Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 093-2018

Saskatchewan New Democratic Party

September 19, 2018

Summary: On May 9, 2018, the Complainant submitted a privacy breach complaint to the Information and Privacy Commissioner's office alleging that two individuals within the Saskatchewan New Democratic Party (NDP), a provincial political party, had inappropriately accessed their personal data. The Commissioner found that the Saskatchewan NDP is not a government institution within the meaning of *The Freedom of Information and Protection of Privacy Act* (FOIP) and that no parts of FOIP apply to this organization. As such, the Commissioner found that his office has no jurisdiction. However, the Commissioner took the opportunity to outline some best practices that political parties may adopt when privacy breaches occur.

I BACKGROUND

[1] On May 9, 2018, my office received a privacy breach complaint from an individual (the Complainant) stating that two named individuals (Individual A and Individual B) within the Saskatchewan New Democratic Party (Saskatchewan NDP) had inappropriately accessed their personal data stored within the federal NDP's online voter system, Populus.

[2] The Complainant first raised privacy concerns related to breaches of their personal data stored in the federal Populus system with Vicki Mowat, Member of the Legislative Assembly, on January 10, 2018. On January 19, 2018, Vicki Mowat responded to the Complainant indicating that an investigation was conducted within her office and no privacy breach occurred in, or through her office. Ms. Mowat's response stated that the online voter system Populus is used by the Saskatchewan NDP and not by her constituency

office. As such, the Complainant's privacy concerns were referred to the Provincial Secretary of the Saskatchewan NDP.

[3] On January 22, 2018, the Saskatchewan NDP informed the Complainant that the access rights of Individual A was suspended in Populus. The Party also informed the Complainant that steps to investigate the alleged privacy breaches were underway and requested the consent of the Complainant to share their name, and other pertinent information, as necessary, for the purpose of the investigation.

[4] On March 6, 2018, after concluding their investigation, the Saskatchewan NDP informed the Complainant that their investigation confirmed Individual A had breached the Complainant's personal data.

[5] The Saskatchewan NDP conducted a subsequent investigation and found that Individual A committed seventeen more privacy breaches using the federal online voter system Populus, relating to twelve other individuals not including the Complainant.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] *The Freedom of Information and Protection of Privacy Act* (FOIP) applies to privacy matters when three elements are present: 1) it involves a government institution as defined in FOIP; 2) it concerns personal information as defined in FOIP; and 3) the personal information at issue is in the possession or control of the government institution. The first element is the most notable for the purpose of this privacy breach complaint.

[7] In determining whether or not the Saskatchewan NDP, a provincial political party, is a government institution as defined in FOIP, I must begin by considering the meaning of a "government institution" at subsection 2(1)(d), and section 3 of the FOIP Regulations which further clarifies subclause 2(1)(d)(ii), as it relates to government institutions.

[8] Section 2 of FOIP provides:

> 2(1) In this Act:
>
> …
>
> (d) "government institution" means, subject to subsection (2):
>
> (i) the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or
>
> (ii) any prescribed board, commission, Crown corporation or other body, or any prescribed portion of a board, commission, Crown corporation or other body, whose members or directors are appointed, in whole or in part:
>
> (A) by the Lieutenant Governor in Council;
>
> (B) by a member of the Executive Council; or
>
> (C) in the case of:
>
> (I) a board, commission or other body, by a Crown corporation; or
>
> (II) a Crown corporation, by another Crown corporation;

[9] The FOIP Regulations provide:

> 3 For the purposes of subclause 2(1)(d)(ii) of the Act:
>
> (a) the bodies set out in Part I of the Appendix; and
>
> (b) subsidiaries of government institutions that are Crown corporations;
> are prescribed as government institutions.

[10] The Saskatchewan NDP is not an office of Executive Council or any ministry of the executive government of Saskatchewan. The Saskatchewan NDP is also not a prescribed body as set out in Part 1 of the Appendix, nor a subsidiary of government institutions that are Crown corporations. The Saskatchewan NDP therefore does not fall within the meaning of subsection 2(1)(d) of FOIP.

[11] Next, I must consider those organizations or bodies that are specifically excluded within the meaning of a "government institution" in FOIP and those to whom FOIP applies in part, in accordance with subsection 2(2), 3(3) and 3(4):

> 2(2) "Government institution" does not include:
>
> (a) a corporation the share capital of which is owned in whole or in part by a person other than the Government of Saskatchewan or an agency of it;
>
> (b) the Legislative Assembly Service or, subject to subsections 3(3) and (4), offices of members of the Assembly or members of the Executive Council; or
>
> (c) the Court of Appeal, Her Majesty's Court of Queen's Bench for Saskatchewan or the Provincial Court of Saskatchewan.
>
> 3(3) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Assembly and their employees as if the members and their offices were government institutions:
>
> (a) sections 24 to 30;
>
> (b) section 33.
>
> 3(4) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Executive Council and their employees as if the members and their offices were part of the government institution for which the member of the Executive Council serves as the head:
>
> (a) sections 24 and 24.1;
>
> (b) sections 25 to 30;
>
> (c) section 33.

[12] When read together, subsections 2(2), 3(3) and 3(4) only makes offices of Members of the Legislative Assembly (MLA) and their employees and Ministers' offices subject to the privacy provisions of FOIP. Nothing in these subsections makes provincial political parties, like the Saskatchewan NDP, subject to FOIP.

[13] I find that the Saskatchewan NDP is not a government institution within the meaning of FOIP and that no parts of FOIP apply to this organization. As such, my office has no jurisdiction over a provincial political party.

[14] Despite not having jurisdiction, there is value in using aspects of this case to outline some best practices that political parties may adopt when privacy breaches occur.

[15] In reviewing the facts related to this privacy breach complaint, the Saskatchewan NDP cooperated fully with my office providing useful information including copies of documents related to the collection and use of voter data, the federal online voter system Populus and the actions taken to investigate and address the alleged privacy breach.

2. Is there personal information involved?

[16] According to the Saskatchewan NDP's submission to my office, Populus contains voter data. This information can include name, residential address, gender, occupation, email address and telephone number, and other information. While FOIP does not apply in this case, the personal data would fall within the meaning of personal information under subsection 24(1) of FOIP, if the data were in the possession or control of a government institution, which in this case it is not.

3. What are some best practices for political parties for responding to privacy breaches involving personal data?

Contain and investigate the privacy breach

[17] My office's *Privacy Breach Guidelines* states that containing a privacy breach involves immediately stopping further breaches by revoking access to personal information. Investigating the breach includes identifying which employees, if any, were involved with the privacy breach, among other steps.

[18] As noted earlier, the Complainant named two individuals, Individual A and Individual B, in their original complaint. The Saskatchewan NDP's submission indicates that when they became aware of the complaint, they immediately suspended the access rights of Individual A in the federal online voter system Populus, conducted an investigation – which later

confirmed Individual A had in fact inappropriately accessed the Complainant's information – and prepared an investigation report.

[19] The investigation report confirms that Individual A was questioned on the findings of the investigation, but they could not provide any valid purpose or reasonable explanation for the searches and retrievals in the system. Later, Individual A did provide an explanation for the vast majority of the breaches committed and confirmed that the data retrieved had not been further used or disclosed. The explanation provided by Individual A does not legitimize the privacy breaches in any way.

[20] With respect to Individual B, the Saskatchewan NDP stated that they determined that this individual did not have an account in the federal online voter system Populus and therefore had no access to personal data in the system; consequently, there was no basis to investigate Individual B.

[21] In light of the facts, I suggest that when allegations of a privacy breach are brought to the attention of a political party, the party should be thorough in containing and investigating the allegation or breach. This involves ensuring that appropriate actions are taken in respect of any individual or group involved, or alleged to be involved, regardless of whether they were named at the outset by a complainant, or identified during the course of an investigation. Also, to ensure a complete and accurate account of all actions taken, these should be detailed in the investigation report.

Notify affected individuals

[22] As stated in guidelines issued by my office, breach notification to affected individuals is a key step in managing privacy breaches and should occur as soon as possible after key facts about the breach have been established. Notifications should include, among other things: a description of the breach, a detailed description of the personal information involved, and steps taken and planned to mitigate the harm and to prevent future breaches.

[23] In a supplementary report, it was indicated that Individual A retrieved the contact details of twelve other individuals, not including the Complainant, on seventeen different occasions without a valid reason.

[24] My office asked the Saskatchewan NDP whether their organization had notified the twelve other individuals whose personal data was also breached by Individual A. The Saskatchewan NDP confirmed that they did not notify these individuals on the basis that the breaches were contained. The Saskatchewan NDP has indicated that they intend to notify these individuals.

[25] In my view, personal data in the possession of political parties, is sensitive data that could be used to cause harm to individuals. Without knowing when their data is breached, and without specific information about the breach, it would be difficult for individuals to take the appropriate steps to further mitigate the risk of harm and protect themselves, beyond any steps that would have been taken by a political party.

[26] Recognizing that nothing in legislation currently requires political parties to notify individuals when their personal data is breached, I encourage political parties to adopt a practice whereby individuals are always notified when their data is breached and that these notifications list the specific information that was breached and when.

[27] My office's *Privacy Breach Guidelines* contains all the elements that I believe should be included in notifications to affected individuals. This document can serve as a model to political parties to ensure all necessary elements are included in their notifications – with the exception of the right to complain to my office, since I do not have jurisdiction to investigate privacy breaches involving provincial political parties.

Prevent future breaches

[28] It is concerning that an individual was able to breach personal data thirty times over a short period of time and that those breaches went undetected. This case may highlight the need

for all political parties to do more to prevent privacy breaches and to detect them when they do occur.

[29] Many political parties, if not all, rely heavily on electronic systems to store sensitive personal data. One way to reduce the risk of privacy breaches is to ensure all systems are capable of producing audit logs of user activity in the system, like the federal online voter system Populus. Logs should record when users have accessed, searched, viewed or altered information in the system. Logs should also time stamp every action of users in the system.

[30] In addition to having audit logs, ensuring that logs are randomly checked, either manually or automatically, allows for a faster identification of potential compromises of information in systems. The use of controls, like audit logs and a process for verifying the logs, could act as a deterrent for system users if they know such controls exist, in addition to identifying occurrence of breaches sooner.

[31] A tool that can be used to identify potential privacy risks and allow an organization to select the appropriate administrative, technical and physical controls that would mitigate, or eliminate, identified risks are Privacy Impact Assessments (PIAs). It is a good practice to undertake PIAs when new systems are implemented, or as changes to existing systems or processes are introduced. An early and complete analysis of any potential privacy risks can reduce the risk of privacy breaches from occurring in the future.

[32] I suggest that political parties implement proactive safeguards that can identify, monitor and audit instances where data stored in electronic systems may be, or is compromised. Safeguards may include the use of audit logs, reviews of audit logs and those identified through the completion of PIAs, among other controls.

Inappropriate access to personal data

[33] My office, and other jurisdictions, have investigated numerous cases involving individuals who intentionally misused their legitimate access to data stored in electronic systems. Such breaches can seriously undermine trust between citizens and organizations.

[34] In Investigation Reports 088-2013 and 100-2015, I stated that disciplinary actions should be strong enough that it deters individuals from intentionally breaching personal data. Those reports involved personal health information, but in my view, the type of data in the possession of political parties may be as sensitive as personal health information and therefore warrants strong disciplinary actions as well.

[35] As outlined in this report, this case involved Individual A intentionally breaching the personal data of thirteen individuals, thirty times over the course of four months. Although Individual A was a volunteer of the Saskatchewan NDP at the time the breaches occurred, Individual A still knowingly used the federal online voter system Populus to inappropriately access the data of thirteen individuals. Individual A's explanation for using the Populus system to inappropriately access data does not condone their actions.

[36] As stated publicly, the disciplinary measures taken against Individual A involved suspending access to voter data for a period of four years, subject to reinstatement of monitored access after one year if the individual completes privacy and information training.

[37] During my investigation, the Saskatchewan NDP stated that, in respect of volunteers, "*…political parties lack the ability to mandate cooperation with an investigation to the same extent possible in the context of an employer/employee relationship*." If that is the case, there must be stricter consequences for volunteers found to have inappropriately accessed personal data.

[38] In my view, volunteers should be aware and provided copies of internal documents related to the personal information handling practices within the organization *before* they get access to sensitive personal data, and that access should be removed indefinitely if they intentionally commit privacy breaches.

Internal documents and training related to the protection of personal data

[39] Internal documents, namely those intended to inform or train staff and volunteers of the appropriate personal data handling practices they must adhere to, should provide sufficient information regarding privacy breaches and the impact that breaches can have on affected individuals. These documents should provide specific examples of what would constitute a privacy breach, describe how personal data could be used to cause harm to individuals and list the specific safeguards already in place to protect the data. Finally, internal documents should also adequately explain the consequences for misusing personal data.

[40] Political parties may wish to review their own internal documents to verify that they include the information described in the preceding paragraph. Staff and volunteers should receive copies of these documents and training *before* they are granted access to personal data.

[41] Only a few copies of documents related to the information handling practices of political parties are available online. Recognizing that there is no legal requirement for political parties to make their internal documents available, I would encourage political parties, where possible, to consider publishing their documents nonetheless. Doing so may provide the public at large a better understanding of the specific personal data in the possession or control of political parties and how their data is being protected.

III FINDINGS

[42] I find that I do not have jurisdiction to investigate this privacy matter involving a provincial political party, but have taken the opportunity to discuss best practices regarding privacy breaches.

IV RECOMMENDATIONS

[43] Although there are currently no legal obligations pertaining to the management of privacy breaches involving political parties, I recommend that political parties consider adopting the following best practices:

a) Be thorough when containing and investigating a breach by ensuring that appropriate actions are taken in respect of any individual or group involved, or alleged to be involved, regardless of whether they were named at the outset by a complainant, or identified during the course of an investigation. Also, ensuring that all actions taken in this regard are documented in the investigation report.

b) Notify affected individuals when their information is breached and ensure these notifications list the specific information that was breached and when.

c) Implement proactive safeguards that can identify, monitor and audit instances where information stored in electronic systems may be, or is, compromised.

d) Ensure all staff, including volunteers, are provided copies of internal documents related to the information handling practices within the party *before* they get access to sensitive personal data. Access should be removed indefinitely if individuals intentionally commit privacy breaches.

e) Review internal documents to verify that they include enough information to allow staff, including volunteers, to understand what are privacy breaches and the consequences for breaching personal data. Political parties may also wish to consider publishing their policies where possible.

Dated at Regina, in the Province of Saskatchewan, this 19th day of September, 2018.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner