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: Garnett Genuis

Garnett Genuis, MP, was interviewed by Commission counsel on August 15, 2024.

Notes to Readers:

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

1. Background

[1] Garnett Genuis is the Member of Parliament ("**MP**") for Sherwood Part-Fort Saskatchewan. He has represented this Electoral District since 2015. He is a member of the Conservative Party of Canada. Prior to his election to Parliament, he has worked as a federal political staffer, in a political not-for-profit, and in a public opinion research firm. He holds degrees from Carleton University and the London School of Economics.

[2] Mr. Genuis has been involved in international human rights issues throughout his parliamentary career, particularly with respect to issues involving the People's Republic of China ("**PRC**") and the Chinese Communist Party.

2. Organization of Members' Offices

2.1 General Organization

[3] Members of Parliament have broad flexibility in how to structure their offices. All Members are provided with a budget and decide how it is divided between their Ottawa and Constituency offices.

[4] Mr. Genuis's Ottawa office is responsible for supporting his Parliamentary work, such as participation in standing committees, communications on national issues, and private members bills. His constituency office is responsible for case work (assisting constituents who are having issues with the federal government) and consultations with

constituents. These are not watertight components, and he values strong communications between his offices.

[5] Mr. Genuis's Ottawa office is made up of 2-3 permanent staff, supported by a mix of interns and volunteers. His constituency office is staffed by an Office Manager, a receptionist, and a one part-time staffer.

2.2 Information Technology

[6] The House of Commons provides information technology ("**IT**") services and equipment for MPs and their staff. They provide Mr. Genuis and his offices with devices (e.g. computers, cell phones) and internet service, and provide IT support in the event of a technical issue. They are responsible for cyber security related to these systems.

[7] Mr. Genuis explained that every MP engages in both parliamentary and partisan work. Partisan work is not part of the job as such, but every MP engages in partisan work to some extent, which includes activities such as fund raising, maintaining relationships with their electoral district association, and preparing to seek re-election. While his partisan work is related to his status as an MP, it would not be appropriate, and indeed against parliamentary rules, to use House of Commons IT equipment to undertake this work. He maintains his own private equipment, such as a personal cell phone, for his partisan work, as well as for other personal activities. The specific way that this separation is structured may vary from MP to MP, and Mr. Genuis emphasized that he could only speak to his own experience, which may differ from the way this distinction is managed by others.

[8] The House of Commons IT department does not provide service for his private IT devices or services, including his home internet. Mr. Genuis does some parliamentary work at home using House of Commons provided devices.

[9] The Conservative Party does not issue devices to Parliamentarians or provide IT services for personal devices. They provide IT support in relation to particular party apps.

[10] Mr. Genuis was not aware of particular services provided by the Canadian Centre for Cybersecurity to MPs related to securing their systems or responding to cyber attacks.

[11] There can be cases where Parliamentary work is discussed on personal channels or devices. Mr. Genuis may receive communications from constituents about legislative matters during an election campaign. Outside of election campaigns, he also receives calls from constituents that relate to Parliamentary business through personal channels, in the same way that someone might approach him in a grocery store or at church to discuss Parliamentary matters. Many communications can have both partisan and parliamentary aspects, such as a call with a prospective donor that involves a discussion of what bills are currently before Parliament.

[12] Mr. Genuis also discussed a situation where a constituent might send a partisan email to his parliamentary email account, which he would then re-route to his non-parliamentary email. He also explained that some parliamentary communications he has with both constituents and colleagues may take place on secure messaging systems like Signal that he has installed on his personal devices.

[13] Mr. Genuis does not give his House of Commons cell phone number to constituents but does provide them with his personal cell phone number from time to time. He therefore does receive parliamentary phone calls and text messages related to constituency work on a private device.

3. Interparliamentary Groups, Associations and Organizations

3.1 Generally

[14] MPs may participate in a range of international groups, associations and organizations of Parliamentarians.

[15] Some organizations, such as Parliamentary Associations and Interparliamentary Groups, are official bodies that are recognized with the House of Commons. These groups are subject to certain regulations and receive some funding from the House of Commons.

[16] There are other interparliamentary organizations that exist outside of the formal structures of the House of Commons that MPs can belong to.

[17] The Interparliamentary Alliance on China ("**IPAC**") falls into the latter category.

3.2 The Interparliamentary Alliance on China (IPAC)

[18] IPAC is an international organization made up of Parliamentarians from across the ideological spectrum. It was founded in 2020.

[19] What unifies members is the thesis that the CCP is a threat to global security and international human rights norms. While individual IPAC members hold a diverse set of views on China, there is a general consensus that there is a need to develop policies and strategies that take into consideration the threat that the CCP poses and to respond to that threat in a more robust and risk-conscious way.

[20] IPAC is organized around an international secretariat that has its own budget and staff. In each country, IPAC has both members and national co-chairs, all of whom are current or former parliamentarians. A country's co-chairs should be from different political parties or groupings.

[21] IPAC serves as a forum for information sharing between its members. It holds both national and international conferences, issues joint statements, and provides communications to its member parliamentarians. Mr. Genuis emphasized the value in Parliamentarians exchanging ideas, perspectives and policy proposals. He noted that a good idea in one jurisdiction can result in action in other countries due to this exchange of ideas.

3.3 Mr. Genuis's Involvement in IPAC

[22] Mr. Genuis became involved in IPAC at the time of its founding in 2020.

[23] He had a pre-existing relationship with Luke de Pulford, who was the co-founder of IPAC and serves as its executive director. Ian Duncan Smith – a British conservative parliamentarian who Mr. Genuis respects – was also involved in the initial organization of IPAC. Mr. Genuis felt that IPAC was a very good fit for him given his existing advocacy work and focus on international human rights and China as an MP.

[24] Mr. Genuis became involved with IPAC as one of Canada's co-chairs, along with two members of the Liberal Party of Canada: John McKay and Irwin Cotler.

[25] Mr. Genuis continues in his role of Canadian Co-Chair of IPAC today.

[26] Mr. Genuis estimates that there are around 20-25 Canadian members of IPAC.

[27] Asked to describe his role as Co-Chair, Mr. Genuis indicated that it entailed a greater coordinating function compared to other members. He viewed his Co-Chair role as to facilitate opportunities for Canadian MP members to be connected into the IPAC network. As a Co-Chair, he was more likely to be invited to speak at IPAC organized conferences.

[28] Mr. Genuis confirmed that in his role of Co-Chair he would have regular communications with the IPAC international secretariat.

[29] Mr. Genuis indicated that IPAC's communications would generally go to his personal email account, and not his parliamentary email account. He believed this was the case because of his pre-existing relationship with Mr. de Pulford, who he communicated with using his personal email. Mr. Genuis noted, however, that IPAC also communicated with his staff using their parliamentary email accounts.

4. Cyber Attacks Conducted by Advanced Persistent Threat 31

[30] Commission counsel questioned Mr. Genuis about his understanding of a coordinated cyber attack against members of IPAC in Canada in 2021 by a PRC-linked entity referred to as Advanced Persistent Threat 31 ("**APT 31**"). The discussion involved both how Mr. Genuis came to be aware of the attacks, as well as his understanding of how Government of Canada and Parliamentary officials learned of the attack.

4.1 Notification of IPAC Members

[31] On 25 March 2024, an indictment[1] was unsealed in the United States District Court for the Eastern District of New York, charging seven individuals with engaging in a range of

[1] COM0000380.

cyber attacks on behalf of the Hubei State Security Department of the PRC. The indictment described the defendants as being members of APT 31. The indictment stated that, in or about 2021, the defendants targeted the email accounts of various government individuals from across the world who were part of IPAC.

[32] IPAC learned of the indictment and reached out to the United States Federal Bureau of Investigation ("**FBI**"). Through these communications, IPAC confirmed the list of its members whose email addresses had been targeted by APT 31.

[33] During the weekend of 19-21 April 2024, Mr. Genuis received a phone call from Mr. de Pulford. Mr. de Pulford informed Mr. Genuis that he had been targeted as part of a cyber attack, and that IPAC was still consulting with the FBI about what information could be released. The two agreed that it was important for Canadian IPAC members to be briefed and arranged for two briefings to occur on April 24: the first for the IPAC Co-Chairs, and another one for all Canadian members of IPAC.

[34] On 24 April, Mr. de Pulford provided a more detailed briefing to Mr. Genuis and Mr. McKay. They were informed, amongst other things, that:

a. The cyber attacks were conducted by APT 31;

b. Both the USA and the UK had attributed the attacks to China;

c. The attacks took the form of a "pixel reconnaissance attack", in which a "tracking pixel" was embedded in an image contained in an email. When the email is opened and the image loads, the pixel sends back some limited information including the recipients IP address, the time, and some limited device data like the operating system used on the device;

d. The FBI had not notified impacted parliamentarians directly due to their own rules respecting state sovereignty; and

e. The FBI did notify the impacted IPAC member's governments in 2022.

[35] Mr. de Pulford also provided some information about measures that could be taken to better protect IPAC members' devices.

[36] Mr. Genuis was informed that it was his personal email address that was targeted by APT 31.

[37] Mr. Genuis was not particularly surprised to learn that the PRC had been targeting him, given his outspoken position on matters related to China. However, he was surprised to learn that the Government of Canada was notified by the FBI in 2022 and yet he was only learning about the attacks in 2024. He noted that the failure to inform was not limited to one party, as there were impacted members from a range of political parties, including the Liberal Party of Canada, and none of them had been notified. He also felt that the failure to notify impacted IPAC members resembled the failure to alert MP Michael Chong about the PRC's targeting of him.

[38] Later in the day on 24 April 2024, Mr. Genuis, Mr. McKay and Mr. de Pulford held an online briefing for impacted Canadian members of IPAC. Mr. de Pulford and other IPAC staff conducted the briefing and conveyed the same information that he had provided to Mr. Genuis and Mr. McKay earlier in the day. Mr. Genuis described that the general response from parliamentarians who attended this online briefing was disappointment that the Government of Canada did not inform them of the incident earlier.

[39] Not all of the impacted Parliamentarians were present for the briefing. In order to ensure that they were notified, IPAC sent an email[2] to all impacted Canadian members on 25 April 2024 containing the information that had been provided during the 24 April briefings.

[40] On 29 April 2024, Mr. Genuis raised a question of privilege in the House of Commons related to both the cyber attacks themselves as well as the failure by Canadian officials to notify the impacted Parliamentarians. This question of privilege is currently under consideration by the Standing Committee on Procedure and House Affairs.

[41] On 9 May 2024, the FBI held an online briefing for impacted IPAC members from around the world. This briefing did not provide any additional information about the

[2] COM0000485.

attacks themselves. The FBI did provide additional guidance about cyber security measures that IPAC members could take.

[42] Mr. Genuis indicated that he has not had any substantive discussions about the cyber attacks or the risk of technology-based foreign interference with either the House of Commons administration, law enforcement, security and intelligence agencies, or other Government departments and agencies outside of his participation in the hearings currently taking place at PROC.

4.2 Notification of Canadian Officials

[43] Mr. Genuis was asked to explain his understanding of when Canadian officials became aware of the cyber attacks.

[44] Mr. Genuis indicated that he understood that the FBI had notified the Government of Canada in 2022, and that the Government informed the House of Commons IT department.

[45] Mr. Genuis also understands that there is a suggestion that the Government of Canada was aware of the cyber attacks in 2021, but that he is unclear about exactly what Government officials have said that they knew at that time. Similarly, he does not know the nature or scope of information shared by the Government of Canada to the House of Commons IT, and whether the latter was authorized to disclose that information further.

4.3 Impacts of Cyber Attacks

[46] Mr. Genuis indicated that the cyber attacks had not had a significant visible impact on his personal or professional life, as he had already assumed that foreign states – particularly China – would be monitoring his activities. He does not believe that it is plausible that China would target him in a way that would threaten his safety or wellbeing on Canadian soil, although they may be trying to disrupt or otherwise impact his work. He does use secure channels of communication more than he previously has, though he already used such channels prior to learning about the attacks. The real downstream impacts of these attacks remain unknown.

[47] Mr. Genuis also understands that the cyber attacks were largely unsuccessful. He is not aware of any Canadian IPAC members being targeted with any further attacks by APT 31, and is aware that the House of Commons administration has confirmed that the House's IT systems were not compromised. Mr. Genuis's own personal devices and private email system have not been forensically examined to assess whether they were compromised by APT 31.

[48] Mr. Genuis does believe that the failure to notify him and his colleagues did deprive them of the opportunity to take defensive measures in a timely way. Mr. Genuis has followed the cyber security advice he was given by IPAC and the FBI, including by disabling image loading on his emails. Had he been informed of the cyber attacks in 2021 or 2022, he would have taken these measures years earlier than he did.

5. Reflections on the Cyber Attacks and Recommendations

[49] Mr. Genuis believes that targeted Parliamentarians should have been notified by the Government of Canada of the cyber attacks when officials first became aware of them. The House of Commons administration is not a security and intelligence agency and so did not have the responsibility to notify MPs. Even when the Parliamentary administration was notified by the Government, the information that they received may have been subject to caveats, which would have limited or prevented them from disclosing information to impacted parliamentarians. The responsibility of notifying parliamentarians should have been with security and intelligence agencies such as the Canadian Security and Intelligence Service ("**CSIS**").

[50] Mr. Genuis noted the recent changes to the *CSIS Act* contained in Bill C-70, which he understood would enhance its ability to share information outside of the Government of Canada. Mr. Genuis indicated that only time would tell whether these amendments will actually assist. He noted that there is a cultural problem within the Canadian government about the declassification of information. He expressed his view that greater disclosure of information can be an effective tool for countering foreign interference.

[51] When dealing with classified or sensitive information, Mr. Genuis believed that there should be a balancing of the public interest in disclosure of information. He also believes that, in some situations, the targets of foreign interference should have an absolute right to know. He stated that what specific information should be provided would depend on the circumstances. It might be appropriate to hold back some information, so long as enough information is disclosed to permit a target to take actions to protect themselves. It would be in the public interest to allow people to protect themselves against foreign interference, which requires promptly informing those targeted by interference operations.

[52] Mr. Genuis was asked about who should be responsible for making decisions about disclosure: Ministers, or senior civil servants. Mr. Genuis indicated that both options presented challenges. In a system of responsible government, there was a good case to be made that Ministers should be the ones to make these decisions. On the other hand, there is an inherent conflict of interest due to the fact that Ministers are also political actors. Senior security and intelligence officials are not partisan actors, but may have other incentives around not disclosing. Clearly the government of the day bears ultimate responsibility for whether or not the system is working, and if the system is not working then ministerial responsibility dictates that the government has to take responsibility.

[53] Mr. Genuis indicated that it would be preferable for there to be clear rules or guidelines about when and how disclosure of sensitive information to targeted individuals should occur.

[54] Mr. Genuis reviewed the May 2023 *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*.[3] He confirmed that he was not notified of the cyber attacks pursuant to this Direction, and noted that the Direction is silent as to its application to events that occurred prior to May 2023. Mr. Genuis indicated that the Direction should apply to any incident in the past that could still have a present-day impact on Parliament or parliamentarians.

[3] CAN021931.

[55] Commission counsel referred Mr. Genuis to paragraph 3 of the Direction, which addresses notification of parliamentarians when threats to the security of Canada are directed at them. Commission counsel asked Mr. Genuis about the fact that the duty to disclose was limited to circumstances where notification was "possible within the law and while protecting the security and integrity of national security and intelligence operations and investigation". Mr. Genuis indicated that this language provided a great degree of discretion and could result in no notification occurring in circumstances where notification should occur. He viewed the issue of the government culture of secrecy as being a significant issue that would likely impact the application of the Direction.

[56] Mr. Genuis discussed the challenges presented by foreign states targeting the personal devices of individuals. He noted that this type of targeting presented risks not only related to exposing parliamentary work or politically sensitive information, but also exposing targets to blackmail. Currently, the security supports for these devices – compared to House of Commons devices – was limited.

[57] It was difficult to say who should be responsible for providing additional support. Government agencies would have the capabilities to do so, but there are concerns about government actors having access to politically sensitive systems. Political parties could provide devices or support, but there would be similar challenges if such devices were used for intra-party contests like leadership races or nomination contests. Parliamentarians could be permitted to use their House of Commons devices to engage in partisan activities, but this would involve an effective public subsidy for partisan activity. However, Mr. Genuis noted that there are other areas in which public subsidies for partisan campaign activities already exist.