UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

25 June 2018

Owuor Okiro
Procurement Technical Analyst
owuor.okiro@neb-one.gc.ca
National Energy Board
517 Tenth Avenue S.W.
Calgary, Alberta
T2R 0A8

By email

cc: Peter Watson, Chair/CEO, peter.watson@neb-one.gc.ca
Lyne Mercier, Vice-Chair, lyne.mercier@neb-one.gc.ca
Alex Ross, Acting Executive Vice President, Law and General Counsel, alex.ross@neb-one.gc.ca
Sandy Lapointe, Executive Vice President, Regulatory and Acting Executive Vice President, Transparency and Strategic Engagement, sandy.lapointe@neb-one.gc.ca
Alexis Williamson, Vice President, People and Knowledge, alexis.williamson@neb-one.gc.ca
Mark Power, Vice President, Performance and Results and Chief Financial Officer, mark.power@neb-one.gc.ca

Dear Mr. Okiro:

I am writing on behalf of the Citizen Lab, an interdisciplinary research laboratory based at the Munk School of Global Affairs at the University of Toronto. Our work involves research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

This letter is with regard to the recent Request for Information for "Security Threat Monitoring Services" issued by the National Energy Board (RFI Process # 84084-18-0093). The RFI was brought to the Citizen Lab's attention through an article in *CBC News* entitled "NEB seeks contractor to monitor 'vast amounts' of online chatter for potential security threats," (Robson Fletcher, 21 June 2018). The RFI raises significant human rights concerns that we wish to bring to your attention. We are also seeking your clarification with regard to a number of questions related to the RFI, which we have detailed below.

As you are certainly aware, pipelines and energy development are pressing policy issues that impact all people in Canada. The decisions made by the Government of Canada and the National Energy Board have far-reaching impacts, ranging from climate change, health, migration, and economic policy to matters of sovereignty and global security. Energy policy and climate change also have particularly acute

impacts for Indigenous peoples, whose rights and territories are often directly at stake. The federal government's recent acquisition of the Trans Mountain Pipeline has made this conversation even more timely and urgent.

The *Charter of Rights and Freedoms* guarantees all persons in Canada certain fundamental rights and freedoms, including freedom of thought, belief, opinion and expression; freedom of association and assembly; and the right to be secure against unreasonable search or seizure—that is, the right to privacy. It also guarantees the right to equal and non-discriminatory treatment under the law. The National Energy Board's proposed RFI for "Security Threat Monitoring Services," as drafted, risks undermining these constitutionally protected rights.

The Citizen Lab has engaged extensively on cyber security, national security, and human rights threats in Canada, most recently on the technical aspects of Bill C-59 (*An Act respecting national security matters*). Our global research has also consistently demonstrated the ways in which technologies built to monitor, analyze, predict, profile, and surveil can be abused by both governments and the private sector alike. Civil society plays a uniquely critical function in democratic societies, but it is also uniquely vulnerable to these threats. The system proposed in the RFI, as drafted, is inherently oriented toward mass data collection and analysis, and will, by definition, have significant collateral impacts on the rights and interests of individuals who pose no security threat.

While security concerns related to critical infrastructure doubtlessly exist, energy policy is also an area of heightened and essential political engagement, which does not in and of itself amount to a security concern necessitating the measures described in the RFI. That engagement includes protest, critical speech, and civil disobedience on the part of Indigenous land and water defenders, environmental groups, human rights activists, the press, impacted communities, and others. Social media interactions and other online speech facilitate this engagement and are increasingly its primary vehicle. By targeting this expression, the technology and services sought in the RFI may have a serious chilling effect on these constitutionally protected voices, and unjustly infringe on the privacy rights of individuals engaged in legitimate, democratic expression and related activities. The RFI is particularly poised to disproprotionately impact Indigenous communities.

We also note that, the short window of opportunity to submit a response to the RFI—ten days in total—raises concerns that NEB planning in relation to this new mass monitoring capability is already at an advanced stage, and has perhaps already encompassed substantive discussions with potential or likely vendors. In addition, our research and experience with respect to the types of mass, targeted, algorithmic monitoring systems described in the RFI indicates that the concerns we raise below can never be asked early enough. We therefore consider the following questions and issues to be pressing.

We have the following questions with regard to the data, personal information, and online communications that the sought services will monitor and capture:

- What will the collected data be used for? What specific actions does the NEB expect it will take based on the data it acquires? What will collecting the data and information sought enable the NEB to do, that it cannot do now with its current systems and tools?

- Who will own the data that is collected by the third-party contractor? Will ownership remain with the contractor, be transferred to the NEB, or be jointly owned? Will terms to this effect be included in the contract?

- Will the data collected by the third-party contractor be shared with other parties outside of NEB and that contractor? Which parties would those be? Under what circumstances would this data be shared with them?

- If inferences and conclusions about any individuals, groups, or communities are drawn from the collected data, will those inferences or conclusions be shared with parties outside of the third-party contractor and the NEB? Who would that information be shared with, and under what circumstances? What if any safeguards are in place to ensure any information shared in this manner is not misused or mischaracterized?

- If inferences and conclusions about any individuals, groups, or communities are drawn from the collected information, how will the NEB ensure their accuracy and correctness?

- If inferences and conclusions about any individuals, groups, or communities are drawn from the collected information, how will the NEB ensure that such inferences or conclusions are not misused or abused—for example, as to engage in racial profiling or to target individuals engaged in *Charter*-protected activities?

- How does the NEB intend to differentiate between "threats" and activities that constitute an exercise of *Charter*-protected freedom of belief, opinion, expression, association, or assembly? How does the NEB intend to ensure that the provision of these services do not result in a chilling effect on legitimate democratic engagement and freedom of the press?

- Has the NEB begun to undertake a Privacy Impact Assessment regarding the anticipated program that this RFI seeks to realize, or otherwise interacted with the Office of the Privacy Commissioner of Canada regarding potential issues that might arise from the anticipated scope of these services?

- According to the RFI, the NEB expects the successful vendor to collect, process, analyze, and/or interpret, on the NEB's behalf, "vast amounts of traditional media, open source and public social media data in both English and French", including "[a]t least three (3) years of historical reports of incidents and activities impacting government and energy industry" and, as required, "vast amounts of data/information for forecasting issues or events that may increase security risks to the NEB".
    - How will the NEB ensure that these services do not inappropriately capture the private information of individuals whose online activities are subject to such monitoring and analysis?

- How will the NEB ensure that to the extent individuals' personal information is captured in the sought data, monitoring, plain language briefing reports, and forecasts, that it will be appropriately treated (whether removed, redacted, or secured)?
- How will the NEB ensure that to the extent individuals' personal information is captured in the sought data, monitoring, plain language briefing reports, and forecasts, such information will not be misused or abused to target particular individuals or groups, such as political activists?
- How will the NEB ensure that any captured personal information is stored securely? For how long will such information be retained? What are the NEB's, and the third-party vendor's, retention and destruction policies with respect to such captured personal information?

We have the following questions with regard to the procurement process:

- RFI Process #84084-18-0093 was published on June 19, 2018, with a closing date of June 29, 2018. Has your office taken part in any discussions with vendors concerning this RFI or any matter related to its contents, before the RFI was published?
  - If so, which vendors have you spoken with about the NEB's intention to procure these services? When did these discussions take place, and what was the nature of these conversations?

- To our understanding, the Directive on Departmental Security Management, which the NEB has cited as its purpose for seeking the services outlined in the RFI, had an implementation deadline of 2012. Why has the NEB chosen to seek such services now, as opposed to any other time in the intervening six years? What were the specific considerations that led to the NEB determining that there was a need for the kind of services sought in the RFI?

- Why is the NEB seeking services that would include the United States as a geographic area of focus, in addition to Canada?

- The RFI states that the sought service must include "[f]lexibility for end user to adjust geographic areas of focus…". What criteria would justify or prompt an end user to focus on a particular geographic area?

- In its RFI, the NEB cites the following objectives as part of its rationale for seeking algorithmic public monitoring services:
  - Identifying security threats, risks and vulnerabilities;
  - Ensuring protective measures are in place to safeguard employees, and any other attendees at NEB public activities, from workplace violence that could arise because of their respective work duties or participation; and
  - Ensuring measures are taken to ensure preparedness and timely mitigation, response or recovery from security incidents and to prevent or minimize effects and potential losses.

Are the NEB's current tools and systems inadequate to perform these tasks? What is the relationship between the NEB and existing law enforcement and security agencies in identifying and responding to threats related to the NEB's activities?

- Is this envisioned to be an "off-the-shelf" product to be installed and operated solely by NEB or will responding vendors play an ongoing role in the provision of the service, for example, through ongoing analysis, storage or remote access to data?

- Will the NEB place any conditions on a successful bid if it proceeds with procuring the services described in the RFI, in the way of corporate social responsibility and ensuring the protection of the human rights and civil liberties of the individuals and groups whose online activities will be subjected to the described monitoring, briefings, analysis, and interpretation?

Given the RFI's short timeline, the NEB's expressed intent to move forward with the next phase of this process immediately, and the urgent public interest in securing responses to these questions, we are eagerly awaiting your response.

Sincerely,

Ronald J. Deibert, OOnt.
Professor, Political Science Department, University of Toronto
Director, Citizen Lab, Munk School of Global Affairs, University of Toronto
Tel: (416) 946-8916 | r.deibert@utoronto.ca