Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Interview Summary: John McKay

John McKay, MP, was interviewed by Commission counsel on August 19, 2024.

Notes to Readers:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.

1. Background

[1] John McKay is the Member of Parliament ("**MP**") for Scarborough Guildwood. He was first elected as an MP in 1997. He is a member of the Liberal Party of Canada. He is currently the Chair of the House of Commons Standing Committee on National Defence and has previously served as Parliamentary Secretary to the Minister of National Defence and Opposition Critic for Defence. Prior to his election to Parliament, he worked as a lawyer.

2. Members' Offices and IT Services

[2] Mr. McKay discussed how MPs offices were organized and funded. Some expenses are funded directly by the House of Commons – such as MP's Ottawa office space – while other costs are covered by a budget assigned to each member.

[3] MPs procure all of their IT devices and services from the House of Commons. This includes internet services in both constituency and Ottawa offices. When MPs travel abroad, the House of Commons provides travel phones and provides advice on security "do's and don'ts".

[4] MPs and their staff have a number of standard email accounts provided by the House of Commons. This includes a public-facing general account, an account for Member's constituency office, accounts for member's staff, and a personal account for the MP.

[5] Mr. McKay discussed the different roles that MPs play, and how this impacts their use of IT systems. MPs perform both parliamentary and partisan work. Under House of Commons rules, MPs are not permitted to use House resources – including IT equipment – to engage in partisan activities.

[6] Mr. McKay's staff have separate electronic devices to use for partisan activities. Mr. McKay does not personally maintain a separate set of devices, but he does use a personal email account that is not provided by the House of Commons for his partisan activities.

[7] Mr. McKay indicated that he and his staff are careful to respect the rule against using House equipment for partisan activities. However, he noted that the line between parliamentary and partisan can sometimes be blurry, and that inevitably there are times where House equipment is inadvertently used for activities that could be viewed as partisan.

[8] The House of Commons provides IT support for the systems that it provides. Mr. McKay believes that this includes cyber security monitoring. Neither the House of Commons nor the Government of Canada provides support or cyber security services for his staff's non-House of Commons devices or systems.

3. The Interparliamentary Alliance on China (IPAC)

[9] The Interparliamentary Alliance on China ("**IPAC**") is a worldwide group of like-minded parliamentarians who are interested in China-related issues, such as the Taiwan, Hong Kong, and the Uyghur people. It is fundamentally a human rights group.

[10] IPAC organizes activities around the world, which can translate into action in national parliaments by its members. Mr. McKay provided an example of an initiative in the House of Commons that is being organized by Canadian IPAC members.

[11] In each country where it operates, IPAC has individual members, as well as national co-chairs, which are from different political parties. From Mr. McKay's perspective, there is not a significant difference between being a co-chair and a member of IPAC as

parliamentarians may have more or less involvement in the organization in either capacity.

[12] When IPAC was being organized around 2020, the main Canadians involved were Garnett Genuis [a Conservative Party of Canada MP] and Irwin Cotler [a former Liberal Party of Canada MP]. Mr. McKay was asked by Mr. Cotler to serve as a Canadian co-chair of IPAC along with Mr. Genuis. Mr. McKay agreed to do so. He had a background in working on human rights issues related to China, including serving as the Chair of the Canadian Taiwan Friendship Group and his involvement of combating slave labour in supply chains.

[13] Mr. McKay described Mr. Genuis and Mr. Cotler as more actively involved in IPAC's work than himself.

4. Cyber Attacks Conducted by Advanced Persistent Threat 31

[14] Mr. McKay discussed how he came to be aware of a cyber attack targeting him and other IPAC members.

[15] Some time around 24 April 2024, Mr. McKay had a phone call with Mr. Genuis and Luke de Pulford, the Executive Director of IPAC. Mr. de Pulford informed Mr. McKay and Mr. Genuis that some IPAC members had been targeted by a cyber attack conducted by an entity referred to as Advanced Persistent Threat 31 ("**APT31**"), including the two of them. Mr. De Pulford told Mr. McKay that APT31 was identified as being backed by the government of China and that the attack occurred in January 2021. IPAC had recently obtained this information from the United States Federal Bureau of Investigation ("**FBI**").

[16] During this phone call, Mr. du Pulford explained that APT31 conducted a "pixel reconnaissance attack", which used an email appearing to come from a news site to collect basic information about the recipient's computer system, such as IP address and operating system information. He also indicated that the House of Commons system was not penetrated.

[17] Mr. de Pulford also indicated that the FBI had informed the Governments of every impacted country – including Canada – in 2022 about the attacks. The Government of Canada had not notified Mr. McKay at that time, nor did the House of Commons.

[18] Mr. McKay was initially surprised to learn that he had been targeted by a China-affiliated entity. He had not previously given significant tought to cyber security issues or the possibility that he would be a target. However, as he thought more about it, he began to see why it would make sense for him to be a target: his advocacy on China-related matters, coupled with his role in defence matters, such as chairing the Standing Committee on National Defense could make him a subject of interest for China.

[19] A second phone call took place, later that day, to inform all of the impacted Canadian members of IPAC. Mr. McKay was not involved in that phone call, but he understood that Mr. de Pulford would be conveying the same information that he provided earlier in the day to Mr. McKay and Mr. Genuis.

[20] On 25 April 2024, Mr. McKay and other Canadian IPAC members received an email communication from Mr. de Pulford.[1] The email repeated the same information that Mr. McKay had received over the phone the day before.

[21] Some time in late April or early May, Mr. McKay had a discussion with the Speaker of the House of Commons about the cyber attack. Mr. McKay asked the Speaker why he and other IPAC members were not informed by the House of Commons about the cyber attacks. The Speaker indicated that the House of Commons IT systems were frequently targeted by cyber attacks. If MPs were notified of every such attack, there would be a constant stream of notifications.

[22] Canadian IPAC members wished to have a briefing with the FBI. This was arranged with the assistance of the IPAC Secretariat. It occurred in early May 2024. The FBI did not provide additional details about the APT31 cyber attack, but did discuss the scale of the cyber attack threat. The FBI indicated that it only had the resources to investigate a very small portion of the cyber attacks that it became aware of.

[1] COM0000485.

[23] Mr. McKay did not discuss the cyber attacks with the Sergeant-at-Arms, the Parliamentary Protective Service, the Prime Minister, CSIS, CSE or law enforcement.

[24] Mr. McKay was asked about his understanding of how Canadian officials came to be aware of the APT31 cyber attack. He indicated that he did not have firsthand knowledge, but understood that in 2022 the FBI contacted the Parliamentary Protective Service to inform them about the cyber attack. He noted that the information he received from IPAC indicated that the FBI also notified the Government of Canada. He was not aware of discussions between the House of Commons and the Government of Canada.

5. Reflections and Recommendations

[25] Mr. McKay viewed the cyber attacks in the wider context of increasing security threats facing MPs. Over the course of his parliamentary career, Mr. McKay has noted that the political environment has become increasingly toxic, and direct security threats to MPs have increased. This has been particularly true in the last five years. He views the spike in threats to MPs as corrosive for democracy.

[26] The cyber attacks targeting him, while different from the types of physical security threats that MPs frequently face, are another example of the increasingly difficult environment that MPs have to navigate. That said, Mr. McKay did not indicate that the cyber attacks themselves have had a significant impact on his parliamentary work.

[27] Mr. McKay was asked by Commission counsel how he assessed the performance of the House of Commons administration and the Government of Canada in responding to the cyber attacks. He indicated that he did not have enough personal knowledge to say whether they handled it well or poorly, though understood that the Parliamentary IT system was not compromised. He assumed that they handled the situation according to the protocols and processes that existed in 2022. He indicated that the more important question was whether those protocols or processes reflected the realities of 2024, including the question of when MPs should be notified that they have been targeted.

[28] He indicated that the threshold for when an MP should be notified that they are the target of foreign state activities is a complex one. If it is set too high, MPs may not be told important information and may remain vulnerable. If it is set too low, MPs may be notified of minor events – like the regular flow of cyber attacks targeting the Parliamentary system – which undermines the value of notification.

[29] He indicated that, while he had no easy answers, he believed that some consideration should be given to both the nature of the threat, as well as the nature of the target. As an example of the latter, he indicated that MPs in certain sensitive roles, such as membership in a security-sensitive committee, may need to be notified of threats at a lower threshold than others.

[30] Mr. McKay was asked who should be responsible for making decisions about notifying MPs that they have been the target of a foreign state actor. He indicated that this was also a complicated issue and did not have a clear answer, though he favoured the House itself as having the responsibility.

[31] On the one hand, Parliament is an equal and independent branch of government. As such, it should be responsible for ensuring the safety and security of MPs. Along with this duty would come the duty to warn MPs of security threats. Making a government agency responsible risked undermining the separation of powers.

[32] On the other hand, he questioned whether the House of Commons itself has the necessary will to play a lead role in countering foreign interference threats directed at MPs. He pointed to partisanship as being a significant impediment to the House itself serving this function. He believed that non-partisan officials, such as the Clerk of the House of Commons, would need to play a role in decision-making in this regard.

[33] Mr. McKay emphasized that his views were not meant to diminish the role of the Security and Intelligence community. He expressed his confidence in the public services, including bodies such as CSIS and the CSE. As a practical matter, information about threats would likely come from these agencies. However, he believed that information about threats to MPs should probably be conveyed to the House of Commons leadership, who should then be responsible for alerting MPs.

[34] Commission counsel referred Mr. McKay to the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*.[2] Mr. McKay indicated that, in his view, the approach set out in this document was good in the hands of a good Minister, but bad in the hands of a bad Minister. He noted the discretion that existed in the Direction in terms of identifying what was a sufficient threat that warranted notifying MPs, as well as the circumstances in which notification might not occur due to security considerations. Mr. McKay made reference to what he viewed as an overly cautious approach to secrecy amongst some government officials.

[35] Mr. McKay did note that the *Ministerial Direction* was helpful in highlighting the unique role and vulnerabilities of Parliamentarians.

[36] Mr. McKay was asked his views about who should be responsible for providing cyber security for MPs non-parliamentary systems. He indicated that he did not believe that the Government of Canada should do this. He agreed that partisan activities should not occur on devices or accounts provided by the House of Commons but suggested that the House of Commons might provide funding to MPs to obtain their own cyber security services for their private systems. Mr. McKay did not believe that political parties would be well placed to providing these services.

[37] Mr. McKay expressed his view that a greater number of MPs should have security clearances, which would permit them to access classified information relevant to potential foreign interference threats against them. As an example, he suggested members of certain standing committees, such as National Defence or Foreign Affairs, should presumptively have such clearances. He indicated that members of these committees might be attractive targets for foreign interference.

[2] CAN021931.