

# SMARTPHONE APPS BEWARE - BABYLON HEALTH INVESTIGATION PROVIDES INSIGHT INTO COMPLIANCE WITH ALBERTA PRIVACY LAWS

Posted on December 15, 2021

**Categories:** [Insights](#), [Publications](#)

This summer, Alberta's Office of the Information and Privacy Commissioner ("**OIPC**") released an investigation report on Babylon Health, a telehealth and virtual healthcare provider operating in Alberta ("**Babylon**"). The report provides a number of findings and recommendations that provide insights on best approaches to drafting privacy policies and serves as a reminder to organizations to only collect the minimum information necessary to achieve their purposes.

The OIPC divided its investigation into two parts: (i) Babylon's compliance with the *Health Information Act*<sup>[1]</sup> ("**HIA**")<sup>[2]</sup> with respect to individually identifiable health information, and (ii) Babylon's compliance with the *Personal Information Protection Act*<sup>[3]</sup> ("**PIPA**")<sup>[4]</sup>, which applies to Babylon's non-medical digital healthcare tools and virtual consultations with dietitians and mental health care counsellors (the "**PIPA investigation**"). This bulletin will focus on the PIPA investigation, as that statute is more widely applicable to private sector organizations and businesses.

## Key Findings

The OIPC reviewed all instances in which Babylon collected personal information, and its purported reasons for doing so. While the OIPC found that Babylon's collection was reasonable in most instances, there were several areas in which Babylon's collection and use of personal information was determined to be overbroad. For example,

- Babylon collected date of birth from users of its "symptom-checker" application to more accurately assess users' health symptoms. The OIPC noted that date of birth was more specific than necessary, since Babylon could have simply asked for a user's age to achieve the same purposes.<sup>[5]</sup>
- Babylon also asked users to provide a picture of their government-issued identification and a selfie photograph to confirm identity for fraud detection purposes. Babylon then used facial recognition technology to confirm a match. The OIPC found this was unnecessary because medical professionals already confirmed identity in other ways when providing care to individuals, and unreasonable because

- the information would be collected even if the individual subsequently cancelled the appointment.<sup>[6]</sup>
- Babylon collected and disclosed personal information for “quality improvement purposes” but it was unable to specify further what information was collected, and why it was necessary for these purposes, despite claiming it was critical to its operations.<sup>[7]</sup>
  - In addition, the OIPC found Babylon’s method of bringing its privacy terms to users’ attention was ineffective. Babylon provided users with a link to its terms and conditions and privacy policy when they first opened the smartphone app. However, the OIPC found that since these documents were lengthy (14-15 pages for terms and conditions and seven pages for privacy policy) and users generally accessed these documents on their smartphones, it was unlikely that users would have fully read them. Therefore, it was unlikely that users would have a reasonable understanding of the purposes for collection of their personal information, particularly those purposes that were not obvious, such as marketing and data analytics.<sup>[8]</sup>

The OIPC also identified other issues with Babylon’s privacy policy. In particular, the policy was complicated and self-contradictory, failed to indicate what information was used for given purposes, and lacked statutorily required notices for use of service providers outside of Canada.<sup>[9]</sup> Moreover, the OIPC found the app should have provided users with the ability to disable or prevent collection of certain information, such as precise location information.<sup>[10]</sup> The shortcomings of the privacy policy, together with the collection of information that was beyond what was reasonable, led the OIPC to conclude that Babylon did not have sufficient consent to use much of the information it collected.<sup>[11]</sup>

### **Takeaways for Businesses – What Lessons Can be Learned from the Report?**

- **Collection, Use and Disclosure.** The PIPA investigation provides a useful survey of the sorts of information that the OIPC considers reasonable to collect for common purposes such as marketing, fraud detection, technical support services, or processing payments. It also reveals certain instances where the OIPC considers the line to be crossed. In particular, organizations should review their collection practices and consider whether there is any less minimally intrusive way of achieving their purposes.
- **Privacy Policies must be Accessible.** The investigation report is a good reminder to any business that information on the business’s practices with respect to privacy of personal information must be provided in an accessible manner. Smartphone apps in particular need to be creative about how to provide information in a concise fashion, taking into account the way in which individuals are interacting with the app and accessing their policies.
- **Privacy Policies must be Clear and Current.** It is important for companies to remember that their privacy policies must be clear, well drafted and current. Policies must explain the jurisdiction(s) in which

business is being conducted, and accurately inform the individual of what personal information the company is collecting and the purpose(s) for which the information is collected. It is important to note that privacy policies must conform to actual practices and operations. If policies are too narrow, they will fail to obtain sufficient consent. If they are too broad, they risk a finding that the policy was fundamentally misleading, in which case consent will be invalidated.<sup>[12]</sup>

If you have any questions about the Babylon investigations, or would like your privacy policy reviewed by a privacy expert, a member of our Privacy and Cybersecurity group would be happy to assist you.

[1] *Health Information Act*, [RSA 2000, c H-5](#).

[2] [H2021-IR-01: Investigation into the use of Babylon by TELUS Health by Alberta physicians](#)

[3] *Personal Information Protection Act*, [SA 2003, c P-6.5](#). [**Alberta PIPA**]

[4] [P2021-IR-02: Investigation into Babylon by TELUS Health's compliance with Alberta's \*Personal Information Protection Act\*](#) [**Babylon PIPA Investigation**]

[5] *Babylon PIPA Investigation*, para 94-100.

[6] *Babylon PIPA Investigation*, paras 109 and 115.

[7] *Babylon PIPA Investigation*, para 159.

[8] *Babylon PIPA Investigation*, para 175.

[9] *Alberta PIPA*, [s. 13.1](#).

[10] *Babylon PIPA Investigation*, para 128.

[11] *Babylon PIPA Investigation*, paras 258-262.

[12] *Babylon PIPA Investigation*, para 194; see also for example, [PIPEDA Report of Findings #2019-002](#).

by [Julia Loney](#) and [Robbie Grant](#)

#### **A Cautionary Note**

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2021