

December 4, 2018

## Privacy Impact Assessment

### Gathering Residents to Improve Technology (GRIT Toronto) Testing by Code for Canada

#### BACKGROUND

Code for Canada is a national non-profit organization that, through its programs, enables governments to deliver better digital public services. One of Code for Canada's programs is called Gathering Residents to Improve Technology (GRIT Toronto). The GRIT program is designed to help test technology with its potential users in order to diagnose usability issues and, ultimately, find solutions that will improve the technology.

To this end, Code for Canada will be testing technology through a series of testing sessions to be held in public places such as libraries and community centres. It is anticipated that most tests will be conducted in-person, with one proctor guiding the participant through a series of evaluation questions and scenarios in order to identify usability issues.

#### RECRUITING TEST PARTICIPANTS

Test participants will be recruited as follows:

1. **Sign-ups:** As part of an initial incentive, those who sign up to be test participants will choose to receive \$5 in either a Visa gift card in the mail, or an Interac e-transfer. Participants will need to fill out a brief form via the program website that asks for their contact information and some other personal information (discussed in greater detail below).

Note: People can sign up on their own devices whenever they want, or they will be able to sign up on a Code for Canada device at an event. The form will be the same.

2. **Text message verification:** In order to mitigate abuse around sign-ups, after submitting the form, the person will receive a text message to verify the sign-up.
3. **Broad call-out email:** To all participants giving them a general purpose of the test, the test date and any specific requirements of the test. This email links to a screening form that participants must fill out if they want to be considered for the test.
4. **Screening form:** Asking testers about their availability during a [three]-hour time period on the test date, and some test-specific questions. For example:
  - o Do you have a child/children that attend a Toronto public school? (yes or no)
  - o How often do you visit your child/children's school's website? (multiple choice)
5. **Scheduling email:** To participants who pass the screening phase. An email discussing the specifics of the test, including location and test type, and asking them to confirm their availability, along with a preferred [45]-minute slot in the context of the entire test period.
6. **Rejection email:** Emails to the set of people who did not get segmented into the test.

7. **Confirmation email:** Once they've picked a slot, a confirmation email will follow with all of the test info.
8. **Reminder email:** Sent the day before the test to remind participants of the upcoming test, including time, location and any other relevant details.
9. **Consent form:** Immediately before the test is conducted, testers will be obligated to read and sign a consent form.

Note: the consent form will also be sent via email a few days before the test so testers have ample time to read through it.

10. **Test documentation:** A test proctor and notetaker will be present during the test to capture written details of the participant's actions as well as any pertinent qualitative information (i.e, does the participant seem frustrated or confident while navigating the website?) Notes will either be taken by hand and then transcribed into a Google spreadsheets via a Code for Canada computer or tablet, or notes will be entered directly into Google spreadsheets. Before the test begins, the test proctors will be reminded not to make any copies of files or data.

Other forms of documentation will be considered, including:

- Video (live stream or recorded only)
- Photos
- Some photos will be used in blog posts and/or social media as part of shared learning or program promotion

11. **Test observation:** One or more members of the client team will be invited to be present for the test in order to observe the session, add to qualitative data, ask follow up questions or answer questions.
12. **Key findings published:** Key findings from test sessions will be published in an aggregated, anonymized manner.
13. **Raw data release to client:** With the exception of photos/videos, all of the notes that were taken during the test, will be released to the client after the test in an aggregated, anonymized manner.
14. **Final report for the client:** A final report, with key recommendations on improving the client's technology, will be issued once the raw data has been synthesized. A breakdown of participating testers' demographics, without revealing their personal information, will be provided to the client.
15. **Public report/blog post:** In the interest of shared learning and transparency, Code for Canada desires to share key findings from each test on a public forum, such as a blog. The key findings will centre on the actionable items that Code for Canada would recommend the client take in order to improve their technology. The public report/blog post will include the testing methodology that was used, general findings and other useful observations as well. The general findings from test sessions will be published in an aggregated, anonymized manner.

16. **Participant profile building:** In order to help prioritize who should participate in future tests, Code for Canada will collect the following data that will constitute profiles for each participant in GRIT, in much the same fashion as a Customer Relationship Management (CRM) strategy:
- information about Code for Canada's interaction with test participants (email openings and responses)
  - responses to Code for Canada's screeners (including additional demographic data that test participants offered)
  - test participation (which tests participants did, whether they showed up for the test, whether their feedback was useful)
  - proctor notes that are relevant in order to assess reliability.

These profiles will never be shared.

In exchange for their input, participants will receive compensation in the form of Visa gift cards, Interac e-transfer payments or similar forms of compensation, upon test completion.

#### Tools Used

In organizing and conducting the GRIT testing, Code for Canada anticipates to leverage the following tools:

- Mailchimp or equivalent tool - to communicate with testers
- Wufoo or Typeform or equivalent tool – for registration and screening forms
- Google Docs and Sheets or equivalent tools - to organize the written raw data and create a final report, password-protected
- Google Drive or equivalent tool - to store any photos or videos
- Medium or equivalent tool - to post blog content

#### **ANALYSIS**

##### Privacy Protection in Canada

Privacy protection under Canadian law takes the form of regulation of the collection, use, disclosure, safeguarding, retention and disposal of personal information. Underpinning privacy protection in Canada are the following fair information principles:

**Accountability** - An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

**Identifying Purposes** -The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.

**Consent** - The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

**Limiting Collection** - The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

**Limiting Use, Disclosure, and Retention** - Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

**Accuracy** - Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

**Safeguards** - Personal information must be protected by appropriate security relative to the sensitivity of the information.

**Openness** - An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

**Individual Access** - Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

**Challenging Compliance** - An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

#### Personal Information

"Personal information" is defined in various Canadian privacy statutes as "information about an identifiable individual." Existing jurisprudence has further clarified that "information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."<sup>1</sup>

Pursuant to documentation provided by Code for Canada for the purposes of this assessment, the following information will be collected in the context of the GRIT program:

##### CONTACT INFO:

- First name
- Last name
- Email
- Phone number (if we do text message verification)
- Address
- Postal code

##### DEMOGRAPHICS

- Age (multiple choice)
- Education level (multiple choice)
- Tech skills level (multiple choice)
- Household income range (multiple choice)
- Gender identity (checklist)
- Ethnicity (checklist)
- Preferred language (multiple choice)
- Newcomer or immigrant status (multiple choice)

---

<sup>1</sup> See, for example, *Gordon v. Canada (Health)*, 2008 FC 258 at para. 34.

- Disability status (checklist)

Some of this information such as, for example, full name, email or physical address, may constitute “personal information” on their own. The balance of the above information items will fall within the definition of “personal information” when combined with the name and contact information as it would serve to further identify an individual and provide specific details about them.

#### Compliance with Fair Information Principles

Given that the GRIT program will require personal information, in collecting and handling this information, Code for Canada should strive to adhere to the above-noted fair information principles.

#### **Accountability**

According to the Code for Canada *Privacy Policy* available on its website, there is contact information that can be used to raise any data related issues or concerns. In addition, the draft Consent Form provides the name and contact information for a Code for Canada official for any GRIT Program-related questions. Code for Canada will appoint a designated individual within the organization to be responsible for privacy.

*It is **recommended** that Code for Canada provides contact information for privacy related questions within all of its correspondence with the test participants, including on the consent form to be discussed in greater detail below.*

The accountability principle also requires Code for Canada to remain accountable throughout the entire life cycle of the personal information it is processing. This includes: processes to monitor and demonstrate compliance with the privacy program, and training for all team members who will handle personal information and/or interact with users.

As such, it is incumbent that due diligence be done with respect to the tools/contractors being used.

*It is **recommended** that Code for Canada review the terms of service for each of its tools/contractors to ensure that adequate provisions are in place to protect personal information throughout the project. This should include an ability to return or destroy the personal information that will be provided to these tools/contractors.*

#### **Identifying Purposes**

Pursuant to documentation provided by Code for Canada for the purposes of this assessment, Code for Canada intends to provide the test participants with a consent form both via email a few days before the test so testers have ample time to read through it, and on the day of the test immediately before the test for their additional review and signature.

This consent form will identify what information will be collected, the methods of collection, how it will be used and shared, where applicable. In addition, pre-test correspondence sent to test participants will equally provide this information.

#### **Consent**

See the *Identifying Purposes* section immediately above.

In addition, Code for Canada intends to leverage third party tools for various aspects of the GRIT program, as explained elsewhere in this document. It is assumed that Code for Canada's use of those tools is governed by the standard Terms and Conditions or similar terms for the public use of those tools. In other words, it is assumed that Code for Canada has not entered into any specific contracts with the relevant tools and have not negotiated any specific terms and conditions upon which it will be using the relevant tool, including privacy protection requirements.

*As such, it is **recommended** that Code for Canada clearly explains to the test users what tools and for what purposes it will use and advise the test users that those tools may be collecting their personal information and that the collection will be subject to those tools' privacy policies and provide the links to those privacy policies. Code for Canada might wish to provide this information at different touch points throughout the GRIT program starting with the broad call out email to be sent to all participants.*

### **Limiting Collection**

*It is **recommended** that Code for Canada ensure that it only collects information that is demonstrably necessary for the stated purposes of the GRIT program.*

### **Limiting Use, Disclosure, and Retention**

*It is **recommended** Code for Canada ensure that it uses information that qualifies as personal only where it is demonstrably necessary to achieve the stated purposes of the GRIT program.*

- *For example, Code for Canada requires a test participant's email address in order to communicate to them the details of the GRIT program, schedule their participation, etc. Therefore, the email address information should only be used for these purposes and promptly and securely disposed of once it has served its purpose.*

*In the same vein, Code for Canada may require personal information in order to conduct the test and obtain required evidence. However, it is **recommend** that, in sharing the test results with its client and/or publicly, Code for Canada be cautious to only do so by using aggregate, anonymized data.*

- *For example, Code for Canada may wish to develop personas or profiles based on common socio-economic characteristics of the test participants for the purposes of synthesising and presenting the results of its test. For example, a persona may be a combination of sex, age range, education/professional status, falling within a certain income range and exhibiting certain response to the test technology.*

*It is **recommended** that, once the test results have been processed and packaged in this manner, unless there is any other compelling reason for keeping the personal information of the test participants, such be securely disposed of.*

### **Accuracy**

Given that the personal information will be collected directly from the impacted individuals that is, test participants, there are no concerns about the accuracy of the information.

### **Safeguards**

As long as Code for Canada retains the collected personal information, it must ensure that such is adequately protected from the risk of unauthorized use and/or disclosure.

*To this end, it is **recommended** that Code for Canada clearly define the circle of internal stakeholders who require access to the involved personal information. Further, access to both electronic and physical personal information should only be provided to such stakeholders through the implementation of physical safeguards (locked storage cabinets, restricted access to certain areas housing physical and/or electronic personal information, etc.) and electronic safeguards (e.g., encryption, password-based access, etc.), as required. Further, to the extent that personal information exists in electronic form, such should be encrypted both at rest and in transit. Again, once the personal information has served its stated purpose, it must be securely and irrevocably disposed of.*

### **Openness**

See the *Accountability, Identifying Purposes, and Consent* sections above.

### **Individual Access**

See the *Accountability* section above.

### **Challenging Compliance**

See the *Accountability* section above.

### Consent Form

Code for Canada provided a draft consent form for the purposes of this assessment.

### Tester Withdrawal

*If a tester decides to withdraw from the GRIT program, irrespective of the stage of the testing, it is **recommended** that any personally identifiable information about the tester collected up to that point not be used for any purposes and be securely and irrevocably disposed of.*