The CNSC's Presence on Twitter, a Microblogging Social Media Platform

Privacy impact assessment summary

Canadian Nuclear Safety Commission

Government Official Responsible for Privacy Impact Assessment

Sunni Locatelli
Director General
Strategic Communications Directorate

Head of the Government institution / Delegate for section 10 of the *Privacy Act*

Phil Dubuc
Senior ATIP Advisor

Description of program or activity

As part of the commitment to better connect with citizens and businesses, the Government of Canada (GC) is improving access to government services and information, and examining opportunities to streamline its Web presence (Economic Action Plan 2013). In this context, the GC's Web Renewal strategy aims to modernize online communication capabilities, in particular its use of websites and social media. The Web Renewal strategy also supports Canada's commitment to open government and enables greater information sharing, public dialogue and collaboration.

Twitter is a microblogging and social network platform that complements the current Facebook and YouTube platforms in use now by the CNSC. Twitter is a significant part of the CNSC's social media strategy as it will mainly be used to draw social media users to content hosted on the CNSC's website, Canada.ca, and content generated for the CNSC's Facebook page. Currently, the strategy does not call for original content for Twitter broadcast.

Twitter will be an additional resource to help meet the CNSC's mandate, which includes the dissemination of technical, regulatory and scientific information about the activities it regulates.

The CNSC has been posting original content to its Facebook and YouTube pages. The Twitter account will be used as a broadcast account to draw social media users back to the other platforms where original content will be posted. The Twitter account will also be used to broadcast Commission business in the form of links back to the home page where the content (such as decisions, presentations and discussion papers) can be found.

Description of the Class of Record and Personal Information Bank associated with the program or activity

Operational information that may be collected via the CNSC Twitter presence is not limited to any one specific program or activity for the CNSC and would be more closely compared to the CNSC's receipt of correspondence from the general public. As such, the CNSC will rely on two standard Classes of Records to reflect the operational information that this initiative is likely to generate:

PRN 939 Communications
PRN 904 Cooperation and Liaison

In the event that an individual chooses to provide specific program-related information using Twitter, other Classes of Records may be relevant. However, that will only be determined by the nature of information that users post.

The CNSC will rely on two standard Personal Information Banks to reflect the personal information:

PSU 914 Public Communications
PSU 938 Outreach Activities

Legal authority for program or activity

Nuclear Safety and Control Act, section 9(b)

Risk area identification and categorization

1. **Type of program or activity**

   The personal opinions or views that the CNSC's Twitter presence may collect are not intended to be used for administrative purposes (i.e., personal information is not expected to be used for the purpose of making decisions about an identifiable individual), except in exceptional circumstances. The social media platform is intended to disseminate information, to engage with individuals, to manage and moderate discussions, and to perform account analytics.

   Level of risk to privacy – 2

2. Type of personal information involved and context

The CNSC's Twitter presence involves the collection, use, disclosure and retention of personal information that is generally considered to be non-sensitive in nature. Moreover, personal information is intended to be collected directly from the individual. While the CNSC will not solicit sensitive personal information via Twitter, the Commission recognizes that the personal opinions reflected in an individual's tweets or responses to the CNSC's tweets may be considered sensitive in some contexts. Even though the receipt of personal information via Twitter is discouraged, there is still the possibility that an individual can tweet his or her personal information (or the personal information of others). Any information that would be referred to the CNSC areas responsible for compliance and regulation would not likely be personal, though it is recognized that this cannot be guaranteed by the CNSC.

Level of risk to privacy – 2

3. Program partners and private sector involvement

Twitter is a third-party private sector organization and, as such, both the CNSC and individuals will be governed first and foremost by Twitter's terms of service and privacy policies related to the collection, use, disclosure and retention of the information held within Twitter's platform. The use of private third-party platforms by the Government creates a risk that the use of those platforms may conflict with the personal information handling and privacy requirements of the *Privacy Act.* The CNSC is including privacy notice statements on CNSC Web pages that facilitate access to any social media platform to help ensure that users are aware that they are not on the CNSC website and help them protect their information.

Level of risk to privacy – 4

4. **Duration of the program or activity**

The CNSC's Twitter presence is intended to be a long-term initiative, without an established sunset date. The extended period over which the CNSC (and the Government in general) will maintain a presence on Twitter presents an elevated risk to an individual's privacy in that the longer the duration of the initiative, the more personal information federal institutions are likely to collect (individually and in aggregate).

Level of risk to privacy – 4

5. Program population

The CNSC does not intend to use any of the personal information collected via its Twitter presence for administrative purposes. As such, and despite expectations of significant use by social media users, the initiative is unlikely to present widespread risks to a large population of individuals.

Level of risk to privacy – 1

6. Technology and privacy

a. Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?

Risk to privacy – No

b. Is the new or modified program or activity a modification of an IT legacy system and/or service?

Risk to privacy – No

c. Enhanced identification methods: This includes biometric technology (e.g., facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID)) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e., identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip, or only a memory chip with non-programmable logic).

Risk to privacy – No

d. Use of surveillance: This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance/interception, computer-aided monitoring including audit trails, or satellite surveillance.

Risk to privacy – No

e. Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the *Directive on Privacy Impact Assessment*, government institutions are to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Risk to privacy – No

7. Personal information transmission

The reproduction, dissemination and circulation of personal information posted to Twitter is generally accepted as being difficult, if not impossible, to control. Information posted to the Internet not only becomes public; it may also become a matter of permanent record. Due to the high likelihood that information posted by an individual to a government-operated social account site may be transmitted beyond the Government's control, the privacy risks to the individual are considered to be relatively high.

Level of risk to privacy – 4

8. Risk impact in the event of a breach

Whereas personal information from official social media accounts is to be collected exclusively from publicly available sources (i.e., official social media accounts on selected platforms), the privacy impact on individuals in the event of a data breach by a federal institution is considered to be low. Information collected is to be limited to that required for common uses and is to be provided by individuals directly with their knowledge and consent. Privacy impacts on the individual may increase where personal information gathered by federal institutions from official social media accounts is used (without consent or authority) for secondary purposes and/or where it is disclosed or revealed in a context that is different from that in which it was first collected. This is not the intention of the CNSC.

Level of risk to privacy - 1