Editor's Note:
Privacy Final Recommendation V1.0 Public Review

Pan-Canadian Trust Framework

October 29th, 2021
Version 1.0

1 Overview

This document provides a summary of comments received during the alpha testing of Version 1.0 of the Pan-Canadian Trust Framework PCTF Privacy Component, which closed May 15, 2021. The alpha testing was based on the Privacy Component Overview V1.0 and Privacy Conformance Profile V1.0 Final Recommendations documents.

Alpha testing is a process that is used to validate that the PCTF will perform as expected and meet the needs of public and private sector stakeholders. The goals for the alpha testing:

- Verify that the PCTF will perform as expected
- Ensure the PCTF is prepared for the PCTF Trustmark Assurance Program

The alpha testing for the Privacy component was carried out by a mix of 12 Canadian public and private sector DIACC member organizations, who volunteered to take part in the alpha test and applied the component criteria against one or more of their digital identity solutions or services.

The majority of the feedback from the alpha testing was general feedback on the PCTF Privacy Conformance Profile, commenting on the overall component (12) or subsets of criteria (40), with a limited number (5) of comments on specific criteria. Very few editorial comments were received.

2 Major Themes

The Editorial Team noted the following themes:

Outcomes-based Approach

- Within the general feedback, several reviewers proposed an outcomes-based framework that aligns with Canadian privacy law and suggested 43 revised outcome-based criteria.
- The proposed framework was not adopted as a whole for this revision. The Privacy Design team opted for a compromise -- retain the same structure of the Profile based on PIPEDA but refine the criteria to focus on the outcome identified in each Principle.
- The Privacy criteria were reviewed and updated to ensure each directly related to the outcome identified in the associated PIPEDA Principle.
- The revised criteria proposed by reviewers were considered and incorporated as much as possible with the existing criteria.

Broader View of Privacy

- Reviewers questioned why the PCTF Privacy does not consider a broader range of Privacy frameworks (e.g., GDPR, the Privacy Act), as well as the forthcoming, modernized PIPEDA.
- Current structure based strictly on PIPEDA Principles does not lend itself to updates as PIPEDA is reformed, and other Privacy regulations are incorporated. As well, there is overlap between Principles that leads to redundancies in the criteria.
- Reviewers noted that, as is, the Privacy component roles and takes a fairly restrictive view that may not apply to different business and operating models in the current market.
- Suggest better clarification on the roles, and particularly when one organization (or the User) performs multiple roles.
- The Privacy Design team recognizes the current format could be expanded or reworked to encompass broader set and/or updated of privacy frameworks. At this point the focus is on publishing a final 1.1 version approved for assessment use.
- As the PCTF components evolve, we expect subsequent releases of the PCTF Privacy Profile to be updated and incorporate privacy considerations from a broader set of Canadian focussed sources, and potential restructuring of the criteria.

Auditability

- A key reason for conducting an alpha testing review was to gain insight into how these criteria would be applied for real-world solutions and services.
- As part of the feedback resolution process, each Privacy criteria was evaluated strictly from an auditability perspective. Auditability has been defined for this purpose as follows:

Conformance criteria must be defined with sufficient precision and objectivity so that auditors are able to examine appropriate evidence and provide a reasonable assurance on the adequacy and effectiveness of the controls and processes established by the auditee to comply with the criteria.

- The Privacy criteria were updated and reworded to be auditable. For example, all instances of “have confidence” were replaced with outcome-based terminology such as “have policies” or “have documentation that”.

Governing Body Role and Criteria

- The Privacy Design Team sought guidance from TFEC on whether conformance criteria for the Governing Body belong in the Privacy component, or should be relocated to a different component. While some were specific to Privacy, many would apply to some or all of the PCTF components (e.g. investigate deviations from compliance).
- As well, reviewers noted that some criteria for Governing Body overstep their primary function of monitoring framework to stipulate regulatory-type powers.
- For this release, it was decided to keep the Governing Body criteria as part of the Privacy component. They are valid, have been reviewed, and assessed for auditability – we do not want to lose them.
- In the next major release of the PCTF, consider a separate component for Governance and have a broader review of Governance in the context of all the components, not just Privacy.

Editorial Comments

- Simplify wherever possible and be concise; use consistent wording if the intent is the same.
- To that end, criteria that were the same for multiple roles were combined into single criteria applicable to all.
- Several potentially redundant criteria were identified; these were reviewed and merged where it was clear the intent was similar; or reworded to clarify the differences.

3 Other Items

Although not explicitly identified in the alpha testing feedback, while reviewing and considering updates, the Privacy Design team did cross-reference with the PCTF Notice and Consent component, to ensure consistency.

As noted in earlier iterations, there remains a need to rationalize the PCTF Privacy component with the PCTF Notice and Consent component. For example:

- Significant overlap in the Principle 3 – Consent in the Privacy component and the Notification and Consent sections of the PCTF Notice and Consent component
- For this release, added cross-references from the Privacy component to the more detailed requirements in the PCTF Notice and Consent component, and checked for consistency between the components
- For next major release, recommend checking for redundancies and improving alignment across both, or all, components. As well, recommend considering a Governance Profile and adjusting component criteria in the Profiles accordingly.