Canada's Privacy Impact Assessment Policy: History, Content, Analysis, and Implications (Postprint)

Authors: Chen Mei, Liang Yikai

Date: 2023-04-01T16:02:55+00:00

Abstract

[Purpose/Significance] From a policy perspective, this study investigates the policy support for Privacy Impact Assessment (PIA) in Canada, aiming to provide references for PIA policy formulation in our country and to provide tools for government protection of citizen privacy.

[Method/Process] Employing literature review and case study analysis, this study takes Canada as an example, obtains first-hand materials through investigating literature and website content to elaborate on the development history of Canada's Privacy Impact Assessment policy, systematically reviews the policy objectives, policy subjects, and policy content, and analyzes the strengths and weaknesses of Canada's Privacy Impact Assessment policy on this basis.

[Results/Conclusion] Proposes recommendations for enhancing the skills of policy implementers, formulating PIA policies at an early stage, and strengthening recognition of PIA policies.

Full Text

Canadian Privacy Impact Assessment Policy: History, Content, Analysis, and Implications

Chen Mei[1], **Liang Yikai**[2] [1]School of Public Administration, Zhongnan University of Economics and Law, Wuhan 430073 [2]School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan 250014

Abstract: [**Purpose/Significance**] From a policy perspective, this paper investigates the policy support for Privacy Impact Assessment (PIA) in Canada to provide references for China's PIA policy formulation and tools for government protection of citizens' privacy. [**Method/Process**] Using literature research

and case analysis methods, and taking Canada as an example, this paper expounds on the development process of Canada's PIA policy through investigation of literature and website content to obtain first-hand materials, sorts out the policy objectives, policy subjects, and policy content, and analyzes the advantages and disadvantages of Canada's PIA policy. [**Result/Conclusion**] The paper proposes recommendations to improve the skills of policy implementers, formulate PIA policies as early as possible, and strengthen identification with PIA policies.

Keywords: Privacy Impact Assessment; Canada; Government Open Data; Privacy Risk **Classification Number:** D035 **DOI:** 10.13266/j.issn.0252-3116.2021.17.014

With the rapid development of information and communication technologies, numerous possibilities and advantages have emerged. The use of personal computers and telecommunications networks has improved service efficiency and made our daily lives more convenient. However, technology has also brought new dangers to personal privacy and freedom. In many cases, transmitted data involves natural persons, and databases or files related to personal data are created, used, disclosed, and sold, making it difficult to know who owns the data and what these people are doing. Individuals can no longer control their data, and the risk of misuse is increasing. Therefore, it is necessary to analyze data processing to identify corresponding risks and impacts. As a government tool, "Privacy Impact Assessment" (PIA) can evaluate the impact of data controllers' activities on data protection and personal privacy, minimize potential risks, and create a safer environment for data controllers and data subjects to exercise their rights and freedoms. The concept of PIA has been proposed since at least the 1980s, along with policy debates targeting technology. By combining the two sub-concepts of "PIA" and "policy," PIA policy refers to the guidelines and standards established by political parties, administrative organs, and relevant political groups to achieve privacy impact assessment, including regulations, directives, speeches and instructions by senior officials, etc. The reason for selecting Canada as a case study for PIA policy is that, on the one hand, although some domestic scholars have studied PIA standards at home and abroad [1] and analyzed the relevant provisions of the Data Protection Impact Assessment system in the EU's General Data Protection Regulation (GDPR) [2], and studied the origin, value, and implementation of PIA [3], no systematic research has been conducted on Canada's PIA policy; on the other hand, from a practical perspective, Canada's PIA policy is relatively well-developed. Therefore, by sorting out the development history of Canada's PIA policy, analyzing its policy content, and discussing the policy's advantages and disadvantages, this paper aims to provide references for China's personal privacy protection and big data governance.

1. Development History of Canada's PIA Policy

Dividing the development process in chronological order can clearly present the trajectory of PIA policy changes and provide deeper analysis of the underlying conceptual shifts. However, time is only the external manifestation of policy evolution, not its essence, so attention should also be paid to its degree of development. Therefore, this paper divides the development history of Canada's PIA policy into three stages based on chronological order combined with development degree.

1.1 Preparation Stage

In May 2000, the Office of the Privacy Commissioner of Canada (OPC) released the *Annual Report to Parliament 1999-2000*, which emphasized the consequences of insufficient privacy attention: the combination of massive personal databases, powerful computer systems, and growing linkages between provincial social programs and the private sector has raised great privacy concerns. However, if the government does not appropriately assess and mitigate these concerns, or fails to anticipate public negative reactions to the program, it will ultimately lead to greater losses. Although this document describes situations that occurred in the past, it reflects a pioneering moment for privacy protection within the federal government, providing a critical example of the risks brought by poor privacy plans and outlining the PIA process. Details are shown in Table 1 .

In May 2002, the Canadian government promulgated the *Privacy Impact Assessment Policy* (PIA Policy) [5], requiring PIAs for all government actions that would increase privacy risks, and sharing the analysis results and recommended measures to address identified risks with the OPC for review and evaluation. Government agencies must also publish summaries of their PIAs on their websites [5]. The policy aims to assure Canadians that privacy principles will be considered when proposing plans and services that raise privacy concerns in the design, implementation, and development of programs, services, and initiatives. The policy addresses policy requirements, roles and accountability, monitoring and oversight, and stipulates the development and maintenance of PIAs, requiring government agencies to inform the Privacy Commissioner and the public of PIA results.

In August 2002, Canada issued the *PIA Guidelines: A Framework to Manage Privacy Risks* (PIA Guidelines) [6], containing guidelines designed to provide a comprehensive framework for completing PIAs. The 40-page document is divided into six chapters, including introduction, purpose, PIA procedures, process overview, detailed process description, and privacy impact analysis report. Specifically, the framework for completing a PIA includes: a checklist for when a PIA is needed; PIA objectives; process overview (resource requirements, documenting data flows, privacy analysis, privacy impact analysis report, addressing risks); questionnaires for federal programs and services; questionnaires for cross-

jurisdictional initiatives; Preliminary Privacy Impact Assessment (PPIA); and a model table for PIA content. This policy ensures that privacy principles and legislation are considered and complied with throughout the entire lifecycle of new programs, services, or initiatives, and where appropriate, for the transformation or redesign of existing ongoing services.

In August 2002, Canada released the *PPIA Model* [7], an electronic template for standardized production of PPIAs and PIAs (PIA report template). In March 2003, Canada released the *Report on PIA Best Practices* [8], identifying practical tips and best practices for implementing PIA policy and guidelines in departmental daily operations. In October 2003, Canada released the *PIA E-learning Tool* [9], including three aspects: an overview module reviewing the basic principles of privacy rights in Canada and discussing the rationale for privacy protection procedures, including key privacy definitions, review of Canadian privacy legislation and policies, main features and benefits of PIA, overview of the PIA process, and main stakeholders involved in PIA; a management or supervision module designed to review key concepts related to PIA, such as legislation and policies and key stakeholders, but examining the entire PIA process in more detail than the overview module described above, including tips from "best practices" of Canadian government personnel involved in PIA projects, coordinating and supervising PIA projects; providing step-by-step review of the PPIA or PIA process, such as how to write an executive summary of a report or how to use a document change control table, and filling out federal program and service questionnaires, while also providing links to the *Privacy Act* [10], *Personal Information Protection and Electronic Documents Act* (PIPEDA) [11], and even definitions of key terms.

This stage mainly focuses on policy planning and formulation, that is, the process of identifying the occurrence of privacy protection issues, identifying policy problems, planning solutions, and legitimizing the solutions to produce formal policies. For example, the Privacy Commissioner Office's report, driven top-down, raised privacy protection as a policy issue, which was quickly adopted by the government and actively promoted.

1.2 Implementation Stage

In May 2004, Canada released the *PIA Audit Guidelines* [12], including several aspects: introducing policy requirements and relevant information and key sources to understand the basic knowledge of the PIA process; providing background information to expand readers' understanding of the responsibilities of key stakeholders involved in completing, reviewing, and approving PIAs; and proposing audit objectives and standards that internal auditors can use to develop customized audit plans based on risk-based audit approaches.

On April 1, 2008, the *Social Insurance Number (SIN) Directive* came into effect, replacing the "Policy Requirements Related to Social Insurance Number" in the *Privacy and Data Protection Policy* [13] promulgated in 1993. In 1993,

Canada promulgated the *Privacy and Data Protection Policy*, whose objectives were to ensure that government agencies effectively and consistently apply the provisions of the *Privacy Act* and *Privacy Regulations* [14]; ensure that data matching and data linking of personal information for administrative purposes comply with the above legal requirements; limit the scope of collecting and using Social Insurance Numbers (SIN) for administrative purposes to those permitted by specific acts, regulations, and programs, and set conditions for their collection. Appendix B of the *Social Insurance Number (SIN) Directive* stipulates three steps for obtaining policy approval: preliminary assessment, analysis and consultation, and seeking approval. The second step mentions that before seeking approval from the President of the Treasury Board, the following process must be completed: submit a complete PIA report on the new collection to the Information and Privacy Policy Division of the Treasury Board Secretariat (TBS); notify the Privacy Commissioner according to Article 6.2.12 of the *Privacy Protection Policy* and Article 9(4) of the *Privacy Act*.

On April 1, 2010, the Treasury Board Secretariat of Canada issued a new directive on PIA, the *Directive on Privacy Impact Assessment* [15]. This directive replaced the *PIA Policy* that had been in effect since May 2, 2002, and the data matching portion of the *Privacy and Data Protection Policy* promulgated in 1993. This new directive applies to government agencies but not to the development of new legislation. The directive states that the Government of Canada is committed to ensuring that privacy protection is a core consideration in the initial development and subsequent management of programs and activities involving personal information.

In March 2011, the Office of the Privacy Commissioner (OPC) released a guidance document, *Expectations: A Guide for Submitting PIAs to the Office of the Privacy Commissioner of Canada* [18], to clarify expectations for the type and depth of information agencies should provide to the government when submitting final PIA reports. Although the policy formulated by the Treasury Board Secretariat requires PIAs, the Privacy Commissioner has called for reforming the *Privacy Act* as part of a broader reform and requiring this reform. The Privacy Commissioner supports the *Directive on PIA* but believes that converting it into law would give it stronger effect.

1.3 Development Stage

From March 13, 2020, to September 30, 2020, the *Interim Policy on Privacy Protection* [16] came into effect, replacing the *Privacy Protection Policy* released on July 1, 2018. According to Article 4.2.14 of this document, government agency heads ensure that PIAs and multi-agency PIAs are developed, maintained, and published where applicable; however, for emergency COVID-19-related initiatives, deputy heads or their assistant deputy representatives may exercise discretion to complete a privacy compliance assessment for new or substantially modified programs in lieu of a complete PIA. If discretion is exercised for programs continuing after December 31, 2020, a complete PIA must be completed

by June 30, 2021.

From March 13, 2020, to September 30, 2020, the *Interim Directive on Privacy Practices* [17] came into effect, replacing the *Directive on Privacy Practices* issued on May 6, 2014. According to Article 6.1.4 of this document, government agency heads must submit requests to the Treasury Board Secretariat to register each new Personal Information Bank (PIB) or terminate existing PIBs, and ensure that requests are accompanied by the following information: in cases requiring registration of a new PIB, all elements of the PIB described in items 11(1)(a)(i) to (vi) of the Act, and a completed and approved core privacy impact assessment. A PIB refers to a collection or grouping of personal information.

From March 13, 2020, to September 30, 2020, the *Interim Directive on Privacy Impact Assessment* [17] came into effect, replacing the *Directive on PIA*. In March 2020, the document *Expectations: A Guide for Submitting PIAs to the Office of the Privacy Commissioner of Canada* was updated to provide federal public sector institutions with guidance on how to comply with the *Privacy Act* and effectively manage privacy risks as part of the PIA process. It presents key concepts and proposes how institutions can assess their programs and activities, including legal requirements and privacy principles to consider [18].

With the development of information technology, it is necessary to improve the original PIA policy and leverage its guiding role. Therefore, this stage focuses on adjusting the PIA policy to not only coordinate the relationship between policy objectives and policy solutions but also ensure the coherence of PIA policy. Specifically, Canada has made different forms of adjustments to its PIA policy, such as policy replacement (*Interim Policy on Privacy Protection*, *Interim Directive on Privacy Practices*, *Interim Directive on Privacy Impact Assessment*) and policy updates (*Expectations: A Guide for Submitting PIAs to the Office of the Privacy Commissioner of Canada*).

This stage not only focuses on the nature of PIA policy issues, policy objectives, and the feasibility and possible consequences of policy solutions, but also on the interaction between PIA policy and privacy protection law. There is mutual linkage between policy and law, presenting an interactive relationship with two sides. On the one hand, policy legalization means converting policy into legislation: legislating PIA policy. On the other hand, it attempts to use the law (*Privacy Act*) to influence and change people's institutional behaviors, guiding people's behavior in the direction hoped for by policymakers and legislators—that is, law is a tool to achieve PIA policy objectives.

2. Analysis of Canada's PIA Policy System

2.1 Policy Objectives

The specific objectives of PIA include: building trust and confidence with citizens; enhancing awareness and understanding of privacy issues; ensuring privacy protection is a key consideration in the initial framework of program objectives

and activities; establishing clear accountability for privacy issues; reducing the risk of having to terminate or substantially review programs or services after implementation to comply with privacy requirements; providing decision-makers with necessary information to make informed policy, system design, or procurement decisions based on understanding of privacy risks and options for mitigating these risks; and providing basic documentation on business processes and personal information flows for departmental staff to jointly use and view, and as a basis for consultation with stakeholders [6].

2.2 Policy Subjects

Different policy subjects can participate in formulating PIA policy. These subjects start from perceiving privacy protection issues, make them issues for government action, place them on the government agenda for consideration, and finally ensure relevant government actions, all of which require stakeholder participation in the form of government action. In Canada, the Office of the Privacy Commissioner (OPC) and the Treasury Board are PIA policy subjects that not only understand the role of PIA in promoting national development goals but also implement relevant policies.

2.2.1 Office of the Privacy Commissioner (OPC) The OPC not only provides advice and information to individuals on personal information protection but also enforces the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). These two federal privacy laws stipulate the rules that federal government agencies and certain enterprises must follow when handling personal information [19]. For example, the *Privacy Act* covers how the federal government handles personal information; PIPEDA is Canada's private sector privacy law covering how enterprises handle personal information. Under the *Privacy Act* [10], the Privacy Commissioner of Canada has the authority to inspect how government agencies subject to the Act collect, use, disclose, retain, and dispose of personal information. Thus, the Privacy Commissioner is a core figure in implementing legislative privacy requirements, responsible for protecting and promoting privacy rights of individuals in Canada. To ensure a comprehensive and up-to-date understanding of the privacy impacts inherent in proposed or redesigned programs and services, OPC representatives also participate in the earliest development stages of PPIAs or PIAs. By reviewing documents in collaboration with agency officials, they can provide advice and guidance to agencies and identify solutions aimed at addressing potential privacy risks. After receiving the final PIA, the Privacy Commissioner may, at his discretion, provide advice to agency heads or deputy heads [5]. To promote PIA policy, the Privacy Commissioner of Canada or his staff have delivered a series of speeches on PIA, as shown in Table 2 .

2.2.2 Treasury Board The key subject for conducting PIAs of public institutions is the Treasury Board. Although federal legislation does not explicitly require privacy impact assessments, they are considered best practices for

achieving compliance with privacy legislation requirements. As described in Section 1 above, based on this, the Treasury Board has developed a series of policy instruments and documents, including PIA Policy, PIA Guidelines, PIA Report Template, PIA Best Practices Report, PIA E-learning Tool, and PIA Audit Guidelines. The policy responsibility for implementing PIAs lies with central agencies, namely the Treasury Board Secretariat of Canada (TBS). The Treasury Board Secretariat not only advises the Treasury Board and provides recommendations on how the government spends money on programs and services, how it regulates, and how it manages, but also helps ensure that the government spends taxpayers' money wisely and effectively for Canadians [28]. The Treasury Board Secretariat has 18 subordinate departments, and the central agency responsible for government privacy policy is the Information and Privacy Policy Division under the Chief Information Officer of Canada, which is responsible for managing and interpreting policies and providing advice to various agencies, the President of the Treasury Board, and the Treasury Board.

The task is to develop and maintain guidelines to assist agencies in implementing the policy and to monitor compliance. According to Article 7 of the *Financial Administration Act* (Duties and Powers of the Treasury Board) [29] and Article 71(1)(d) of the *Privacy Act*, the President of the Treasury Board is the minister responsible for the administration of government legislation. As the lead agency, the Treasury Board Secretariat cooperates with the Department of Justice on legislative amendments and with the Privy Council Office on cabinet confidential matters.

2.3 Policy Content

2.3.1 PIA Guiding Principles According to the *Interim Directive on Privacy Impact Assessment*, PIA guiding principles include 10 articles, commonly referred to as "Fair Information Principles" (see Table 3), which are articulated in the *Canadian Standards Association Model Code for the Protection of Personal Information*. These principles are also included in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

2.3.2 PIA Process The *PIA Guidelines: A Framework to Manage Privacy Risks* [6] has three annexes providing PIA directories, PPIA directories, and summary table examples. PIA includes four steps: Project initiation. Determine the scope of the PIA and adapt the tools provided in the guidelines to specific circumstances. If the specific project is in the early concept or design stage and detailed information is not yet clear, departments and agencies should consider conducting a Preliminary Privacy Impact Assessment (PPIA). Once the project develops and privacy risks exist, departments and agencies are required to conduct a complete PIA. A preliminary PIA may also be conducted in unusual cases where, after reviewing policies and guidelines and obtaining expert advice, the need for a PIA remains unclear. PIA is a dynamic process that should be reviewed and updated as designs in business processes change.

Data flow analysis. This activity includes describing and analyzing the business processes, architectures, and detailed data flows under consideration in the proposal. The purpose of this step is to describe personal information flows. Privacy analysis. Privacy analysis examines data flows in the context of applicable privacy policies and regulations. Questionnaires can be used as checklists to help assessment subjects identify major privacy risks or vulnerabilities associated with proposed programs. The guidelines provide two sets of questionnaires, referring to federal programs and services in Annex A, and cross-jurisdictional initiatives in Annex B. Privacy impact analysis report. Based on the results of previous steps, this is the final and most critical component of the PIA process. This is a written assessment of privacy risks and their associated assessments, and discusses possible remedial or mitigation strategies.

Later, the revised *Expectations: A Guide for Submitting PIAs to the Office of the Privacy Commissioner of Canada* in March 2020 updated the PIA process (see Figure 2 [Figure 2: see original paper]), including: confirming whether a PIA is needed; planning; consultation (including OPC); assessing necessity and proportionality; identifying and assessing specific risks; developing mitigation measures; obtaining approval; reporting to the Treasury Board Secretariat (TBS) and the Office of the Privacy Commissioner (OPC); and continuous monitoring.

2.3.3 PIA Applicability Figure 2 [Figure 2: see original paper] can help assessment subjects determine the potential privacy impacts of a program or activity and understand the risk level. Based on this assessment, agencies may choose to conduct a PIA even if personal information is not used for management purposes. Agencies should consider each program individually to decide whether a PIA is required.

Additionally, according to Article 6.3.1 of the *Interim Directive on PIA*, a PIA must be conducted for a program or activity when: personal information is used or intended to be used as part of a decision-making process that directly affects individuals; personal information is used or intended to be used for administrative purposes after substantial modification to an existing program or activity; or a program or activity is outsourced or transferred to another level of government or the private sector, resulting in substantial modification to the program or activity. Furthermore, Article 6.3.2 of the *Interim Directive on PIA* also stipulates that consultation with responsible officials is required to determine whether a new or substantially modified information processing plan or activity has privacy implications and to ensure that a PIA is conducted; the government agency's privacy agreement is sufficient to address the potential privacy impacts of such procedures or activities. Thus, the above five situations require consideration of conducting a PIA.

2.3.4 PIA Regulatory Objects At the central government level in Canada, the Treasury Board's policy requires all departments and agencies to conduct

PIAs for all new program and service proposals involving privacy issues. The policy applies to all government agencies listed in the schedule of the *Privacy Act*, except the Bank of Canada. Specifically, these agencies include Canadian national departments and ministries, as well as a series of government-related institutions, including most Crown corporations (such as Canada Lands Company, Canada Post Corporation, Telefilm Canada), federal agencies (such as Canadian Transportation Agency, Canada Revenue Agency), and other institutions wholly or partially appointed by the government (such as the Canadian Wheat Board).

3. Analysis of Canada's Central Government PIA Policy

3.1 Advantage Analysis

3.1.1 Improving Policies and Regulations to Strengthen Application
In Canada, PIA is a policy requirement, not a legal obligation. Therefore, Canada focuses on providing legal basis for PIA and enhancing PIA policy effectiveness through improving laws and regulations. For example, according to Article 3.4 of the *Interim Directive on PIA*, this directive is issued under paragraphs 71(1)(d) and sections 71(3), 71(4), 71(5), and 71(6) of the *Privacy Act*; according to Article 3.5, this directive should be read together with the *Privacy Act*, *Privacy Regulations*, *Interim Policy on Privacy Protection*, *Interim Directive on Privacy Practices*, *Directive on Privacy Requests and Correction of Personal Information* [31], and the *Directive on Social Insurance Number* [32]. To enhance legal support, the Treasury Board Secretariat also initiates and promotes consultations with the OPC on PIA policy matters. For example, PIPEDA does not mandate PIAs. Similarly, generally speaking, unless there is a data or information matching program, New Zealand's *Privacy Act* also does not mandatorily require PIAs [33]. Therefore, on January 28, 2020, the OPC of Canada launched a consultation in which it proposed some recommendations for enhancing the application and regulation of PIPEDA in artificial intelligence systems. The OPC recommended increasing legal requirements for transparency to authorize PIA documentation requirements, including assessments related to the impact of AI processing on privacy and human rights [34].

3.1.2 Dedicated Responsibilities to Strengthen Regulatory Capacity
In Canada, the legal basis for PIA is ministerial-issued instruments, and relevant PIA policies are issued under Article 71(1) of the *Privacy Act*. Article 71(1) of the *Privacy Act* stipulates: The designated Minister shall cause to be prepared and distributed to government institutions directives and guidelines concerning the implementation of this Act and the regulations, subject to paragraph (2)(d). According to Article 3(1) of the *Privacy Act*, the President of the Treasury Board has been designated as the Minister referred to in certain sections of the Act. By optimizing the dedicated responsibilities of the Treasury Board, its responsibilities in control work in PIAs are further clarified. For example, the Treasury Board defines PIA as "the process of identifying the

impacts of proposals on personal privacy and ways to mitigate or avoid any adverse impacts." In addition, this institution also focuses on policy performance, such as the Treasury Board Secretariat conducting a comprehensive review of the terms and operation of the *PIA Policy* within 5 years after it takes effect [5]. Thus, the *PIA Policy* not only makes agencies responsible for proving that their collection and use of personal information respect the 1983 *Privacy Act* and the 2000 *Personal Information Protection and Electronic Documents Act* (PIPEDA), but also orders government agencies to communicate with citizens about why their personal information is collected, how it is used and disclosed, and how to address privacy impact issues.

3.1.3 Emphasis on Multi-Subject Cooperation Canada emphasizes cooperation. Articles 6.3.4, 6.3.5, 6.3.6, 6.3.7, and 6.3.8 of the *Interim Directive on PIA* regulate PIA situations involving multiple agencies: in cases involving programs executed by two or more government agencies, the directive favors a lead agency and envisions an inter-departmental coordination committee composed of key (government) stakeholders. It favors a single, holistic, or multi-agency program execution agency rather than independent program execution agencies by individual departments.

In terms of specific PIA operations, PIAs are reviewed by audit and compliance staff of the Office of the Privacy Commissioner of Canada, who do not approve or reject but provide comments on the quality of the process undertaken. Similarly, according to Article 8.1.1 of the *Interim Directive on PIA*, the Treasury Board Secretariat will also timely check the content of approved core PIAs to ensure assessments are completed. The Treasury Board Secretariat does not approve PIAs but only reviews core PIAs to fulfill its obligations for reviewing and approving PIBs. However, according to Article 8.1.4 of the *Interim Directive on PIA*, the Treasury Board Secretariat annually reviews the "core PIAs" in Annex C to ensure core PIAs remain relevant and proposes amendments when needed. The above shows that both the Office of the Privacy Commissioner and the Treasury Board Secretariat are responsible for reviewing PIAs but do not approve PIAs. To fill this responsibility gap, according to Article 6.1 of the *Interim Directive on PIA*, government agency heads are responsible for establishing PIA development and approval processes and ensuring that PIAs are completed by senior officials or executives in the agency responsible for new or substantially modified programs or activities. In addition, the *Interim Directive on PIA* links PIAs to project approval and funding submissions to the Treasury Board, which is also one of the most significant features of Canada's PIA policy.

3.2 Disadvantage Analysis

Public policy has subjectivity and uncertainty. PIA policy is designed by policymakers to achieve their goals through the actions of relevant departments, so the success of this policy depends on PIA policy design and implementation.

The ambiguity of PIA policy not only limits objectives but also affects policy instruments. Overall, Canada's PIA policy has ambiguity in objectives, norms, and implementation.

3.2.1 Ambiguous PIA Policy Objective Setting Due to concerns about the impact and costs of future privacy issues in government service delivery processes, the Treasury Board was tasked with developing the *PIA Policy* as a management tool: ensuring privacy is considered in the design or redesign of programs or services; assessments will determine the extent to which proposals comply with all appropriate regulations; assessments help managers and decision-makers avoid or mitigate privacy risks and promote fully informed policy, program, and system design choices [5]. Similarly, according to Annex C of the *Interim Directive on PIA*, the "core PIA" consists of standardized elements of PIA directly related to policy and legal compliance. This could be interpreted as PIA being merely a compliance exercise, but this may be an unfair interpretation because, as described above, the directive regards PIA as part of risk management, where risks may arise even if programs comply with the law.

3.2.2 Ambiguous PIA Policy Norms Although Canada's PIA has the advantage of being mandatory for government agencies, guidelines on when and how to consult with stakeholders are unclear. Similarly, it is unclear why only summaries of PIAs are published on agency websites, rather than complete PIAs like the checklist function in the PIA policies of the UK and US, but users may want to view such checklists, especially for actions that only require yes/no responses, because approaches that "fool" the PIA concept in ways inconsistent with the actual needs of risk assessment. For example, various US government departments have established personal privacy protection guidelines from the perspective of standardized and instrumental management of PIA, analyzing the collection, storage, protection, sharing, and management of information in identifiable ways to ensure that system users and relevant organizations consciously incorporate personal privacy into the lifecycle management of a system [35].

3.2.3 Ambiguous PIA Policy Implementation Canada's PIA policy requires that Canadian departments and agencies must provide the Privacy Commissioner with copies of assessment results and publish summaries of assessment results in both English and French, and should consider regular publication and Internet publication. The government can adjust the information in these summaries to remove information that cannot be published under relevant legal provisions or that could make systems or security measures vulnerable. However, in practice, departments fail to meet requirements by not publishing PIA implementation results and the information quality of PIA reports.

There are many benefits: PIAs allow agencies to fully assess privacy risks in their information sharing plans; they lay the foundation for developing comprehensive and effective information protection policies while maximizing the

use of technology infrastructure and data sharing opportunities; PIAs help organizations review the intentions of proposed programs, identify and prevent expansion beyond the intended purpose of information collection, review and accept risks, develop policies, and identify positions in the organization responsible for handling personal information; they also create documentation to inform individuals, upon request, where and when their personal information is collected, used, and disclosed. On the other hand, policymakers need to comprehensively identify PIA policy stakeholders such as data controllers and data users, thereby formulating PIA policies that meet fairness and justice and enhancing policy subjects' support for and identification with PIA policy. This is because, as a policy, PIA policy involves different stakeholders, which will seek their own interests based on their own characteristics, and different stakeholders may gain benefits but may also suffer corresponding losses.

4. Relevant Policy Recommendations

4.1 Improving Skills of Policy Implementers

PIA is a technology that can be used by any agency handling personal information, especially government, because the technology sector is more suitable for government. Conducting assessments and completing privacy impact reports requires various skills, but one person does not need to master all skills. Assessors need not only good analytical and writing skills but also familiarity with information privacy and data protection methods. If individuals do not have relevant technical skills or experience, assessors need to be able to absorb paperwork related to the project and be able to get along with technical personnel, ask relevant questions, understand answers, and translate them into PIA reports that others can understand. For an organization, an inquisitive mind and the ability to think "laterally" are valuable. Thus, to improve PIA policy implementation, the following aspects can be addressed: Agencies should recruit subjects skilled in: policy formulation, operational planning and business design, technical and professional knowledge, risk and compliance analysis, procedures and law. To reduce the "PIA skills gap" among policy implementers, it is recommended to encourage departments to share PIA tools, templates, and frameworks. It is recommended to provide more training and guidance to policy implementers to make them aware of their responsibilities in PIA policy and provide them with the knowledge and skills needed to conduct PIAs. The process includes planning, analysis, and educational activities, as well as multiple skills to identify and assess privacy impacts. These skills include privacy expertise, legal expertise, business solution and business design skills, technical and system expertise, and information and record-keeping skills.

4.2 Formulating PIA Policies as Early as Possible

Whenever there is a new or substantially changed e-government project, organizations should complete project impact assessments. PIAs are most useful when conducted early in project development because they can be used during

the design phase to identify risks and address privacy issues. Organizations that delay PIAs risk having to make expensive and time-consuming changes to programs to ensure compliance with personal privacy protection laws and regulations. PIAs enable public and private institutions to make wise choices. Typically, if privacy-enhancing solutions are identified early in project planning, the difficulty and cost of implementing them will not be higher than other solutions. PIAs show that considering privacy from the initial stage of system development and throughout the information lifecycle (i.e., collection, use, retention, processing, disclosure, and destruction) ensures privacy protection is embedded in systems from the beginning rather than as an afterthought, which could be much more costly or could affect project feasibility.

In recent years, as personal information leakage incidents have erupted frequently, China has begun to continuously design personal privacy protection systems. On May 25, 2020, the work report of the Standing Committee of the National People's Congress pointed out in its next-step work arrangements that this year it will formulate a personal information protection law and a data security law around national security and social governance [36]. On May 28, 2020, the Third Session of the Thirteenth National People's Congress passed the "Personal Information Protection" chapter in the Personality Rights section of the *Civil Code of the People's Republic of China*, summarizing China's existing legislative experience (such as the *Cybersecurity Law*) and academic consensus to establish basic rules for privacy rights and personal information protection [37]. On July 22, 2020, the Supreme People's Court and the National Development and Reform Commission jointly issued the *Opinions on Providing Judicial Services and Guarantees for Accelerating the Improvement of the Socialist Market Economic System in the New Era*, clearly stating the need to strengthen data rights and personal information security protection, legally protect data collection, use, transactions, and resulting intellectual achievements, and improve the data protection legal system [38]. On October 13, 2020, the much-anticipated draft personal information protection law was submitted to the 22nd meeting of the Standing Committee of the Thirteenth National People's Congress for review, stipulating pre-risk assessments for high-risk processing activities such as processing sensitive personal information [39]. The *Information Security Technology - Personal Information Security Impact Assessment Guidelines* states that it is a supporting standard for the *Personal Information Security Specification*, drawing on the latest legal provisions, institutional designs, and practical approaches in the United States, Europe, and other countries and regions regarding personal information security impact assessment (internationally known as Privacy Impact Assessment (PIA)), and proposes scientific, effective, and implementation-guiding personal information security impact assessment guidelines based on domestic existing legislation, administrative regulations, and standard requirements [40]. Even so, this document is not mandatory, so it is recommended that China further improve PIA-related norms in the *Personal Information Protection Law* or *Data Security Law*. In terms of policy content, it should include applicability, regulatory objects, privacy risk assessment mod-

els, and prior consultation obligations; in terms of policy formulation subjects, it should absorb policy actors such as the People's Congress, government, and citizens to determine the PIA obligations of data controllers.

4.3 Strengthening Identification with PIA Policy

Although the main purpose of Canada's PIA policy is to ensure privacy protection is a key consideration in the initial framework of program objectives and activities, even in some cases where there is evidence that program or service delivery may generate privacy issues, PIAs may still not be completed at all. While privacy issues are clearly evident in threat and risk analysis of government IT projects, privacy protection considerations are much less for projects involving inter-agency and cross-regional personal information flows. Some Canadian government agencies have actively worked to implement PIA policy, but more efforts are needed to ensure the policy achieves its intended effect, that is, to improve awareness and understanding of privacy impacts related to projects and service delivery in PIA policy. Therefore, on the one hand, there is a need to improve awareness of PIA. Cognition belongs to the spiritual level and can effectively predict satisfaction and identification. By improving awareness of PIA policy, beliefs are formed through relevant value assessments, which directly affect identification with PIA policy. For specific agencies, improving awareness of PIA policy can thus form beliefs through relevant value assessments that directly affect identification with PIA policy.

References

[1] Xiang Liling, Zhang Xuanyu. Comparison of Chinese and Foreign User Privacy Impact Assessment Standards [J/OL]. Information Studies: Theory & Application. [2021-06-27]. https://kns.cnki.net/kcms/detail/11.1762.G3.20210301.1633.004.tml. [2] Cui Congcong, Xu Zhixin. Data Protection Impact Assessment System: EU Legislation and Chinese Solutions [J]. Library and Information Service, 2020, 64(5): 43-51. [3] Chen Chaobing, Hao Wenqiang. Privacy Impact Assessment as a Government Tool: Origin, Value, Implementation, and Implications [J]. Chinese Public Administration, 2020(2): 144-151. [4] Annual report to parliament 1999-2000 [EB/OL]. [2021-06-27]. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_{index}/02_{{{04}}{{08}}}/. *[5] Privacy impact assessment policy [EB/OL]. [2021-06-27]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450. [6] Treasury board of canada secretariat. Privacy impact assessment guidelines: a framework to manage privacy risks [EB/OL]. [2021-06-27]. http://www.tbs-sct.gc.ca/pubs*{pol}/ciopubs/pia-pefr/paipg-pefrld-PR-eng.asp?printable=True. [7] Treasury board of canada secretariat. Preliminary privacy impact assessment template [EB/OL]. [2020-07-07]. http://www.tbs-sct.gc.ca/pgol-pged/ppia-efpvp/prelim-temp-modl/prelim-temp-modl00-eng.asp. [8] Treasury board of canada secretariat. Report on pia best practices [EB/OL]. [2020-07-14]. http://www.tbs-sct.gc.ca/pubs_{pol}/gospubs/TBM_{128}/dwld/chap1_{1_e}.rtf. [9] Trea-

sury board of canada secretariat. PIA e-learning tool [EB/OL]. [2020-07-26]. http://www.tbs-sct.gc.ca/pol/pged/piatp-pfefvp/index-eng.asp. [10] Privacy act [EB/OL]. [2020-08-12]. https://laws-lois.justice.gc.ca/PDF/P-21.pdf. [11] Personal information protection and electronic documents act (pipeda) (canada) [EB/OL]. [2020-08-14]. http://laws.justice.gc.ca/en/showdoc/cs/P-8.6//20090821/en?command=search&caller=SI&search_{type}=all&shorttitle=Personal%20information%20p
[12] Treasury Board of Canada Secretariat. Privacy impact assessment audit guide [EB/OL]. [2020-09-14]. http://www.collections-canada.gc.ca/. [13] Privacy and data protection policy [EB/OL]. [2020-10-11]. https://www.tbs-sct.gc.ca/pubs{pol}/gospubs/TBM_{128}/dwld/chap1_{1_e}.rtf. [14] Privacy regulations [EB/OL]. [2020-10-24]. https://laws-lois.justice.gc.ca/eng/regulations/SOR-83-508/index.html. [15] Directive on privacy impact assessment [EB/OL]. [2020-11-14]. http://www.rogerclarke.com/DV/TBC-2010.pdf. [16] Interim policy on privacy protection [EB/OL]. [2020-11-14]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510. [17] Interim directive on privacy practices [EB/OL]. [2020-11-24]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309. [18] Expectations: opc's guide to the privacy impact assessment process [EB/OL]. [2020-01-14]. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_{{{exp}}*{{202003}}}/#toc4-9. [19] Office of the privacy commissioner of Canada [EB/OL]. [2020-10-13]. https://www.priv.gc.ca/en/. [20] Privacy impact assessment [EB/OL]. [2020-10-06]. https://www.priv.gc.ca/en/opc-news/speeches/02*{05}a_{020508}/. [21] The role of the privacy impact assessment [EB/OL]. [2020-10-11]. https://www.priv.gc.ca/en/opc-news/speeches/2004/sp-d_{040310}/. [22] The privacy impact assessment: your gps through the new landscape of privacy protection [EB/OL]. [2020-10-24]. https://www.priv.gc.ca/en/opc-news/speeches/2011/sp-d_{{{20110928}}*{{cb}}}/. *[23] Facing the breach: privacy and security as an ecosystem [EB/OL]. [2020-04-04]. https://www.priv.gc.ca/en/opc-news/speeches/2013/sp-d*{{{20130618}}*{{cb}}}/. *[24] A risk based approach for accountability and compliance [EB/OL]. [2020-04-15]. https://www.priv.gc.ca/en/opc-news/speeches/2013/sp-d*{{{20130926}}*{{cb}}}/. *[25] Working together as privacy champions [EB/OL]. [2020-04-26]. https://www.priv.gc.ca/en/opc-news/speeches/2014/sp-d*{20141210}/. [26] The interconnected worlds of privacy and cyber-security [EB/OL]. [2020-05-04]. https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_{20160420}/. [27] Modernizing federal privacy laws to better protect canadians [EB/OL]. [2020-05-11]. https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_{20200309}/. [28] Treasury Board of Canada Secretariat [EB/OL]. [2020-05-19]. https://www.canada.ca/en/treasury-board-secretariat.html. [29] Financial administration act-laws.justice.gc.ca [EB/OL]. [2020-05-26]. https://laws-lois.justice.gc.ca/eng/acts/f-11/page-2.html#h-228122. [30] Personal information protection policy [EB/OL]. [2020-06-04]. https://www.ferocorp.com/pages/privacy.html. [31] Directive on privacy requests and correction of personal information [EB/OL]. [2020-07-23]. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18311. [32] Directive on social insurance number [EB/OL]. [2020-08-11]. https://www.tbs-sct.gc.ca/pol/doc-

eng.aspx?id=13342. [33] Chen Mei, Tan Weidong. Privacy Risk Assessment and Prevention of Government Open Data: New Zealand's Experience [J]. Information Studies: Theory & Application, 2020, 43(5): 110-114, 90. [34] Consultation on the opc's proposals for ensuring appropriate regulation of artificial intelligence [EB/OL]. [2020-09-18]. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_{{{ai}}*{{202001}}}/. *[35] Zhou Qingshan. Thoughts on Improving China's Personal Information Protection Management System [J]. Social Governance, 2018(1): 34-41. [36] Breaking news! Personal Information Protection Law and Data Security Law are finally coming! [EB/OL]. [2020-10-16]. https://k.sina.com.cn/article{{{1750987934}}*{{685df49e01900mvol}}}.html?from=news&subch=onews. [37] Privacy rights and personal information protection stipulated in the Civil Code [EB/OL]. [2020-10-17]. http://m.workercn.cn/wq/2020/0804/200804093628350.shtml. [38] Supreme Court and NDRC issue opinions: Strengthen data rights and personal information security protection [EB/OL]. [2020-10-18]. https://www.sohu.com/a/410614389*{741570}. [39] Draft Personal Information Protection Law of the People's Republic of China unveiled for the first time [EB/OL]. [2020-10-19]. https://www.sohu.com/a/424842464_{100014118}. [40] *Personal Information Security Impact Assessment Guidelines* (GB/T39335-2020) officially released [EB/OL]. [2021-06-05]. https://www.secrss.com/articles/27363.

Author Contributions: Chen Mei: Data collection and organization, writing and revising the paper; Liang Yikai: Literature research, data collection and organization.

Mengzhu, Wang Chuanqing **Phone:** (010) 82623933 **Postal Code:** 100190