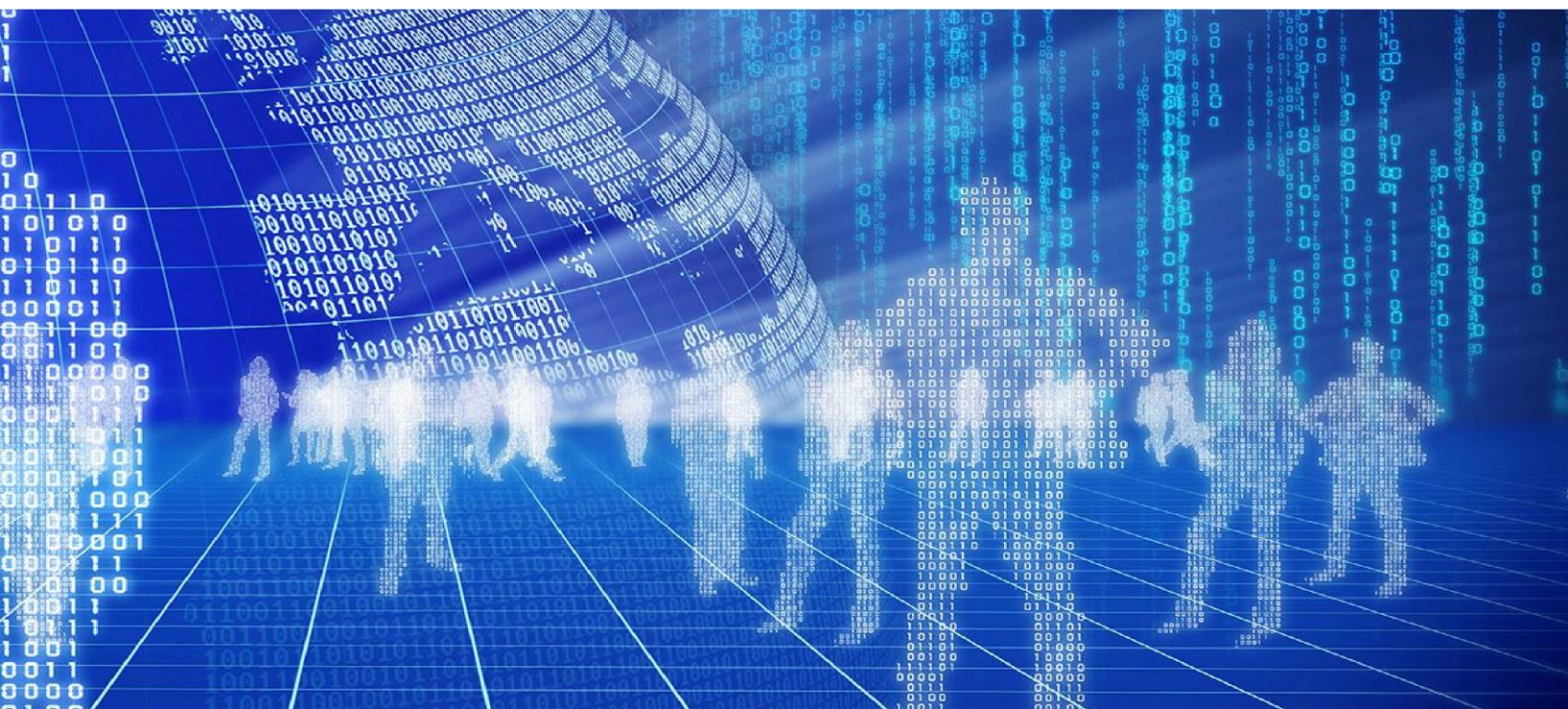


# A Path to Trustworthy People Beneficial Data Activities

A Report prepared for Innovation, Science and Economic  
Development Canada

March 2020





## **Executive Summary**

The Canadian Ministry of Innovation, Science and Economic Development (ISED) and the Information Accountability Foundation (IAF) have a mutual interest in exploring how the concept of People Beneficial Data Activities might be developed in a new privacy law or in revisions to the existing privacy law, The Personal Information Protection and Electronic Documents Act (PIPEDA), in order to further balance the full range of Canadians' interests in how personal data are used and to support Canada's digital strategy<sup>1</sup>. As a result, the IAF conducted a multi-stakeholder process to assist in developing the concept of People Beneficial Data Activities as a form of demonstrable accountability. The results of this multi-stakeholder process are set forth in this Report and Recommendations to ISED.

In 2017 the Office of the Privacy Commissioner (OPC) recommended amending PIPEDA to allow for socially beneficial activities that the PIPEDA drafters did not envisage where consent is not feasible. In 2020 the OPC made this recommendation again. As the term suggests, the OPC limits socially beneficial activities to those that benefit society. People Beneficial Data Activities are those that promote and enhance the well-being of individuals, groups of individuals, society, and organizations. The goal of Canada's digital strategy is for Canadians to benefit from the opportunities that the digital economy offers while at the same time protecting them from the threats posed by the embrace of digital technologies, including threats to the safety of personal data and to individual privacy. To achieve this goal, data that pertain to people will need to be processed and governed according to a set of common rules that consider the interests of all stakeholders and that meet the threshold of "people beneficial." This governance approach must go beyond a confrontational approach based on the assumptions that organizations want to process data and that people do not want that data processed to an uncontentious approach where all share an interest in data being processed in a demonstrably accountable manner.

To achieve the robust processing called for by the digital technology ecosystem, Canadians must be able to trust that their privacy is protected and that their personal data will not be misused but rather used in a manner that creates benefits for people. In order for this trustworthy relationship to exist between Canadians and organizations that process personal data, IAF proposes it is necessary to have a method for determining: (i) what data activities are people beneficial, and (ii) what accountable process will be required to identify and reduce the risks associated with People Beneficial Data Activities.

People Beneficial Data Activities are those that promote and enhance the well-being of individuals, groups of individuals, society, and organizations and are distinct from organizational data activities that are currently managed under existing authorities to process personal data.

---

<sup>1</sup> See [https://www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00109.html](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html)

- People Beneficial Data Activities might include, for example, greater access to health care, better or lower cost health care, improved education, and environmental enhancements such as water conservation and energy cost reduction.

- 
- “Benefit” means a material, objective and identifiable positive effect or advantageous outcome accruing to individuals, groups of individuals, society and institutions as a result of the processing of personal data and is separate and distinct from any positive outcome, advantageous impact or value that accrues to the organization or to a single person or individual.

A demonstrable accountable process, that includes managing digital risk, is the Common Reference Privacy Framework. The components of this Framework are the requirements that organizations should:

- Designate senior officers who are accountable for People Beneficial Data Activities
- Conduct People Beneficial Impact Assessments (PBIAs)
- Achieve an enhanced standard of transparency covering People Beneficial Data Activities and their associated governance processes
- Have specific internal oversight
- Be subject to independent external oversight
- Keep records of People Beneficial Data Activities
- Protect individual rights and implement transparent redress systems

People Beneficial Data Activities place the responsibility of protecting individuals on the organization, which is in the most practical position to undertake a benefit/detriment analysis and to devise appropriate mitigations. The interests to be considered in this balancing process include the interests of individuals, groups of individuals, society, the organization and, in some cases, other organizations. This accountability process is not a self-regulatory scheme because it is subject to both independent internal oversight and external oversight by a regulator who has the authority to proactively inspect the practices of the organization.

To engage in People Beneficial Data Activities, organizations will need to have a Privacy Impact Assessment (PIA) process. If organizations do not have PIA processes already, they will need to develop PIAs or the PBIAs will need to incorporate the elements of a PIA into the PBIA.

### **Recommendations**

- Explicitly recognize People Beneficial Data Activities as serving a legitimate purpose because on balance the activities are beneficial to people when the risks to people are reduced to an acceptable level. Limiting People Beneficial Data Activities to those provided within the “conditions of the supply of a product or service” might contribute to personal data not being used for people beneficial purposes.

- Explicitly move beyond consent as the primary authority to process personal information for People Beneficial Data Activities where consent is not fully effective.
- Explicitly recognize People Beneficial Data Activities as a new or expanded authority to process personal information beyond reliance on the concepts of consent and legitimate purposes tied to the provision of products and services. This recognition would lessen reticence risk (i.e. a reduction of any inhibition to data driven innovation) and would provide more benefits to stakeholders because these activities have not been limited to those provided within the “condition of the supply of a product or service,” as long as the People Beneficial Data Activities meets all the elements of demonstrable accountability and are aligned with the objectives, culture, and values of the organization.
- Expressly provide a method for determining what data activities are people beneficial and provide clarity regarding this processing through public policy. This express provision will reduce reticence risk to people, society and organizations and help to implement Canada’s Digital Charter while protecting the privacy of Canadians.
- So that People Beneficial Data Activities are transparent, expressly provide in policy requirements the elements of demonstrable accountability: be accountable, conduct a people beneficial data impact assessment (PBIA), be transparent, have internal oversight, be subject to independent external oversight, keep records, and protect individual rights.

### **Next Steps**

Without independent external oversight, demonstrable oversight will be less successful. Regulators may not accept that organizations have acted with integrity and in good faith, and organizations may not be able to use data for People Beneficial Data Activities. What this independent external oversight consists of and how this external oversight is conducted is beyond the scope of this Report and Recommendations. But this Report and Recommendations recognizes that such oversight is necessary for People Beneficial Data Activities to be an independent authority for processing personal information. IAF suggests what that enforcement and oversight should entail and how that enforcement and oversight should be conducted are topics appropriate for another multi-stakeholder process.

### **Background**

ISED and IAF have mutual interests in exploring how the concept of People Beneficial Data Activities might be developed in a new privacy law or in revisions to the existing privacy law, PIPEDA, in order to further balance the full range of Canadians’ interests in how personal data are used. This exploration included consideration of: (i) how public policy might define People Beneficial Data Activities as an additional or an expanded authority to process personal information beyond reliance on the concepts of consent and legitimate purposes tied to the

provision of products and services,<sup>2</sup> and (ii) what parameters would need to be demonstrated in order to use this new or expanded authority to process personal information. People Beneficial Data Activities are those that promote and enhance the well-being of individuals, groups of individuals, society, and organizations. Depending on the activities, they may be

---

distinct from organizational data activities that are currently managed under the existing authorities to process personal information.

IAF's research also has been supported and informed by Canadian businesses who brought their insights to this initiative. Furthermore, the concepts and processes expressed and described in this Report and Recommendation were evaluated in a multi-stakeholder meeting on December 3, 2019 in Toronto. The draft of this Report and Recommendation was revised based upon feedback received at the multi-stakeholder session.<sup>3</sup> Depending on the nature of the comment, most often the feedback is incorporated directly into the revision and is not expressly noted, but sometimes the feedback is commented upon and so has been paraphrased. This Report and Recommendation is the responsibility of the IAF research team, and the IAF thanks all funders and participants. This Report and Recommendation does not necessarily reflect the views of the Canadian government, multi-stakeholder participants or the IAF board of trustees and funders.

### **Generally: The Problem People Beneficial Data Activities Addresses**

It is anticipated that the pace of adoption of technologies, such as the Internet of Things and Artificial Intelligence (AI), fed by observation and decision-making being built into how things work continually, will increase. For this broad application of technology enabled data activities to be accepted, Canadians must have high confidence that their rights and interests in both protection and improved circumstances are protected by law and demonstrable practices. For this level of confidence to be achieved, concepts, such as trustworthy people beneficial processing, need to evolve and provide for the processes and controls that will be the authorizing mechanisms for the collection, disclosure or use (processing) of personal information. For the more robust processing called for by a digital technology ecosystem to be trusted, it is necessary to have a method for determining and demonstrating which data activities are people beneficial and what accountable process will be required to identify and reduce the risks associated with People Beneficial Data Activities. Without the clarity of accepted trustworthy processes that authorize People Beneficial Data Activities, reticence risk (i.e. the risk that organizations may not engage in data activities that are people beneficial) may

---

<sup>2</sup> Sections 3 and 5(3) of and Principles 1 and 3 of Schedule 1 to PIPEDA, S.C. 2000, c. 5; Towards Privacy by Design: Review of The Personal Information Protection and Electronic Documents Act, at 19 (testimony of Adam Kardash), <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>.

<sup>3</sup> See Appendix 1 for Participating Contributors

occur and increase because the lack of clarity creates the perception that the risks are too high. Expressly providing a method for determining that data activities are people beneficial and providing clarity of this processing through public policy will reduce reticence risk and thereby help to implement Canada’s Digital Charter while protecting the privacy of Canadians.<sup>4</sup>

---

Today, an organization may process personal information in the course of its commercial activities if it has the authority to do so by relying on consent or one of the exceptions to consent. The appropriate form of valid consent, whether implied or express, varies depending on the sensitivity of the personal information and the circumstances of the processing.<sup>5</sup> In all cases, the purposes for processing personal information must be reasonable in the circumstances. An organization can process personal information for legitimate purposes based on implied consent as a condition of the supply of a product or service.<sup>6</sup> Well understood examples of such legitimate purposes include business innovation, such as operational efficiency, service improvements, product and service development, understanding customers better and increasingly for People Beneficial Data Activities related to the organization’s business. The authority for an organization to process personal information for purposes that are people beneficial are limited to those that are within the “condition of the supply of the product or service.”<sup>7</sup> In the future, therefore, because there will be increasing opportunities to advance more and broader People Beneficial Data Activities outside of these limitations, to maximize these opportunities, an explicit recognition of such broader People Beneficial Data Activities as the authority to process personal information beyond the existing concepts of consent and legitimate purposes will be needed.

People Beneficial Data Activities could be an exception to consent, but that would not be optimal. Advances in technology and the use of lengthy, legalistic privacy policies too often have made the control – and personal autonomy – that should be enabled by consent nothing more than illusory. Consequently, several Canadian privacy and information commissioners set forth guiding principles for consent and reaffirmed that organizations must generally obtain express consent when the information being processed is sensitive, the processing is outside of

---

<sup>4</sup> Comments were made at the multi-stakeholder session that too much emphasis is being placed on reticence risk. It has been the experience of the IAF that reticence risk is real, and if the benefits of the digital economy are to be achieved, it is the view of the IAF that reticence risk needs to be recognized and evaluated. Another comment cautioned that the costs of not undertaking the data processing in question should be incorporated into the benefit and not the risk side of the equation so that double counting does not occur. This balancing occurs in the People Beneficial Impact Assessment (PBIA) discussed in The Components of the Common Reference Privacy Framework that Includes Managing Digital Risk section *infra*.

<sup>5</sup> Principles 4.3.1 and 4.3.6 of Schedule 1 to PIPEDA; Office of the Privacy Commissioner of Canada & the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, Guidelines for obtaining meaningful consent, 2018, [https://www.priv.gc.ca/en/privacy-topics/collecting-personalinformation/consent/gl\\_omc\\_201805/](https://www.priv.gc.ca/en/privacy-topics/collecting-personalinformation/consent/gl_omc_201805/) [hereinafter Consent Guidelines]

<sup>6</sup> Sections 3 and 5(3) of and Principle 4.3.3 of Schedule 1 to PIPEDA

<sup>7</sup> Section 4.3.3 of Schedule 1 to PIPEDA

the reasonable expectations of the individual and/or the processing creates a meaningful risk of significant harm.<sup>8</sup> Because it may be too hard to describe the processing and because the processing may be beyond the individual's expectation, the Consent Guidelines narrowed the form of and the method for obtaining consent. This narrowing may result in a reduction in the ability to process personal information. Moreover, given this narrowing of consent, having People Beneficial Data Activities be an exception to consent might result in the exception being broader than the general rule. If Canadian policymakers believe robust, people beneficial processing meets policy objectives, then another trustworthy mechanism to process personal information, People Beneficial Data Activities, is needed as an authority in addition to consent rather than an exception to consent. If People Beneficial Data Activities is an authority to

---

process personal information in addition to consent, then it was urged at the multi-stakeholder session that the independent oversight needs to be broader than is currently available for consent. The authority of People Beneficial Data Activities is not a form of self-regulation. Rather, enforcement and oversight agencies will need the ability to conduct spot checks to determine whether organizations are in compliance with their own internal processes.

### **Specifically: What the Problem is and How People Beneficial Data Activities Addresses It**

#### **Benefits of the Digital Economy to Canada**

Much as the printing press revolutionized society starting in the 15<sup>th</sup> century, the digital revolution has had, and will continue to have, an enormous impact upon Canadian economy and society and therefore on Canadians' daily life. Canada has the right ingredients to thrive in an increasingly digital world. It has a strong research capacity, a diverse and highly educated workforce, and a strong investment climate. Its people are tech savvy and well-connected with 87 percent of Canadians and 85 percent of Canadian businesses connected to the Internet. Eighty-eight percent of Canadians have a mobile device.<sup>9</sup>

Today, an ecosystem of interdependent digital technologies – consisting of the Internet of Things, emerging 5G networks, cloud computing, big data, AI, blockchain, and computing power - underpins digital transformation and will evolve to drive economic and societal changes.<sup>10</sup> Digital transformation progressively touches all sectors in the economy, but it does so with differing speeds and extents. Only one sector, information and communications technology

---

<sup>8</sup> Consent Guidelines. The seven guiding principles for meaningful consent are: (1) emphasize key elements, (2) allow individuals to control the level of detail they get and when, (3) provide individuals with clear options to say "yes" or "no," (4) be innovative and creative, (5) consider the consumer's perspective, (6) make consent a dynamic and ongoing process, and (7) be accountable: stand ready to demonstrate compliance.

<sup>9</sup> OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, Chapter 4, at 70, OECD Publishing, Paris, <https://doi.org/10.1787/9789264312012-en> [hereinafter *Going Digital: Shaping Policies, improving Lives*]

<sup>10</sup> Id.



(ICT) services, stands out as being the most digital intensive.<sup>11</sup> Digital adoption and embracing new technology-enabled business practices fuel productivity, economic growth and international competitiveness.<sup>12</sup>

Business, communications, entertainment, transportation, banking, education, health care, interpersonal transactions and physical movements – almost every aspect of individuals’ lives - interact with digital technology. With these interactions, enormous amounts of data about individuals are being created and harnessed for a vast array of purposes. More broadly, digital and data-driven technology is already empowering science, supporting innovation, and driving economic growth.

Data-driven innovation pushes out the frontier of what is possible, driving creation, productivity and sustainable growth and development. Digital innovation is a fundamental driver of digital transformation, leading to radical changes in the way individuals interact, create, produce and consume. Digital innovation not only gives rise to new and novel products and services, but it

---

also creates opportunities for new business models and markets, and it can drive efficiencies in the public sector and beyond. Digital technologies and data also drive innovation in a wide range of sectors, including education, health, finance, insurance, transportation, energy, agriculture, fisheries and manufacturing, as well as ICT.<sup>13</sup>

Based on these impacts, “benefit” means a material, objective and identifiable positive effect or advantageous outcome accruing to individuals, groups of individuals, society and organizations as a result of the processing of personal information. These effects and outcomes are separate and distinct from any positive outcome, advantageous impact or value that accrues to the organization and to a single person or individual. Canada’s plan is to grow its economy through the benefits of this innovation and build sustainable growth by leveraging digital and data transformation.<sup>14</sup>

### **A Common Reference Privacy Framework that Includes Managing Digital Risk is Needed**

Trustworthy processing is the lynchpin of the digital and data-driven economy. A strong foundation of trustworthy processing and transparency between individuals, organizations and

---

<sup>11</sup> OECD (2019) *Measuring the Digital Transformation: A Roadmap for the Future*, Chapter 1.2, at 45, OECD Publishing, Paris, <https://doi.org/10.1787/9789264311992-en>.

<sup>12</sup> Positioning Canada to Lead in a Digital- and Data-driven Economy: Discussion Paper, <https://www.ic.gc.ca/eic/site/084.nsf/eng/00007.html>

<sup>13</sup> *Going Digital: Shaping Policies, Improving Lives*, Chapter 4, at 70

<sup>14</sup> Canada’s Digital Charter in Action: A Plan by Canadians, for Canadians – Minister’s Message, [https://www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00109.html](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html); Canada’s Digital Charter: Trust in a Digital World, [https://www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00108.html](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html)

government will enable the digital economy.<sup>15</sup> Trustworthy processing is the foundation on which Canada's digital and data-driven economy is being built.<sup>16</sup>

The power and potential of digital technologies and data for individuals, society, and organizations depend on their effective use of the digital technology ecosystem by allowing data to be processed. One way to enable more sophisticated usage is to enhance trust in the digital environment. One way to do that, according to the Organisation for Economic Cooperation and Development (OECD), is to empower individuals, organizations and government to better manage digital risk.<sup>17</sup> The most important parts of this equation are the institutions that are actually using the data to create value. Data used in a thoughtful, responsible, transparent manner will enhance trust in digital processes. For this reason, the risk of organizations not using data to create value, reticence risk, is just as big a risk as organizations misusing data.

Trustworthy processing underpins most digital relationships, and a lack of trust in processing is an important barrier to effective use of the digital technology ecosystem by not allowing personal data to be processed.<sup>18</sup> Trust in digital environments depends on the context and varies with what is at stake, including opportunities and challenges. To fully embrace and benefit from digital transformation, individuals, society, and organizations need to be confident that engaging in the digital environment to conduct their social and economic activities will

---

bring more benefits than detriments. To achieve trustworthy processing, it is critical to mitigate, as much as possible, the detriments.<sup>17</sup>

In practice, the most effective way to deal with detriments is to manage digital risks to stakeholders. As risk is a cross-boundary, cross-sector and multi-stakeholder issue, digital risk management needs a common reference Framework. According to the OECD, the components of this Framework include:

- Establishing the objectives and the context of an activity and determining the acceptable level of risk in light of the expected benefits
- Assessing risk by identifying risk factors and evaluating the likelihood and severity of risk occurrence

---

<sup>15</sup> Canada's Digital Charter in Action: A Plan by Canadians, for Canadians

<sup>16</sup> Canada's Digital Charter: Trust in a Digital World, [https://www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00108.html](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html) <sup>17</sup> *Going Digital: Shaping Policies, Improving Lives*, Chapter 3, at 54. <sup>18</sup> *Id.* at 62.

<sup>17</sup> *Id.* Chapter 7, at 122

- Treating risk, including through accepting some, reducing it to an acceptable level through appropriate measures, sharing or transferring some, and/or avoiding some altogether
- Monitoring and reviewing on an ongoing basis the risk management cycle to adapt it to a constantly changing environment.<sup>18</sup>

Since the goal is to develop a strong, inclusive and interoperable privacy Framework that includes a risk management approach that achieves trustworthy processing,<sup>19</sup> this goal is just another way of saying that organizations should be accountable. “Done properly, [accountability] should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organizations.”<sup>20</sup> The development of a strong, inclusive and interoperable privacy Framework that includes a risk management approach achieves accountability.<sup>21</sup> This is because if done properly, accountability promotes trust and confidence on the part of individuals, thereby protecting the privacy rights of Canadians and enhancing the competitive and reputational advantages for organizations.<sup>22</sup> Privacy is key to achieving a strong, competitive economy and building a more inclusive, prosperous Canada.<sup>23</sup>

---

In addition to consent to process an individual’s personal information, PIPEDA<sup>24</sup> requires accountability, specifying that organizations are responsible for the personal information under their control.<sup>27</sup> An accountable organization must have in place appropriate policies and procedures that promote good practices which taken as a whole constitute a privacy

---

<sup>18</sup> Id. A question was raised at the multi-stakeholder session about whether the issue should be phrased in terms how to better protect the right of privacy rather than how to use data. It is not an either/or situation. Providing an additional authority to process personal data – People Beneficial Data Activities – upon compliance with a common reference privacy Framework addresses both issues.

<sup>19</sup> *Going Digital: Shaping Policies, Improving Lives*, Chapter 7, at 120-121.

<sup>20</sup> *Getting Accountability Right with a Privacy Management Program*, Office of the Information & Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information & Privacy Commissioner of British Columbia (Joint Accountability Guidance), [https://www.priv.gc.ca/media/2012/gl\\_acc\\_201204\\_e.pdf](https://www.priv.gc.ca/media/2012/gl_acc_201204_e.pdf).

<sup>21</sup> *Going Digital: Shaping Policies, Improving Lives*, Chapter 7, at 120-121.

<sup>22</sup> Joint Accountability Guidance

<sup>23</sup> Canada’s Digital Charter in Action: A Plan by Canadians, for Canadians – Minister’s Message

<sup>24</sup> PIPEDA is based on the internationally accepted principles contained in the OECD *Guidelines on the Protection of Privacy and Transborder Flows off Personal Data*. Strengthening Privacy for the Digital Age: Proposal to modernize PIPEDA, [https://www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00107.html](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html); Joint Accountability Guidance at 3.

<sup>27</sup> Principle 4.1 in Schedule 1 to PIPEDA.

management program.<sup>25</sup> Part of that program is a process for identifying and mitigating the privacy and security risks, including the use of PIAs and security threat risk assessments.<sup>29</sup> The Joint Accountability Guidance predates current OECD work and does not include benefits from data use in the explicit manner recommended by the OECD. Including management of digital risk from use and non-use of personal data, among other risks, as part of an organization's privacy management program, helps the organization determine whether data-driven activities should proceed and demonstrate how that determination was reached. Demonstration of how those conclusions were reached is an important part of accountability.

### **The Components of the Common Reference Privacy Framework that Includes Managing Digital Risk**

People Beneficial Data Activities as a new and expanded form of authority to process personal information are those that promote and enhance the well-being of individuals, groups of individuals, society, and organizations. The two-step base test to determine whether data activities are people beneficial, and therefore form the basis of an authority to process personal information, is:

- The data-driven activity must have a describable purpose and a benefit that accrues to "people" (plural). "Benefit" means a material, objective and identifiable positive effect or advantageous outcome accruing to individuals, groups of individuals, society and organizations as a result of the processing of personal information and must be separate and distinct from any positive outcome, advantageous impact or value that accrues to the organization and to a single person or individual. Because the benefit can be to society, the benefit from the data of a group of individuals does not have to benefit each and every individual within that group of individuals.
- Negative consequences or detriments, including the risk of not using personal data for People Beneficial Data Activities, must have been mitigated to a satisfactory and demonstrable level. Negative consequences or detriments that must be reduced include the likelihood of illegal disparate impact.

When this base test is used, in connection with the Framework below, People Beneficial Data Activities become an accountable basis for the processing of personal information for datadriven activities in many contexts. This authority results because People Beneficial Data Activities involve a trustworthy, rigorous assessment balancing the benefits and detriments for

---

individuals, groups of individuals, society and organizations. People Beneficial Data Activities place the responsibility of protecting individuals on the organization, which is in the most practical position to undertake a benefit/detriment analysis and to devise appropriate

---

<sup>25</sup> Joint Accountability Guidance at 1.

<sup>29</sup> Id. at 12.

mitigations.<sup>26</sup> The interests to be considered in the balancing process include the interests of individuals, groups of individuals, society, the organization and maybe even other organizations, which could include competitors.

Therefore, under this Framework, an organization should:

- **Be Accountable:** Designate one or more senior/executive employees who are responsible and accountable for the specific People Beneficial Data Activity from the time the organization considers engaging in the activity through the time the activity is conducted. At the multi-stakeholder session, it was suggested that the senior corporate officer be the accountable party. If this comment suggests the Chief Executive Officer is always accountable for People Beneficial Data Activities, the accountability requirement may be defeated. Accountability requires the involvement of a senior executive, but it is more effective if the senior executive is one within the immediate governance structure.
- **Conduct a PBIA:**<sup>31</sup> Conduct a PBIA, a form of risk assessment contemplated by the OECD. To engage in People Beneficial Data Activities, organizations will need to have PIAs, and if an organization does not have a PIA, it will need to develop a PIA, and the PBIA will need to incorporate the elements of a PIA into the PBIA. The PBIA must:
  - Establish the objectives and the context of a data-driven activity (i.e. define a precise problem and differentiate between activities that develop insights and activities that apply insights);
  - Determine all the stakeholders and the acceptable level of risk in light of the expected benefits for all stakeholders. Determining benefits and risks may necessitate the involvement of stakeholders such as consumer groups;
  - Assess risk by identifying risk factors and evaluate the likelihood and severity of risk occurrence. It may be necessary to get very granular about all benefits and all risks;
  - Treat and reduce risk to an acceptable level through appropriate measures, including architectural controls. This includes through sharing or transferring some risks and/or avoiding some risks altogether depending on the benefit to the groups of individuals and society;
  - Conduct PBIA's continually and repeatedly (e.g. at the initial posing of a question, to determine whether there are new insights, and after an initiative is underway); and

---

<sup>26</sup> Participants at the multi-stakeholder session cautioned that private organizations whose primary mandate is to make money are not equipped to make the value judgments necessarily required for this kind of analysis and that without a rigorous oversight mechanism in place the exercise of weighing costs and benefits to society should be undertaken by a public interest organization whose mandate does not place it in any conflict of interest. IAF agrees that rigorous oversight and enforcement are necessary for People Beneficial Data Activities to be an independent authority for processing personal data. <sup>31</sup> See Appendix 2 for a Model PBIA

- Monitor on an ongoing basis the content of the PBIA and keep it current. The PBIA must conclude that risks are at a low enough or nonexistent level so that they are counter-balanced by the benefits created for the individuals and/or society by the processing. An appendix to this Report and Recommendation is a Model PBIA that organizations can use, customize or expand.
- **Be Transparent:** Demonstrate transparency to the public, to employees and to the government. There are different audiences, and organizations should make sure they are reaching the right audience with the right communication method. For example, on the organization’s websites, organizations may disclose:
  - The types of People Beneficial Data Activities the organization engages in, how data are used to achieve each people beneficial purpose and the types of third parties to which personal data may be transferred in order to achieve each people beneficial purpose;
  - Descriptions of the governance processes it employs (e.g. policies and procedures) regarding People Beneficial Data Activities;
  - A description of the PBIA process, including identification of benefits to people, its conclusion why the organization’s interests are people beneficial, identification of processing risks and appropriate ways to reduce risk, analysis of residual risks, identification of risks from forbearing activity, and explanation of why the factors that support processing are not outweighed or counterbalanced by residual risks (this is meant to be a summary of the PBIA process and is not meant to include a summary PBIA for each People Beneficial Activity);
- **Have Internal Oversight:** Oversee the PBIA process consistent with the level of risk (e.g. if the People Beneficial Data Activity is high risk, then the organization may want to seek expert advice which may include external, in addition to internal, input from, for example, industry experts or members of the public). An organization can achieve this level of oversight by having in place a review board that is independent of the assessment process, that assesses the full range of internal and external interests, that expresses the voice of the community through focus groups and/or external experts, and that is transparent by having a structure and charter that is made public and by being ready to demonstrate its governance process.<sup>27</sup> This independent oversight program ascertains that the overall PBIA process is being conducted as intended and that the PBIA process is effective and conducted with integrity. This determination should use a commonly agreed upon format and should be based on a review of the organization’s internal systems, processes and activities, including how the organization has conducted specific PBIA’s. Internal oversight also needs to include a review of the

---

<sup>27</sup> This type of review board is more fully discussed in IAF’s Report for the Comprehensive Assessment Oversight Dialog: Canadian Ethical Data Review Boards Project, March 2018, <http://informationaccountability.org/wpcontent/uploads/Report-for-the-Comprehensive-Assessment-Oversight-Dialog-Canadian-Ethical-Data-ReviewBoards-Project.pdf>

overall PBIA accountability requirements and process. This internal oversight could be anchored with, for example, an Internal Audit group. The independent oversight

---

process should be part of the transparent description of the publicly available governance process;

- **Be Subject to Independent External Oversight:** Respond to external independent oversight of the organization's determination that an activity is people beneficial and which is subject to internally independent oversight. This accountability process also should be demonstrated to a regulator and therefore is not self-regulation. The regulator should have the authority to proactively inspect the practices of the organization.<sup>28</sup> However, if proactive inspection means spot audits, then organizations need procedural fairness/due process based upon administrative law principles.<sup>34</sup>
- **Keep Records:** Internally keep a detailed record of People Beneficial Data Activities that documents what happened and how all accountability requirements were met, and, in addition to the summary information provided on its website, annually externally report at an aggregate level the types of People Beneficial Data Activities in which the organization engaged (e.g. in the organization's annual report or sustainability report) or through a trade association annually on an aggregate industry level; and
- **Protect Individual Rights:** Create an accessible, transparent redress system so that individuals can complain to the organization about the processing of their own personal data. Once the organization receives such a complaint, the personal data referred to in the complaint will not be processed unless the organization can demonstrate compelling legitimate grounds for the processing of the individual's personal data which override the individual's interests.

All these organizational requirements that enhance trustworthiness of processing<sup>29</sup> could form the basis of a formal Code of Practice that could become guidance to organizations, especially small and medium sized businesses.<sup>30</sup> In addition, they could form the basis for some form or

---

<sup>28</sup> What more this independent external oversight consists of and how this external oversight is conducted is beyond the scope of this Report and Recommendation, but this Report and Recommendation recognizes that such oversight is necessary for People Beneficial Data Activities to be an independent authority for processing.<sup>34</sup> What more that enforcement and oversight should entail and how that enforcement and oversight should be conducted are outside the scope of this Report and Recommendation, and IAF suggests it is a topic appropriate for another research project.

<sup>29</sup> At the multi-stakeholder session, the criticism was made that the governance necessary to decide what is beneficial is missing. The components of the Common Reference Privacy Framework, these organizational requirements that enhance trustworthiness of processing, are the necessary governance.

<sup>30</sup> The suggestion of a formal Code of Practice is not meant to suggest self-regulation. IAF envisions a Code of Practice that constitutes a promise or representation, the breach of which would be enforced by the appropriate regulatory agency.

degree of external validation in some higher impact data activities or as part of a co-regulatory model.

When all of these requirements have been met, the authority to process personal information on the basis of People Beneficial Data Activities, which goes beyond the existing concepts of consent and legitimate interest, have been met. There should be an explicit recognition of this broader and expanded authority. Explicit recognition of this method for determining which data activities are people beneficial creates transparency and a strong foundation of trust

---

between individuals, organizations and government. Clarity among all stakeholders as to the accepted process and requirements will reduce reticence risk and will achieve both a robust digital future and a privacy protective environment for Canadians. This Framework will help implement the digital technology that brings benefits to business, communications, entertainment, transportation, banking, education, health care, interpersonal transactions and physical movements.

### **The PBI and its Associated Governance Model Builds on Previous IAF Work**

Starting in 2015, as part of its Big Data Ethics Initiative, a project to develop an approach to responsible deployment of big data built on ethics-based rules, the IAF developed three assessments: (1) the “Big Data Assessment and Framework”<sup>31</sup> which identified the elements of an assessment process that would be incorporated into an organization’s overall information accountability governance program and made subject to both internal and external oversight; (2) a generic model for assessing the appropriateness of big data analytics;<sup>32</sup> and (3) a model adapted specifically to use of big data in digital marketing.<sup>33</sup>

In 2017 and 2018, IAF conducted two projects in Canada. Part of the first project was the Canadian Assessment Framework,<sup>34</sup> a questionnaire, which could be part of an organization’s PIA and which helps organizations evaluate whether big data processing is reasonable, appropriate and legitimate. The second project, the Ethical Review Board Project,<sup>35</sup> determined

---

<sup>31</sup> “Big Data Assessment Framework and Worksheet,” The Information Accountability Foundation, July 2015, <http://informationaccountability.org/wp-content/uploads/IAF-Big-Data-Ethics-Initiative-Part-B.pdf>.

<sup>32</sup> “Enforcing Big Data Assessment Processes: IAF Big Data Ethics, Initiative, Part C,” The information Accountability Foundation, 2015, <http://informationaccountability.org/wp-content/uploads/Enforcing-Big-Data-AssessmentProcesses.pdf>.

<sup>33</sup> “Contextual Assessment Worksheet for the Marketing Industry: IAF Big Data Ethics Initiative, Part D,” The Information Accountability Foundation, 2015, <http://informationaccountability.org/wp-content/uploads/IAF-BigData-Ethics-Initiative-Part-D-For-Marketing.pdf>.

<sup>34</sup> “Canadian Assessment Framework,” The Information Accountability Project, July 2017, <http://informationaccountability.org/wp-content/uploads/Canadian-Assessment-Framework-w-CAorganizations.pdf>.

<sup>35</sup> “Canadian Ethical Data Review Boards Project,” The Information Accountability Foundation, March 2018, <http://informationaccountability.org/wp-content/uploads/Report-for-the-Comprehensive-Assessment-OversightDialog-Canadian-Ethical-Data-Review-Boards-Project.pdf>.



that two principles that govern the work conducted by Research Ethics Boards (REBs) associated with clinical research could be used to enhance the trustworthiness of organizations' assessments of data processing activities: (1) there needs to be a trusted assessment process consisting of independence, transparency, and oversight, and (2) there needs to be a common template that is used throughout the process.

In 2018, the IAF was commissioned by the Privacy Commissioner for Personal Data, Hong Kong, China, to develop the Model Ethical Data Impact Assessment (EDIA) and an Oversight Assessment.<sup>36</sup> The EDIA is an ethical and values based assessment that takes into account data

---

activity benefits as well as risks to individuals and society, considering all the interests of the parties who may be part of the activity. The EDIA uses well-established risk-modeling processes where the outcome of the analysis (significance, likelihood and effectiveness of controls) is depicted in a "net benefit/risk heat map." The Oversight Assessment is separate and independent from the EDIA and sets forth a detailed template consisting of uniform questions that should be used for overseeing the EDIA process.

### **The OPC's Proposed Socially Beneficial Activities**

In its 2016-17 Report on Consent and again in its 2020 Consultation for Ensuring Appropriate Regulation of Artificial Intelligence, the OPC recommended that Parliament consider amending PIPEDA to allow for socially beneficial activities that the PIPEDA drafters did not envisage where consent is not feasible. The OPC is of the view that the concept of socially beneficial activities needs to be limited to circumstances where consent is not likely practicable and to where the social benefits clearly outweigh the privacy incursions and where several prior conditions must be met before information can be used for such purposes. The OPC recommends that Parliament consider the circumstances where such exceptions might be warranted from a broader societal perspective. In the OPC's view, those situations where consent is likely not always practicable include: search engines indexing web sites and presenting search results to Internet users where appropriate; geolocation mapping services that society has become increasingly reliant upon; or certain data processes, such as big data analytics, Internet of Things, AI or robotics applications where commercial and societal interests align. As for prescribed conditions, those could include an organization having to demonstrate, on request that:

- It is necessary to use personal information;
- It is impracticable to obtain consent;
- Pseudonymized data will be used to the extent possible;
- Societal benefits clearly outweigh any privacy incursions;

---

<sup>36</sup> "The Hong Kong Report," The Information Accountability Foundation, October 2018, <http://informationaccountability.org/wp-content/uploads/Hong-Kong-Report-FINAL-for-electronic-distribution->

- A PIA was conducted in advance;
- The organization has notified the OPC in advance;
- The organization has issued a public notice describing its practices; and
- Individuals retain the right to object.<sup>37</sup>

The OPC's socially beneficial activities concept is similar to People Beneficial Data Activities, and a participant in the multi-stakeholder session asked why the commonly used term "social benefit" was replaced with the term "people benefit". As the term suggests, the OPC limits

---

[10.22.18.pdf](http://informationaccountability.org/wp-content/uploads/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf); "Ethical Data Impact Assessment," The Information Accountability Foundation, October 2018, <http://informationaccountability.org/wp-content/uploads/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf>. socially beneficial activities to activities that benefit society.<sup>38</sup> The OECD, in its recommendation of a Common Reference Privacy Framework that includes digital risk management, takes a much broader approach. It sets up an accountability-based Framework that includes looking at the use of the digital technology ecosystem from the perspective of groups of individuals, society and organizations and weighing the benefits and detriments and mitigates, as much as possible, the detriments from all three perspectives. Only such a broad, accountable risk analysis coupled with increased transparency will achieve the trustworthy processing that is necessary to a digital and data-driven economy. In this way, data are respectful of and serve the interests of people. An OECD-type privacy Framework helps organizations determine whether data activities benefit people. Indeed, the OPC reaches much the same conclusion in its Privacy Law Reform Report contained in its most recent Report to Parliament when it urges that organizations and federal government institutions should be required to demonstrate their accountability.<sup>39</sup>

### **The OPC's Proposed Demonstrable Accountability**

---

<sup>37</sup> Consultation for ensuring appropriate regulation of artificial intelligence, Proposal 7, [https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos\\_ai\\_202001/](https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/); 2016-17 Annual Report to Parliament on PIPEDA and The Privacy Act – OPC Report on Consent, [https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\\_index/201617/ar\\_201617/](https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/).

<sup>38</sup> In its 2018-19 Annual Report to Parliament on the Privacy Act and the PIPEDA – Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy, [https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\\_index/201819/ar\\_201819/](https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/) [hereinafter "Privacy Law Reform Report"], the OPC agrees that its exception to consent, socially beneficial activities, is limited to activities that benefit society. "Societal benefits have also been referred to by some as "socially beneficial purpose" or "public good". We are of the view there has to be a more critical examination of what companies (and governments) believe to be societal benefits. We have learned through our investigative and advisory work that purported socially beneficial uses by a company, industry or government are not always aligned with the public's idea of societal good or individual interests – some benefits are greater than others, and there are limits to how much individuals are willing to compromise their rights in the name of the public good"

<sup>39</sup> Privacy Law Reform Report

In the Privacy Law Reform Report, the OPC argues that the current accountability Framework needs to become more robust and advocates for an enhanced and strengthened law that will require demonstrable accountability. Specifically, the OPC feels the following enhancements to the law would help support demonstrable accountability:

- Proactive inspection powers without grounds. The OPC wants a provision added to PIPEDA that gives the Privacy Commissioner the legal authority to proactively inspect the practices of organizations, i.e., carry out investigations at his discretion in order to ensure an organization is compliant with PIPEDA.
- A requirement to provide evidence of accountability on demand. Organizations should be required by law to maintain records to provide evidence of adherence with accountability requirements. The record keeping requirement would facilitate the OPC's ability to conduct proactive inspections under PIPEDA.
- A requirement to design for privacy and assess privacy risks at the start of the planning process. Accountability involves building privacy assurance into the very design of a product, service or initiative, from the early phase of conception through to its execution, deployment and beyond. PIAs are an effective tool to assist with this effort, and the OPC advocates that PIAs be mandatory in law.

---

The IAF agrees with these comments of the OPC about demonstrable accountability. People Beneficial Data Activities, as an authority either alternative to or in addition to consent and legitimate purposes, is not a self-regulatory scheme but rather demonstrable accountability. People Beneficial Data Activities require, in addition to accountability by appropriate internal individuals, transparency, internal oversight, and protection of individual rights:

- Independent external oversight, including proactive inspection of organizational practices, by the appropriate regulator
- A record of all People Beneficial Data Activities engaged in by the organization, including a record of how all accountability requirements have been met
- People Beneficial Impact Assessments (PBIAs), a part of privacy by design, which, among other things, assess risk during the life cycle of the activity.

### **Conclusion**

Presently, the processing of personal information for legitimate purposes based on implied consent in connection with People Beneficial Data Activities is authorized as long as it is limited to those activities provided within the "condition of the supply of a product or service."<sup>40</sup>

---

<sup>40</sup> Sections 3 and 5(3) of PIPEDA

However, in order to maximize the opportunities for People Beneficial Data Activities, there should be a provision in a future law or in revisions to the existing law that expressly recognizes People Beneficial Data Activities as an authority to process personal information. This explicit recognition would lessen reticence risk, i.e. a reduction of any inhibition to innovation, and would provide more benefits if these activities were not limited to those provided within the “condition of the supply of a product or service” as long as they meet all the elements of demonstrable accountability and are aligned with the objectives, culture, and values of the organization.

Limiting People Beneficial Data Activities to those provided within the “conditions of the supply of a product or service” might contribute to personal data not being used for people beneficial purposes. People Beneficial Data Activities as an authority to process personal information requires a Common Reference Privacy Framework that includes managing digital risk. Such a Framework requires being accountable, conducting PBIAs, being transparent, having internal oversight, being subject to external oversight, keeping records, and protecting individual rights. This Framework will create a strong foundation of trustworthy processing for individuals, organizations and government. “[D]ata is about [people]. It should be treated [and used] in a way that it is respectful of [and serves the interests of people.]”<sup>41</sup>

---

<sup>41</sup> Statement of Joni Brennan, President of the Digital ID and Authentication Council of Canada, Leading experts join SCC effort to transform data governance landscape, June 4, 2019, <https://www.scc.ca/en/newsevents/news/2019/leading-experts-join-scc-effort-transform-data-governance-landscape>.

## Appendix 1

### Contributing Participants

*The following individuals and organisations were among the participants in the project.*

Adam Kardash, Osler, Hoskin & Harcourt LLP

Bell Canada

Canadian Marketing Association

Canadian Tire Corporation, Ltd

David Goodis, Assistant Commissioner, Information and Privacy Commissioner of Ontario

Goeasy

Gregory Smolynek, Deputy Commissioner Policy and Promotion, OPC

IBM

Jennifer Stoddart, O.C., Ad.É.

Jordan Prokopy, National Privacy Practice Leader, PWC Canada

Lauren Reid, The Privacy Pro

Loblaw Companies Limited

Manulife

Michael Geist, University of Ottawa, Faculty of Law

Novartis Pharmaceuticals Canada Inc

Office of the Information and Privacy Commissioner of Alberta

Pentavere

Sidewalk Labs

SunLife

Symcor



## Appendix 2

### **People Beneficial Impact Assessment - DRAFT MODEL ASSESSMENT**

A People Beneficial Impact Assessment (PBIA) is a process that looks at the full range of interests of all stakeholders in a data processing and data use activity to achieve an outcome that best facilitates the achievement of benefits and an appropriate mitigation of stakeholder risks. A PBIA assists an organization in looking at the interests impacted by the data collection, use and disclosure in a data-driven activity. A PBIA also could cover a data-driven activity that involves several organizations. The Model PBIA consists of four sections:

- I. **Purpose of the activity**
- II. **Data – a full understanding of the data, data use and parties involved**
- III. **Impact to each stakeholder**
- IV. **Decision – whether an appropriate balance of benefits and mitigated risks supports the data use scenario.**

The very nature of an ethical, fair and values-based assessment requires a careful consideration of the data activity benefits as well as the risks to all stakeholders (e.g., the interests of all the parties who may be part of the data activity and use). While open, structured questions can help, a way to evaluate the ultimate decision as to whether to proceed is to use an optional well-established risk modeling process where the outcome of the analysis (significance, likelihood and effectiveness of controls) is depicted in a “net benefit/risk heat map”. This quantitative portion uses a standardized risk assessment process often found in many organizations’ Enterprise Risk Management (ERM) programs. Whether the quantitative approach is used in addition to the qualitative assessment, the output is to help determine whether there is a net positive benefit to stakeholders that may be impacted by the data use scenario and risks to all stakeholders have been sufficiently reduced through active mitigation actions.

Successful implementation of an PBIA assumes and depends on highly qualified and competent, accountable roles and responsibilities with appropriate separation of duties. For example, PBIA’s could be conducted by the privacy group or a data scenario business owner. However, the evaluation should include appropriate organization representatives of both the benefits and risks to impacted stakeholders. The structure of the overall Model PBIA is illustrative and should be adapted as appropriate for each organization as well as the different data-processing contexts.

The PBIA is broader in scope than the typical Privacy Impact Assessment (PIA); however, the PBIA could be used in conjunction with the PIA. For example, all data and data use are considered in an PBIA and not just personal data. However, to the extent the

PBIA can be used to consider and appropriately mitigate the impact of a personal data practice, the process may supplement (or be woven into) the organization’s already existing PIA process. In this regard, the PBIA process may enhance an organization’s privacy management program and compliance with its legal obligations under various regulatory frameworks. However, a PBIA does not replace a PIA; it is designed to be used in conjunction with PIAs.

**Additional requirements:**

- If the project involves a Phase 1 “learning” stage (e.g. determine through analysis insights that could be used), appropriate and relative risk mitigations should be established and a follow-up PBIA should be committed to before any use of data or insights that could have an impact on stakeholders occurs,
- A follow-up assessment process should be committed to in order to evaluate whether the project is achieving its desired benefits and risks have been mitigated as intended or planned and to determine whether there have been any unanticipated consequences,
- All other/related People Beneficial accountability requirements should be met.

<b>Project Data Overview - Background</b>	<i>Italicized content is provided as an example of types of questions and issues that should be explored as part of the PBIA</i>
What is the <b>summary</b> purpose or objective for this data use scenario?	<i>What is the <b>summary</b> business need/goal/objective for this project? Who are the targeted beneficiaries of this data use scenario and how would they benefit?</i>
Describe how the data activity meets the fundamental criteria of People Beneficial? <ul style="list-style-type: none"> <li>• The data-driven activity must have a describable purpose and a benefit that accrues to “people” (plural).</li> <li>• Negative consequences or detriments, including the risk of not using personal data for People Beneficial Data Activities, must have been mitigated to a satisfactory and demonstrable level.</li> </ul>	<i>The benefit aligns with an externally created societal objective (ideally substantiated benefit) and supports stated social values and activities organizations have committed to</i>  <i>Have a describable purpose and benefit that accrues to “people” (plural)</i>



<p>Is this activity an expansion of a previous activity or a new initiative?</p>	<p><i>Is this activity an expansion of a previous activity? If yes, was a previous assessment done? If a previous assessment was done, what</i></p>
<p>If a previous assessment was done, what has changed in this data activity and why (refer to previous assessment)?</p>	<p><i>has changed in this data activity and why (refer to previous assessment)?</i></p> <p><i>If the Phase 1 of this project involves a learning with data component <b>before</b> and specific use that may have an impact on people, consider both a relative level of risk mitigation and <b>note that a further PBIA will be required</b> as part of a decision to use the data or insights.</i></p>
<p>What are the objectives of this data activity <b>for each group of stakeholders (each entity or group of individuals participating and/or being impacted by the data use scenario)</b>? Explain in terms of explicit outcomes/goals and how these outcomes map to other external positive justification/validation that is generally accepted by the society.</p>	<p><i>Stakeholder 1</i></p>
	<p><i>Stakeholder 2</i></p>
	<p><i>Stakeholder 3</i></p>

- Clearly state the problem that is to be solved.
- Clearly state the measurable goal or outcome of the project
- What is the interest (high-level) for ALL impacted stakeholders?

***Stakeholder 4***

*Objectives should be explicitly describable for each stakeholder and map to some externally validated objective (e.g. broader public policy objective). Consider objectives such as: better/lower cost health care, greater access to health services, or better health outcomes or an improved ability to track and assess health outcomes; more accurate sensors or devices to detect or diagnose health conditions or to improve general wellness; improved education; environmental enhancements such as water conservation, energy cost reduction; infrastructure enhancements; economic improvement; more accessible/usable technology; increased job opportunities; protection of reasonable expectation of privacy, including anonymity; protection of freedom of*

*religion, thought and speech or protection of prohibition against discrimination*

What data is involved in this project? From the PIA, describe what specific types of data about people will be provided, included, collected, tracked, transferred, used and/or stored. Identify which third parties are involved and the sources/disposition of data types. Include how data categories achieve, or are aligned to, the purpose. In the case of any onward transfer of data to a 3<sup>rd</sup> party, determine that the 3<sup>rd</sup> party assumes the same base data use requirements (Principle of Onward Accountability with PBIA Parameters).

***For example: (section could reference PIA content if this information is collected there)***

- *Does this project involve the direct collection of, or use, data about people?*
- *Does the data activity involve personal information?*
- *Is the data observed (created as the result of individuals, or activities about individuals, being observed and recorded)? (e.g. meta data, logs, behavioral data)*
- *Is the data derived (created from other data and becomes a new data element related to an individual/group)? (e.g. lives in a high-income neighborhood)*
- *Is the data inferred (product of a probability-based analytic process)?*
- *What are all the sources of the data (internal and external)?*
- *Is the data going to be shared with third parties? If yes, explain the purpose for the sharing and the role of the third party.*
- *Will the data be matched against, combined with, or augmented by other data sets? If yes, explain.*

<p>Describe the level of Data Identifiability and Sensitivity (actual and perceived)</p>	<p><i>Is the data identifiable to a person or is it deidentified? If de-identified, describe the process to achieve and <b>maintain</b> this state? Is the data or anticipated use of the data sensitive or likely to be perceived as sensitive?</i></p> <p><i>Is the data sensitive? Is the anticipated use of data likely to be considered sensitive?</i></p> <p><i>Sensitive categories of data or data use include information associated with personal data that is used to make a decision or discriminate based on race, ethnic origin, religion or philosophical belief, sexual orientation, physical or mental health, information or data that could be used to facilitate identity theft, information associated with personal data that is used to permit access to an individual's account, precise location and/or there is a reasonable expectation the use of the data would be embarrassing or be considered sensitive to the individual whose data it is</i></p>
<p>Key Issues</p>	<p><i>Are there any identifiable key issues that need to be managed prior to completing the assessment?</i></p> <p><i>Who are all the possible stakeholders and users involved or related to the data activity or use of the metrics or measures? What are their interests and/or potential concerns (high-level)?</i></p>

**Beneficial Impact to the Organization**

<p>What are the benefits of this data activity to the Organization(s)?</p>	<p><i>Determine and describe what the benefits are that could be realized by the principal/organization. Consider factors such as increased revenue, lower costs, improved profitability, greater market share, enhanced employee satisfaction, engagement and productivity, enhanced customer relationship, enhancement or maintenance of brand or reputation, assurance of compliance, fraud prevention, enhancement or maintenance of cyber or physical security, new or improved products or services or customer service, improved manner of marketing, improved ability to assess customer preferences, improvements to innovation or enabling greater, faster, more efficient innovation, improved research processes, improved ability to conduct research and find or enroll study subjects, or improved efficiency with studies, innovative ways to conduct research .</i></p>
--	--

**Beneficial Impact to Specific Stakeholders -**

<p>What are the benefits to the defined impacted other stakeholders? Could the data be used in a way that may result in a specific stakeholder or group of stakeholders being treated differently in a <b>positive way</b> from other groups of individuals?</p>	<p><b><i>Stakeholder 1</i></b></p>
	<p><b><i>Stakeholder 2</i></b></p>
	<p><b><i>Stakeholder 3</i></b></p>
	<p><b><i>Stakeholder 4</i></b></p> <p><i>Determine and describe the positive impacts on the various stakeholders that are expected to come from the application of this data activity. Are there identifiable expectations of individuals, groups of individuals for each beneficial use of the information? Determine what the potential positive goal of the difference in treatment is (if any).</i></p>

What are the factors that may limit the realization of any benefits to external stakeholders?	
How significant is the benefit to impacted stakeholders and how likely is this to happen? (1-Low; 3-Medium;5-High)	

<p><b>Note</b> – The benefits to the principle data scenario organization should not be factored into the qualitative assessment – <b>Quantitative section is a way to express the qualitative section numerically. It is provided for illustration purposes – Format would match organizations’ approach and could align with other risk assessment methodologies</b></p> <table border="1"> <thead> <tr> <th>Description For Significance or Impact</th> <th>Impact Score</th> </tr> </thead> <tbody> <tr> <td>The benefits or circumstance is <b>Highly Impactful</b></td> <td><b>High Impact</b> 5</td> </tr> <tr> <td>The benefits or circumstance is <b>Moderately High Impact</b></td> <td><b>Moderately High Impact</b> 4</td> </tr> <tr> <td>The benefits or circumstance is <b>Moderately Impactful</b></td> <td><b>Moderate Impact</b> 3</td> </tr> <tr> <td>The benefits or circumstance is <b>Moderately Low Impact</b></td> <td><b>Moderately low Impact</b> 2</td> </tr> <tr> <td>The benefits or circumstance is <b>Minimally Impactful</b></td> <td><b>Low Impact</b> 1</td> </tr> </tbody> </table>	Description For Significance or Impact	Impact Score	The benefits or circumstance is <b>Highly Impactful</b>	<b>High Impact</b> 5	The benefits or circumstance is <b>Moderately High Impact</b>	<b>Moderately High Impact</b> 4	The benefits or circumstance is <b>Moderately Impactful</b>	<b>Moderate Impact</b> 3	The benefits or circumstance is <b>Moderately Low Impact</b>	<b>Moderately low Impact</b> 2	The benefits or circumstance is <b>Minimally Impactful</b>	<b>Low Impact</b> 1	
Description For Significance or Impact	Impact Score												
The benefits or circumstance is <b>Highly Impactful</b>	<b>High Impact</b> 5												
The benefits or circumstance is <b>Moderately High Impact</b>	<b>Moderately High Impact</b> 4												
The benefits or circumstance is <b>Moderately Impactful</b>	<b>Moderate Impact</b> 3												
The benefits or circumstance is <b>Moderately Low Impact</b>	<b>Moderately low Impact</b> 2												
The benefits or circumstance is <b>Minimally Impactful</b>	<b>Low Impact</b> 1												

<b>Negative Impact to Specific Stakeholders -</b>	
<p>Considering all the factors relating to the data activity, the likely use of data by each stakeholder, the identifiability and sensitivity of the information and its use, what are the risks (real and/or perceived) to each identified stakeholder?</p> <p><b>Individual Impact</b> – Is it foreseeable that the potential insights or the use of information might seem surprising, inappropriate or discriminatory or might be considered offensive causing distress? Is this use potentially outside of</p>	<i>Stakeholder 1</i>
	<i>Stakeholder 2</i>
	<i>Stakeholder 3</i>

<p>what an individual might reasonably expect or what might be considered reasonable?</p>	<p><b>Stakeholder 4</b></p> <p><i>Consider the risks or increase in risks (real or perceived) to the identified stakeholder as the information is or may be. Areas to consider include: perception of data about them being used in an impactful way, an impact to their employee relationship, reduced status and/or well-being; damage to reputation or embarrassment; shock or surprise at the processing activity or the results of the processing; inappropriate discrimination, the possibility of inappropriate access to or misuse of information by the organization, including sensitive</i></p>
	<p><i>categories of data and directly identifiable data; manipulation of needs or desires/wants of the individual (i.e. creation of a need where one previously did not exist); a negative impact of the information through a probability-based process, such as a score; Who will have access to this information and who won't? Will stakeholders who don't have access to this information or data or the insight suffer a setback compared to those who do? What does that setback look like? What new differences will there be between the "haves" and "have-nots" of this information? Would individual stakeholders be surprised by the activity related to them? Would the information use about individuals align with their perception of whether this data/information should be used this way? Determine whether there are other sensitivity issues with the potential use of insights and what aspect of use of potential insights might be considered unfair to the stakeholder. Are all stakeholders treated equally?</i></p>
<p>For data activities that involve 3<sup>rd</sup> parties (receiving or sourcing data as part of this activity), what are the associated risks?</p>	<p><i>Examples of 3rd parties could include data brokers that sell blocks of information, data aggregators, providers of storage and computing tools, data trusts. Examples of risks could include data accuracy, data protection, downstream use monitoring and control, legitimate data collection (when done through 3rd parties), data availability.</i></p>

How significant is the risk and what is the likelihood? (1 – Low; 3 – Medium; 5 – High) - **Quantitative section is a way to express the qualitative section numerically. It is provided for illustration purposes – Format would match organizations’ approach and could align with other risk assessment methodologies**

Description For Significance or Impact	Impact Score
The risk or circumstance is <b>Highly Impactful</b>	<b>High Impact</b> 5
The risk or circumstance is <b>Moderately High Impact</b>	<b>Moderately High Impact</b> 4
The risk or circumstance is <b>Moderately Impactful</b>	<b>Moderate Impact</b> 3
The risk or circumstance is <b>Moderately Low Impact</b>	<b>Moderately low Impact</b> 2
The risk or circumstance is <b>Minimally Impactful</b>	<b>Low Impact</b> 1

What aspects about the activity have the highest impact on the likelihood any of these risks could be realized?



<p>What are the additional technical and/or procedural safeguards (mitigating controls) that are being implemented to prevent and mitigate risks should they occur?</p> <ul style="list-style-type: none"> <li>• If de-identified data is being used, describe the process to achieve this state</li> <li>• If identifiable data is being used, is this required for the purpose and have commensurate controls been implemented to protect the data?</li> <li>• If data is shared with 3rd parties, describe the way and manner that downstream obligations are to be managed and enforced</li> <li>• Have appropriate governance and accountability measures and processes been established?</li> <li>• Is the accuracy and/or quality of the data appropriate for the data activity? Does the relative accuracy of the data have an impact on individuals/groups?</li> </ul>	<p><i>A mitigating control is a type of control used to discover and prevent mistakes that may lead to uncorrected and/or unrecorded misstatements that would generally be related to control deficiencies. A mitigating control may help to remedy any elevated risk identified in the analyses above. Determine what risks can be mitigated and how these risks can be mitigated. Examples of appropriate governance and accountability measures could include internal oversight, procedural documentation, training, attestation, etc.</i></p>
<p>Is there a less data-intensive way to achieve the goals of the activity (including potential insights)?</p>	<p><i>Determine whether the minimum possible amount of data has been used in the data activity and/or the access of the resulting measure or metrics.</i></p>
<p>Describe the mechanism used to explain externally how data is used, how benefits and risks to individuals that are associated with the processing are considered and/or addressed.</p>	<p><i>Determine what the transparency and individual accountability mechanisms are and whether they are appropriate for the information activity use. Does the application of the information do anything your users don't know about, or would probably be surprised to find out about?</i></p>
<p>How effective are these controls and safeguards in reducing risk</p>	

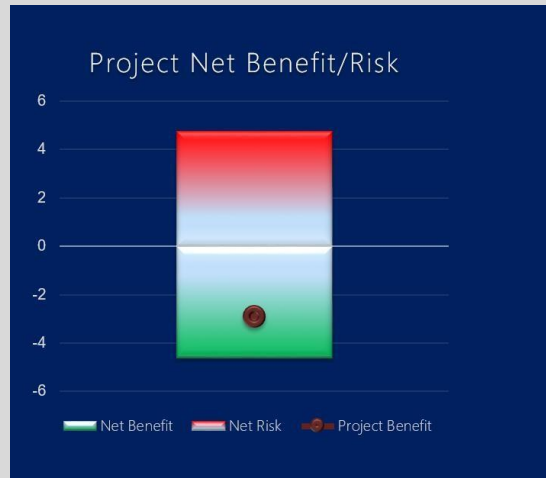
(1 – Low; 3 – Medium; 5 – High) **Quantitative section is a way to express the qualitative section numerically. It is provided for illustration Purposes – Format would match organizations’ approach and could align with other risk assessment methodologies**

Description For Significance or Impact	Impact Score
The controls are <b>Highly Effective</b>	<b>Highly Effective</b> 5
The effectiveness of controls are <b>Moderately High</b>	<b>Moderately High Effectiveness</b> 4
The controls are <b>Moderately Effective</b>	<b>Moderately Effective</b> 3
The effectiveness of controls are <b>Moderately Low</b>	<b>Moderately Low Effectiveness</b> 2
The effectiveness of controls are <b>Low</b>	<b>Low Effectiveness</b> 1

**Decision – whether an appropriate balance of benefits and mitigated risks supports the data processing activity and achieves a goal of “people beneficial”.**

Are there any other factors that should be considered? Determine whether the interests, expectations and rights of individuals have been effectively addressed and what additional contextual based individual participation and choice factors should be considered.

**Quantitative recap/output section is a way to express the qualitative section numerically. It is for illustration Purposes – Format would match organizations’ approach and could align with other risk assessment methodologies**



*Consider are the risks necessary and proportional to the benefits? Have the risks have been mitigated to the extent possible? Are the mitigated risks sufficiently balanced by the benefits? Does the purpose of the activity fit within the values of society?*

*If this assessment represents a Phase 1 of a project (e.g. learning), has a process/date been set for a follow-up PBIA prior to any application of data or insights that may have an impact on people? What is the planned overall follow-up assessment process to evaluate whether the project is achieving its desired benefits and whether risks have been mitigated as intended or planned and whether there have been any unanticipated consequences?*

**Approval by Accountable Officer**

*Describable, achievable **net positive** benefit outcomes (tangible benefits to people) have been demonstrated, and negative consequences have been mitigated to a satisfactory and demonstrable level. The proposed uses of data also incorporate Canadian values of diversity, inclusion, and privacy as a fundamental human right. By definition, the standard of having a clear purpose and value to the proposed use of data, as well as a clear, direct connection to the ways in which the project and*

*proposed data activity would benefit individuals or the community has been met.*

*The assessment of the data driven scenario was completed by highly qualified and competent, accountable roles and responsibilities with appropriate separation of duties. All other People Beneficial accountability elements been satisfied and follow-up assessments been formally established.*