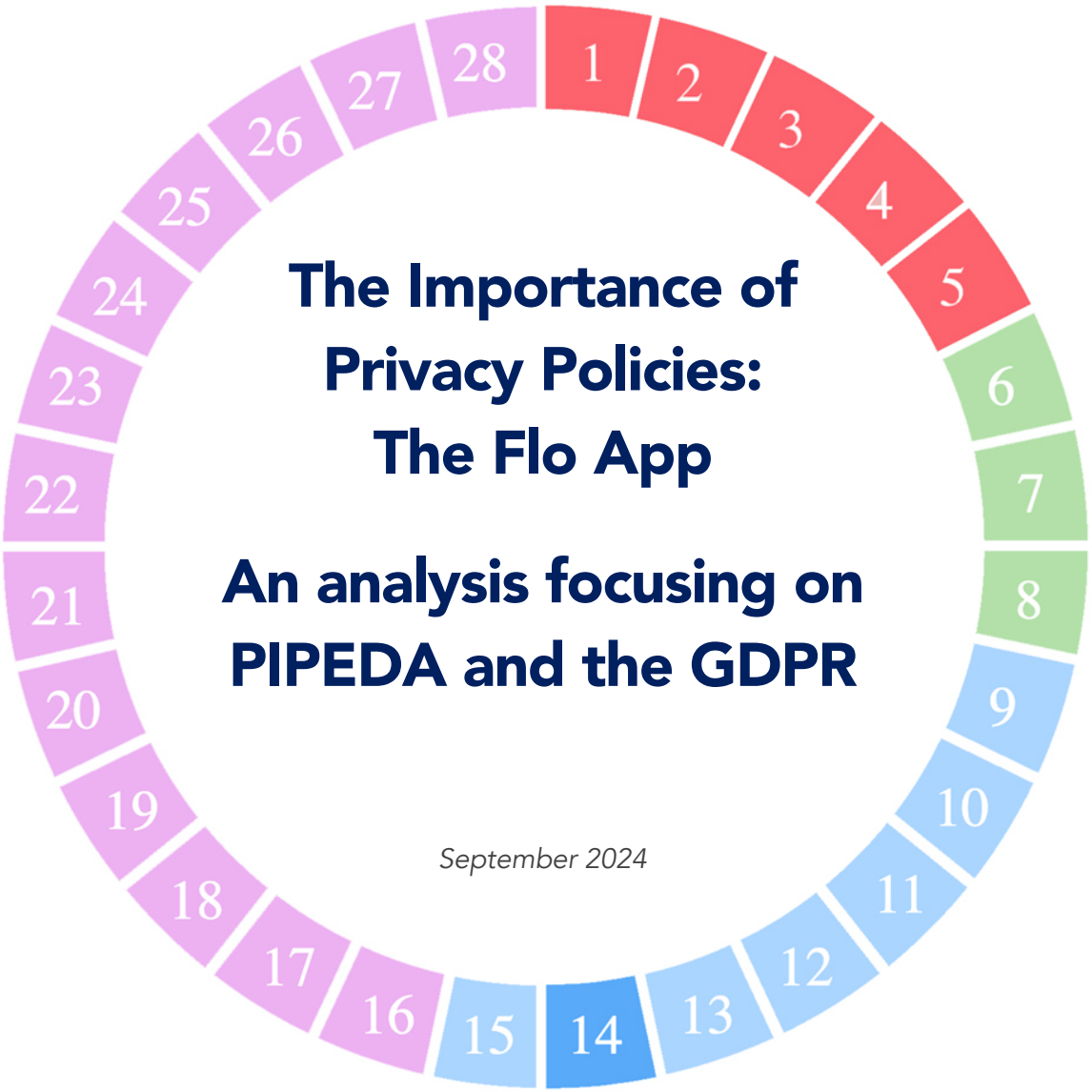

The Importance of Privacy Policies: The Flo App

An analysis focusing on PIPEDA and the GDPR

September 2024

The Voice for Privacy and Access
Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Priveé
www.PACC-CCAP.ca

Abstract: This article explores the current privacy policies used in healthcare applications, specifically the women's health application Flo, focusing on a comparison between Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the General Data Protection Regulation (GDPR) in the European Union. This article emphasizes different elements analyzed on the surface such as the type of personal information Flo collects and the ambiguous language that might be problematic from the use of the word *may*, from a GDPR and PIPEDA perspective.

Updates to this report

This is Version 1.0 of this report, which may be updated periodically.

About the author

This report was produced by the Privacy and Access Council of Canada, with Carla Jiron as lead author. With a background in law, Carla seeks to use her expertise to educate about important issues affecting their rights and freedoms.

We also thank the staff and faculty at Dámh na nDaonnachtaí & na nEolaíochtaí Sóisialta, Ollscoil Chathair Bhaile Átha Cliath / Faculty of Humanities & Social Sciences, Dublin City University for their assistance in facilitating the collaboration between EMILDAI and PACC.

Note to readers

Every effort has been made to verify the accuracy of the information contained in this report. All information was believed to be correct as of September 2024.

Nevertheless, the Privacy and Access Council of Canada - Conseil du Canada de l'Accès et la vie Privée cannot accept responsibility for the consequences of its use for other purposes or in other contexts.

Quotation permitted. Contact Privacy and Access Council of Canada - Conseil du Canada de l'Accès et la vie Privée at media@pacc-ccap.ca regarding derivatives requests.

Table of Contents

Setting the Stage

Over the last decade, the development of healthcare applications has been skyrocketing. Several healthcare applications have fulfilled the demand, including tracking individuals' fitness progress, weight loss, heart rate, sleep and several other health metrics. For these applications to be successful, they need an essential element — you.

Once a person downloads healthcare applications on their phone and starts registering, they must consent to their personal information being collected, processed, and stored. They have no real option but to click ¨I consent¨; and many users click the box and forget about it. However, when people are scrolling around their social media, they suddenly see ads related to supplements for the gym, fertility pills, or scheduling medical appointments for anxiety. People might ask themselves: How does it know I go to the gym? That I want to be pregnant? That I have anxiety? Is my phone reading my mind? The truth is less fanciful — your health-related app might share your personal information with third parties for marketing purposes.

The Canadian Legal Structure

Canada is legally structured through a hierarchy of federal, provincial and municipal jurisdictions according to the country's founding constitution. The Federal law applies to the entire country. Canada has ten provinces and three territories, each with its own government and legislature. In addition, some municipalities pass bylaws that only apply within the boundaries of their municipality. In some cases, federal and provincial laws overlap and must cooperate to find harmony. Nevertheless, federal law has higher supremacy than provincial law. This article compares Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), a federal law, and the EU's General Data Protection Regulation (GDPR).

PIPEDA and GDPR

Consent and privacy are fundamental concepts in both PIPEDA and the GDPR. In PIPEDA, consent is required for the collection, use, and disclosure of personal information by federally-regulated private sector organizations and all organizations in the country's three territories, and consent can be express or implied depending on the sensitivity of the information. When the information is sensitive, express consent is warranted. While consent is not clearly defined in PIPEDA, Schedule 1 of PIPEDA — the "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96" — outlines the types of consent and how to obtain it. It also mentioned the requirements for valid consent which needs to be meaningful, informed and voluntary. This is a great deficiency in PIPEDA since there is no clear definition of consent whereas the GDPR does define it and explains each type

of consent alongside its key elements. Under PIPEDA, privacy focuses on an individual's right to know how their personal information is handled, to access it, and to request corrections of fact. The GDPR also requires consent to collect and process personal information, and explicit consent when referring to special categories of personal information such as sensitive information. Also, both regulations consider ticking or checking a box as an adequate manner to provide written consent. Both laws aim to protect personal information, but the GDPR emphasis provides a higher standard of consent and broader rights for individuals, such as the right to be forgotten.

While PIPEDA and the GDPR share similarities in protecting individuals' privacy and ensuring consent is obtained before or at the time of collecting personal information, they differ in scope and approach. PIPEDA applies primarily to commercial activities and focuses on balancing privacy protection with reasonable business needs, allowing for implied consent in certain contexts. In contrast, the GDPR applies to all entities that process personal data within the EU, regardless of whether or not the activity is commercial in nature, and it requires explicit consent in most cases. Moreover, the GDPR mentions special categories of personal information where they include health data and even goes on to mention anything concerning a natural person's sex life or sexual orientation. While PIPEDA defines personal health information by mentioning *"any information concerning the physical health of the individual"* or *"any health services provided to the individual"*, for example. Both frameworks mandate transparency and accountability from organizations, but the GDPR provides more robust enforcement mechanisms and heavier penalties for non-compliance. Overall, while both regulations emphasize the importance of consent and privacy, the GDPR adopts a more stringent and comprehensive approach compared to PIPEDA.

Flo Health, Inc. vs. Canada

Flo Health, Inc. ("Flo") is an application designed for women. Flo is an ovulation calendar, period tracker, and pregnancy app. Per their website, Flo´s purpose is *"to build a better future for female health by helping you harness the power of your body signals"*[1]. Their slogan is *"know your body. own your health"*[2]. However, do users really *"own their health"* when using Flo? In this context, do users *own* the sensitive data this application collects? The members of a class action under way in Canada contends that they did not.

[1] https://flo.health/about-flo

[2] Ibid.

Foreman & Company, the law firm leading the Canadian privacy law class action against Flo Health, Inc. alleges that Flo unlawfully collected, disseminated and monetized extremely sensitive health and personal information collected from Canadians who used the Flo: Health & Period Tracker app"[3]. The class members that can be included are women who used the app between June 1, 2016, and February 23, 2019.

On March 5, 2021, a statement of claim was issued across Canada, including Ontario, British Columbia and Quebec.[4] On January 6, 2022, the Ontario action was stayed in favor of proceedings out of British Columbia, excluding Quebec. The Quebec action was approved to proceed on November 30, 2022.

The British Columbia court certified the class action on March 7, 2024. In Canada, when a court certifies a class action it does not mean that the allegations have been proven, but that there is a benefit of it being presented before a judge. This is based on the latest status of the case per the Foreman & Company[5] website and CBC News[6]. This case is still ongoing.

The Trade-Off: The Price of Personal Information

On Flo´s website, under the privacy policy section, you can find all their privacy policies since their inception. The Flo app was launched in October 2015, and its original policy based on their website dates to June 15, 2016. The company's privacy policy changed thirteen times before February 23, 2019, changing two to three times each year until 2019. In 2019, its privacy policy changed seven times in that year alone, perhaps in response to the class action lawsuit.

Flo's original privacy policy mentions that "We may share information, including personally identifying information, with our affiliates (companies that are part of our corporate groups of companies, including but not limited to Facebook) to help provide, understand and improve our application". Flo also mentioned that it does not "sell or rent" any of the personal information it

[3] Flo Health, Inc., Class Action, Ontario Superior Court of Justice, alleging unauthorized collection and sale of personal health information by Flo Health, Inc. without user consent, violating privacy laws and causing damages to Canadian users of the Flo: Health & Period Tracker app. For more details, see Foreman & Company: https://www.foremancompany.com/flo-health-inc.

[4] Ibid.

[5] https://www.foremancompany.com/flo-health-inc.

[6] https://www.cbc.ca/news/canada/british-columbia/flo-health-privacy-class-action-1.7137600#:~:text=A%20Canadian%20class%2Daction%20lawsuit%20accusing%20a%20popular%20fertility%20tracking,been%20allowed%20to%20go%20ahead.

collects to third parties; nevertheless, it seems they might have shared some information with Facebook. However, what would be the benefit of sharing this information with Facebook at the time, and how is it related to the improvement of the app?

To answer this question, it is vital to understand the function and purpose of "software development kits" (SDKs). Simply put, an SDKs is a platform building tool in which all necessary components used to building and developing an application can be found in one single place. SDKs provide all the resources to develop an application and access the information collected and integrate it with third-party services such as Facebook. One of the many benefits for developers when using an SDK is the ease of optimizing the user experience based on user data meaning that they can track user behavior and what they prefer or might need all this per Amazon Web Services[7].

Essentially, by using an SDK that might be powered by Facebook, Google or Amazon they will provide the application is functionality and in exchange the application might have to share personal information of their users. It is a way for these companies to identify what the users prefer based on other applications data and facilitate advertising products they might be interested in on their own platforms or other third parties. The fuel for this to keep running is the user's personal information.

Some information collected by Flo is "sensitive" information, as defined in the GDPR, since it relates to users' healthcare, and more specifically, their sexual information. Research indicates that, from 2016 to 2019, Flo was built on an SDK powered by Facebook, so it is not unreasonable to expect that Flo might have shared their user's personal information with Meta to be able to continue using the SDK. Essentially, this is what the Canadian class action against Flo alleges they did between this time.

Flo: Privacy Policy

The latest Flo privacy policy (posted October 31, 2023) implied that Flo has learned from its mistakes. The current privacy policy has a different structure and wording than the original version.

The current Flo privacy policy has an interesting interface: from the start it mentions the word "security". Clearly, there is an interest in impressing upon users that the company cares about

[7] https://aws.amazon.com/what-is/sdk/

the protection of its users' data, which is important. Flo states it is ISO/IEC 27001 certified, meaning they have the highest standards for handling personal information8, but this is a security standard that focuses on information security management. Flo also describes its "anonymous mode" as "further privacy protection" since it allows the user to "access the app without your name, email address, or technical identifiers being associated with the data you put into the app". This assurance is followed with a mention that the users have complete control of their data, and offers a general email for inquiries about handling users' data.

In addition, Flo's policy uses the word *"may"* on several occasions. This can be problematic under the GDPR and PIPEDA since both regulations require transparency related to how personal information is collected, processed and stored. The word may can be ambiguous, since it provides uncertainty to the user on what information will be used and shared, and for what purposes. GDPR and PIPEDA emphasize that consent must be informed, specific, unambiguous, and given freely. Using vague language, such as the word "may", can be viewed as insufficient, and therefore non-compliant with these regulations.

Specifically, when Flo´s privacy policy mentions that information is obtained from external sources, it mentions that they *may* obtain additional information from the user from third parties to enhance or supplement existing information — as if the user's personal and sensitive information is insufficient. A couple of questions arise from this. For example, what information do you collect? Who is the third party?

These questions are answered—to a degree—in Flo's extensive and user-friendly privacy policy that defines general information as "When you sign up to use the Services, we may collect personal data such as your name, email address, year of birth, password, and place of residence and location information, including time zone and language. We may be able to infer your sex and/or gender by your use of the Services"[9]. This definition is consistent with the definition in PIPEDA and the GDPR but, by including the word "may", they once again create ambiguity and lack of transparency to what other types of information they might be collecting. Flo provides a non-exhaustive list of information that will be collected — but there is no mention about the sensitive information they will collect, such as user sexual health. A list of this information is warranted under both PIPEDA and the GDPR since the application predicts periods, ovulation and the highest chance of becoming pregnant — all of which requires collecting user-sensitive

[8] https://flo.health/privacy-policy

[9] Ibid.

information such as their period dates, sexual activity and symptoms. Full disclosure would be warranted under PIPEDA and the GDPR to provide transparency and certainty to the user of the information that will be collected, processed and stored.

The Flo privacy policy clearly states the purpose of processing users' data and provides a non-exhaustive list of examples alongside their definition, and users' privacy rights — which is required under PIPEDA and the GDPR. Other aspects of the policy are less clear. For instance, the last sections of the Privacy Policy include a section titled "United States" in which they point out that "personal information" includes sensitive information in accordance with California laws — and is the only instance throughout the policy that mentions sensitive information. Nonetheless, when they provide examples of the information, they might collect the examples only fit the category of personal information and not sensitive information.

They also explain the type of processing their third-party processors provide and mention their current SDK, AppsFlyer. They also mention that "*With your consent, we may share some of your non-health personal data with AppsFlyer to promote Flo's services*". Once again, they imply they might share the user's personal information to promote Flo´s services, with the user's consent.

The Price Tag

Per Med Tech News, Flo secured a $200 million investment from General Atlantic, a US-based equity investment firm. This investment pushed Flo´s valuation to more than USD $1 billion, making it the first digital women's health app to reach this milestone[10]. Flo offers a free version of its app, but users can opt for a subscription, typically priced at USD $9.99 per month. This subscription provides additional benefits such as advanced cycle tracking, personalized health insights, and an "ad-free experience", among other features. However, the ambiguity in Flo's privacy policy regarding the collection and use of personal and financial information raises concerns about the true value to users who subscribe.

The lack of transparent disclosure about what type of personal information might be shared with third-party services. By integrating AppsFlyer SDK, Flo not only maintains app functionality, but also might facilitate users being targeted with ads based on their sensitive information, and influencing their purchasing decisions.

[10] https://www.med-technews.com/news/medtech-business-merger-acquisition-finance-and-investment-news/flo-health-secures-more-than-200m-investment-from-general-at/

This approach can be seen as deceptive under PIPEDA and the GDPR, especially if it undermines the control that Flo claims users have over their information. Ultimately, the convenience of using the app for tracking periods, ovulation, or fertility might come at a higher price than the USD $9.99 monthly subscription, as it may involve compromising user privacy and sensitive information.

Ethics and Responsibility

Socrates once said, *"The unexamined life is not worth living."* Now, in these times, we might need to say an unexamined app is not worth using. However, what exactly should be examined?

Focusing on privacy policies, or trying to understand what might be important to the application through them, would be a start — but would this be enough? We can try to infer how ethical their practices are; but how can ethics be measured in this context? PIPEDA and the GDPR consider disclosing application processing mechanisms, third-party recipients of personal information and a detailed explanation of how the information is processed as necessary elements. Most application users might have never read a privacy policy, and it might be difficult for them to know if they are consenting to the use of their personal information to an ethical company.

Ethics in this context are difficult to measure, but the GDPR and PIPEDA prescribe the acceptable behavior for organizations that process personal information. Some companies might try to find legal loopholes to use their users' personal information as they find convenient or expedient and might meet the minimum legal requirements to keep operating under the disguise of compliance. The questionable ethics of some organizations does not discount the fact that the GDPR and PIPEDA have been greatly beneficial for human rights and have provided guidance for companies to act ethically. But the question remains: Who is ultimately responsible for the protection of their personal information: the users, the law, or the companies behind these applications?

Conclusion

Applications like Flo offer users convenience; but such convenience comes with a price — the collection, use, and the possible disclosure of personal information to unknown third parties. Through the GDPR, the EU pushed for the importance of protecting human rights specifically regarding their privacy and hence personal information, and countries such as Canada have enacted substantially similar laws. There is no doubt that these laws play a crucial role in safeguarding human rights, particularly in protecting personal information. They provide essential guidelines for companies on how to manage and handle user information responsibly.

Privacy policies should not be the sole metric to be used to determine if an application is ethical but are a solid place to start. Over the last decade several cases against companies have risen from their unfair use of their users' information, such as those mentioned in this article. Such attention has spurred many organizations to improve their practices, as reflected in the extensive changes Flo has made to its privacy policy and how they now handle personal information. Nevertheless, the ambiguity in its privacy policy is difficult to disregard, and questions might arise regarding how exactly the personal and sensitive information shared with (and by) the application is used, and what benefits they might gain from not disclosing this. These questions can be impossible to answer without internal company information and further research.

On the other hand, it is commendable that Flo has contributed to meaningful research for the often-unexplored field of women´s health, which findings are usually published on its website alongside a link to the academic paper. Given the concerns about consent, however, it might not be correct to assume that because findings are published in medical academic journals, that consent for the use of such information was given informed, specific, unambiguous, and freely as required by PIPEDA and the GDPR.

Several other subjects that were not considered in this article might warrant further discussion, such as the analysis of the cookies used, hidden Meta pixels, and the reliance on ISO certification.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Priveé
Suite 330 • Unit 440 • 10816 Macleod Trail SE
Calgary • Alberta • Canada • T2J 5N8