PhD is from École des Hautes Études Commerciales, Université de Montréal. He has served on the faculty of state universities in California and Ohio, as well as several in Canada. He is the recipient of a Fulbright Scholarship and has received recognition for his teaching and research. Recent publications focus on applied business ethics; Indigenous entrepreneurship; social enterprises and innovation; and economic and social development in rural and remote areas, including the survival of Canada's 60+ short line freight railways. His research has appeared in *Sloan Management Review*, *Entrepreneurship Theory and Practice*, *Regional Studies*, *Thunderbird International Business Review*, and *Small Enterprise Research*.



INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the *Journal of Information Systems Education* have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©2026 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, *Journal of Information Systems Education*, editor@jise.org.

ISSN: 2574-3872 (Online) 1055-3096 (Print)