Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

Privacy Implementation Notice 2023-03: Guidance pertaining to the collection, use, retention and disclosure of personal information that is publicly available online

Published: 2023-07-24

© His Majesty the King in Right of Canada,
as represented by the President of the Treasury Board, 2023,

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-77/2023E-PDF
ISBN: 978-0-660-67779-8

This document is available on the Government of Canada website at www.canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Avis de mise en œuvre sur la protection des renseignements personnels 2023-03 : Orientation relative à la collecte, à l'utilisation, à la conservation et à la divulgation de renseignements personnels accessibles au public en ligne

Privacy Implementation Notice 2023-03: Guidance pertaining to the collection, use, retention and disclosure of personal information that is publicly available online

1. Effective date

This implementation notice takes effect on August 1, 2023.

2. Authorities

This implementation notice is issued pursuant to paragraph 71(1)(d) of the *Privacy Act*.

3. Purpose

This implementation notice provides guidance in accordance with the requirements of the *Privacy Act* and related policy instruments to privacy officials in government institutions on the collection, use, disclosure, and retention of personal information that is publicly available online. This notice is also intended to serve as a shareable resource with program

areas, who may use this to guide their activities and develop their own internal policies and procedures. The guidance is meant to complement any existent institutional policies. While it does not address publicly available information from other sources, such as print or television, much of the information is applicable to other media.

4. Context

Government institutions collect, use, retain, and disclose, also known as manage, personal information that is publicly available online for various purposes, such as:

- outreach and public communications [1]
- research, examining trends and identifying emerging issues
- activities in support of national security, law enforcement and administrative investigations

5. Guidance

5.1 Existing requirements

If there is a serious possibility that an individual could be identified, alone or in combination with other information, this information may constitute personal information as defined in section 3 of the *Privacy Act*.

Personal information that is publicly available online should, in most instances, be treated the same way as any other personal information held by government institutions. The following are considerations specifically related to personal information that is available online.

5.1.1 Collection of personal information that is publicly available online

Authority to collect

As described in section 4 of the *Privacy Act*, personal information may only be collected if it relates directly to an operating program or activity. This requirement applies regardless of whether personal information is publicly available or not, and institutions must always ensure that they have the legal authority to collect the information before doing so. Legal authority for a program or activity is usually contained in an Act of Parliament or subsequent Regulations. Approval of expenditures proposed in the Estimates and authorization by an Appropriation Act can be an indication of legal authority for a program or activity.

Direct collection

When personal information is needed for an administrative purpose, direct collection is the default, except in specific circumstances. As described in subsection 5(3) of the *Privacy Act*, direct collection is not required if: the personal information is not used for an administrative purpose; it might result in the collection of inaccurate information; or, it would defeat the purpose or prejudice the use for which the information is collected. Additionally, consideration should be given to the exception in subsection 5(1) of the Act which states that collection need not be direct where the individual authorizes otherwise or where personal information may be disclosed to an institution under subsection 8(2). Before personal information that was obtained online is used for an administrative purpose, individuals to whom the information relates should be given the opportunity to review and correct it if necessary. This may not be appropriate in all cases; for instance, when the individual concerned is the subject of an active investigation. In cases when the institution would not consult with the concerned individual, they would still be bound by the

accuracy obligation defined in section 6(2) of the Act. For administrative decisions, it is not recommended to rely solely on personal information collected from publicly available online sources.

Limiting collection

Even when the personal information is publicly available online, institutions need to limit their collection of this information to what is directly related to and necessary for the government institution's programs or activities as prescribed in 4.2.9 of the *Directive on Privacy Practices*.

When manually collecting personal information from an online source, employees should assess each element of personal information collected to determine whether it meets those criteria. This may not be feasible in some cases where personal information elements are intertwined with others. Nonetheless, institutions should limit their collection to those specific elements.

When using automated methods of collection [2], institutions should consult their departmental privacy officials for advice on how to adjust the software's collection parameters to limit collection to only those elements that are necessary for the program or activity. This reduces the likelihood of overcollection. In the case of overcollection, institutions should engage their privacy officials to assess any potential impacts on the institution or the individual(s) concerned and implement appropriate mitigation measures, which may include disposing of the extraneous information.

As a general rule, personal information disclosed online by inadvertence, leak, hack or theft should not be considered publicly available as the disclosure, by its very nature, would have occurred without the knowledge or consent of the individual to whom the personal information pertains;

thereby intruding upon a reasonable expectation of privacy. Institutions should engage their legal services if they suspect the personal information they are considering collecting meets this scenario.

Presence of a Personal Information Bank

Institutions must identify the elements of personal information they collect from publicly available online sources in a Personal Information Bank (PIB) if that information is intended for an administrative use or if that information is organized in a manner to be retrieved by the name of an individual or an assigned identifying number or symbol. When personal information is used in support of communications activities, institutions may be able to rely on the following standard PIBs: PSU 938 (Outreach Activities) and PSU 914 (Public Communications). If personal information that is publicly available is collected for a new use or if a program or activity requires new personal information elements to be collected, it may be necessary to register or update an institution-specific PIB which better reflects the elements of information collected, the purpose of collection, and the retention period.

Notice of collection

Individuals should be notified if their personal information will be collected in support of an administrative decision that directly affects them unless notification could result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected. This requirement continues to apply to personal information that is publicly available online. Institutions should consult section 4.2.10 of the *Directive on Privacy Practices* for the elements that must be included in a Privacy Notice Statement.

When personal information that is publicly available online is collected indirectly for non-administrative purposes, institutions can indirectly notify individuals of the collection by way of notices posted on the institutions' websites or social media accounts. The notice provides transparency for online users to understand how the institution collects and uses personal information that is publicly available online in support of its mandate and allows individuals the opportunity to request access to their collected information. To ensure a broader reach, institutions are encouraged to employ additional measures of transparency whenever possible.

Use of third-party service or data providers

While private sector organizations are subject to their own obligations with respect to the collection, use and disclosure of personal information under *Personal Information Protection and Electronic Documents Act* and provincial privacy laws, federal government institutions retain ultimate responsibility, under the *Privacy Act*, when employing third-party service or data providers for the management of personal information that is publicly available online. These responsibilities, outlined in this notice, continue to apply when obtaining personal information from third parties by request, subscription or purchase. Contracts, agreements or arrangements established with third-party service or data providers should clearly outline measures to protect personal information in accordance with the requirements of the *Privacy Act* and related policy instruments, including a requirement to immediately notify the government institution of a privacy breach should one occur.

When employing a third-party service or data provider, institutions must take care to ensure that they have legitimately and legally obtained the personal information that will be provided to the institution. Additionally, while not a requirement, institutions are encouraged to also consider the

third party's history of privacy-related incidents. For additional guidance on engaging third parties, consider Guidance Document: Taking Privacy into Account Before Making Contracting Decisions.

5.1.2 Use and disclosure

As per 69(2) of the *Privacy Act*, personal information that is publicly available is not subject to the use and disclosure restrictions set out in sections 7 and 8 of the *Privacy Act*. However, as soon as personal information ceases to be publicly available, it becomes subject to the use and disclosure requirements of section 7 and 8. This means that institutions can no longer, without the consent of the individual to whom the information relates, use the personal information except for the purpose for which the information was originally obtained or for a use consistent with that purpose. Program officials will need to assess how available the information is to the public at the time of intended disclosure. This includes verifying, where possible, if the information to be disclosed is **identical** to that which is in the public domain at the exact time of disclosure. Moreover, Privacy Notice Statements should be updated to include the additional uses of the collected information, especially if the new uses differ significantly from what was described in the initial notice. Finally, institutions should meet the requirements set out in the *Directive on Privacy Practices* with respect to ensuring the accuracy of the information and establishing safeguards for its use and disclosure as well as its retention.

Verifying accuracy

As required by the *Privacy Act*, institutions must ensure that personal information collected for administrative purposes is as accurate, up-to-date and complete as possible. This requirement applies to personal information

that is publicly available online when used in a decision-making process. As a starting point, collecting personal information directly from the individual to whom it relates decreases the likelihood of inaccuracies.

The *Directive on Privacy Practices* expands on the Act's accuracy obligation to also require institutions to document the source or technique used to validate the accuracy of the personal information and identify these in the description of the relevant Personal Information Bank. This can be particularly challenging in the digital realm, given the increase of misinformation. To mitigate associated risks, institutions should consult multiple sources when collecting personal information from an online source, especially when the personal information does not originate from the individual to whom the information relates. Institutions should establish a process to determine confidence levels related to the information's accuracy, attributability and truthfulness. This may involve verifying the information through other sources or directly with the individual concerned. Regardless of confidence levels, personal information obtained from a publicly available online source should not generally be used on its own for an administrative purpose. When personal information is collected for a non-administrative use, such as observing online trends and narratives, institutions should ensure the information is as accurate as necessary for that specific purpose.

Safeguards

The public online availability of personal information does not exempt institutions from obligations related to safeguarding it. This is particularly salient in situations where publicly available personal information is combined to create a potentially expanded profile. Even when personal information is publicly available online, and it can be used for purposes beyond which it was originally collected, institutions should limit its access

to individuals who need it to perform functions or duties related to a program or activity. Administrative, technical and physical safeguards should continue to be used to protect the information. Additionally, as required by the *Policy on Privacy Protection* (see 4.2.1), employees must be made aware of policies, procedures and legal requirements under the *Privacy Act* before being allowed access to any personal information that has been collected, even when the information is widely available online. In addition, much like with any other personal information, institutions should put in place appropriate measures to ensure that access to the personal information is monitored and documented to allow for accountability.

5.1.3 Retention

As required under paragraph 4(1)(a) of the *Privacy Regulations*, all personal information used for an administrative purpose, whether obtained from publicly available online sources or not, must be retained for a minimum of two years. This retention period enables individuals to exercise their right of access under the *Privacy Act*. Subject to other legal or policy obligations, personal information used for non-administrative purposes should be disposed of as soon as it is no longer required by the program or activity. Institutions should review the information regularly and determine if continued retention is required. In all cases, clear retention periods, coupled with robust access controls and audit trails, can help mitigate privacy risks. Additionally, when retaining personal information obtained from a publicly available online source, institutions should consider labelling the information as “publicly available online,” and noting the date and source of collection. This can help ensure that any future uses of the information will consider its source and treat it accordingly.

5.2 Additional legal obligations

There is a risk that the collection of personal information that is publicly available online could engage legal requirements beyond those of the *Privacy Act*. For example, some institutions are subject to special rules set out in departmental legislation and policies uniquely applicable to them, and all institutions must comply with the *Canadian Charter of Rights and Freedoms*. Institutions should consult their legal services to determine the extent to which their practices with personal information may implicate legal requirements that apply and develop appropriate compliance measures.

Furthermore, it is important to note that, although the terms and conditions and/or end-user licence agreements of social media platforms or other online sources differ, some prohibit an institution from collecting publicly available personal information for certain purposes. An individual who views or collects content from these platforms, including personal information, can be deemed to have accepted the respective platform's conditions of use, even where registration or login is bypassed or not required to access the content.

Some of the conditions of use of certain platforms explicitly prohibit the use of their content by anyone associated with or acting on behalf of a government entity, and it may even specifically bar actions relating to surveillance or the gathering of intelligence. Thus, consider the conditions of use prior to the collection. Institutions should work with their legal services to undertake a detailed examination of any proposed collection activity in conjunction with the specific conditions of use associated with each platform to be engaged. Institutions are encouraged to update this assessment overtime as conditions of use change. Institutions' legal services can also support institutions in identifying other legal risks

involved, including potential copyright infringement caused by unauthorized copying of the platform's content or when other risks triggered by circumventing technological protection measures.

5.3 Measures to protect privacy

This section will discuss practices which can help safeguard privacy when managing personal information that is publicly available online.

Authorizing a collection

Developing a process for authorizing a collection and clarifying subsequent permissible uses can be a useful safeguard to manage privacy risks. Collecting personal information from online sources involves different degrees of privacy invasiveness. This depends on the extent and methods of collection, the privacy features of the specific platform where the search and collection occur, as well as users' reasonable expectation of privacy in that specific digital space. Institutions are encouraged to develop a clear process for authorizing the collection of personal information that is publicly available online which specifies the authorization level (for example, Manager / Supervisor, Director, Director General) required, that relates to the degree of invasiveness of the collection.

Assessing privacy implications

A Privacy Impact Assessment is required in accordance with the *Directive on Privacy Impact Assessment* when the collection of personal information is for an administrative purpose, including any personal information that is publicly available online. In a non-administrative context, such as collecting social media data solely to observe online trends or narratives, a privacy protocol should be established as per 4.2.5 of the *Policy on Privacy Protection*. A Privacy Impact Assessment may also be warranted for

programs or activities which collect personal information from publicly available online sources for a non-administrative purpose, but where the extent or nature of the collection may heighten privacy concerns. Program officials should work with their institution's privacy officials, often located within the Access to Information and Privacy (ATIP) office, to determine which tool should be used to appropriately identify the privacy risks, and the commensurate mitigation measures.

Privacy preserving techniques

When processing publicly available personal information obtained online, institutions should consider using privacy preserving techniques, such as de-identification and data minimization. These measures can assist in the protection of personal information while engaging in communications and outreach activities, as well as research and analysis. For further information, institutions may wish to consult the Privacy Implementation Notice 2023-01: De-identification and the Privacy Implementation Notice 2020-03: Protecting privacy when releasing information about a small number of individuals.

Internal policies

Internal policies at the program level, designed in consultation with the institution's privacy officials, are another important measure that can help reduce privacy risks when collecting personal information from publicly available online sources. An internal policy might include the following core elements:

- a list of activities for which the use of personal information obtained from publicly available online sources are and are not authorized
- an authorization process for collection

- any limitations on collection to minimize privacy risks, ideally considering not only what is legally permissible, but also what is conducive to fostering public trust
- the tools and methods used to collect the information
- the procedures used to note the source and date of the collection
- the operational measures needed to ensure compliance with applicable laws and policies, especially with regard to accuracy and overcollection

Use of attributable versus non-attributable accounts

When obtaining personal information from publicly available online sources, employees should use accounts attributable to their institutions. Please see the Privacy Implementation Notice 2021-01: Privacy Requirements for Official Social Media Accounts for more information.

Non-attributable accounts should only be used by institutions with specific investigative or intelligence collection mandates, as established in their enabling legislation. It is recommended that institutions consult with their legal services prior to using non-attributable accounts as the regulatory regimes to which they are subject may have transparency requirements. If non-attributable accounts are used, institutions should engage in the following best practices:

- avoid the use of any identifying information, such as a photo of a randomly selected individual found online as the account's profile picture; [3] instead, institutions should rely on synthetic information
- restrict access to these accounts to specific employees who have a clear business need to use them. Ensure that the creation of these accounts is documented and approved at the appropriate levels and in consultation with the institution's privacy officials and legal services
- review the necessity of maintaining these accounts on a regular and case-by-case basis

- ensure that non-attributable accounts are associated with a specific employee and deleted at the employee's departure if they are no longer necessary

6. Application

This implementation notice applies to the government institutions as defined in section 3 of the *Privacy Act*, including parent Crown corporations and any wholly owned subsidiary of these corporations. However, this notice does not apply to the Bank of Canada.

7. References

Legislation

- *Access to Information Act*
- *Canadian Security Intelligence Service Act*
- *Canadian Charter of Rights and Freedoms*
- *Communications Security Establishment Act*
- *Criminal Code*
- *Personal Information Protection and Electronic Documents Act*
- *Privacy Act*

Related Treasury Board policy instruments and guidance

- *Directive on Privacy Impact Assessment*
- *Directive on Privacy Practices*
- *Guidance on Preparing Information Sharing Agreements Involving Personal Information*
- *Guideline on Service and Digital*
- *Policy on Privacy Protection*

- *Policy on Service and Digital*
- Privacy Implementation Notice 2020-03: Protecting privacy when releasing information about a small number of individuals
- Privacy Implementation Notice 2021-01: Privacy Requirements for Official Social Media Accounts
- Privacy Implementation Notice 2023-01: De-identification
- Guidance Document: Taking Privacy into Account Before Making Contracting Decisions

8. Enquiries

Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries at questions@tbs-sct.gc.ca for information about this implementation notice.

Employees of government institutions may contact their Access to Information and Privacy (ATIP) coordinator for information about this implementation notice.

ATIP coordinators may contact the Treasury Board of Canada Secretariat's Privacy and Responsible Data division at ippd-dpiprp@tbs-sct.gc.ca for information about this implementation notice.

Appendix A: definitions

administrative purpose
The use of personal information about an individual in a decision-making process that directly affects that individual (see section 3, *Privacy Act*). This includes, but is not limited to, all uses of personal information for confirming identity (that is, authentication and verification purposes) and for determining eligibility of individuals for government programs (see Appendix A, *Policy on Privacy Protection*).

material privacy breach

A privacy breach that could reasonably be expected to create a real risk of significant harm to an individual. Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property (see Appendix A, *Policy on Privacy Protection*).

non-administrative purpose

The use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistical, audit and evaluation purposes (see Appendix A, *Policy on Privacy Protection*).

personal information

Information about an identifiable individual that is recorded in any form (see section 3, *Privacy Act*).

privacy protocol

A set of documented procedures to be followed when using personal information for non-administrative purposes including research, statistical, audit and evaluation purposes. These procedures are to ensure that the individual's personal information is handled in a manner that is consistent with the principles of the Act (see Appendix A, *Policy on Privacy Protection*).

publicly available information

Information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. It does not include information in respect of which a Canadian or a person in Canada has a reasonable expectation of privacy (from the *Communications Security Establishment Act*).

1 See Annex A, Question 4, Privacy Implementation Notice 2021–01: Privacy Requirements for Official Social Media Accounts

2 Such as use of third-party providers with Application Programming Interface access to social media platforms or web scraping to collect information directly from websites or social media platforms.

3 Using the personal information of individuals to create a non-attributable account could violate sections 366 and 403 of the *Criminal Code*

© His Majesty the King in Right of Canada, as represented by the President of the Treasury Board, 2023

ISBN: 978-0-660-67779-8

Date modified:
2023-09-05