ELECTORAL DATA PRIVACY: A DISCUSSION DOCUMENT

ELECTIONS NEW BRUNSWICK - FEBRUARY 2025

ELECTIONSNB
YOUR TRUSTED ELECTION SOURCE

Elections New Brunswick
Electoral Data Privacy – February 2025
ISBN 978-1-4605-4136-4 (print, bilingual edition)
ISBN 978-1-4605-4137-1 (English PDF)
ISBN 978-1-4605-4138-8 (French PDF)

Contents

Executive Summary 1

Key Findings 1

Recommendations Requiring Legislative Change 2

Recommendations Requiring Process or Policy Change 2

Recommendations Requiring Funding, but Not Legislative Change 2

Discussions with Political Parties 3

Conclusion 3

Data Privacy and Elections in 2024 4

Introduction—Why Privacy Matters 4

The Best Time was 10 Years Ago, the Next Best Time is Now 4

Overview of Recommendations from Previous Elections NB Publications 8

Modernizing New Brunswick's Electoral Legislation (2019) 8

2021 Electoral Modifications and Post-Election Recommendations 9

Elector List Data Collection and Disclosure 10

Current Collection and Sharing Requirements 10

Jurisdictional Comparison 11

Areas for Improvement & Risk Mitigation 17

Other Personal Data Collected By Elections NB 21

Current Requirements 21

Jurisdictional Comparison 21

Areas for Improvement & Risk Mitigation 22

Discussions with Political Parties 24

Registered Political Parties Engagement 24

Recommendations 26

Recommendations Requiring Legislative Change 26

Recommendations Requiring Process or Policy Change 29

Recommendations Requiring Funding, but not Legislative Change 30

Conclusion 31

Appendix A: Original Recommendations Related to Data Privacy 32

Modernizing New Brunswick's Electoral Legislation (2019) 32

2021 Electoral Modifications and Post-Election Recommendations 35

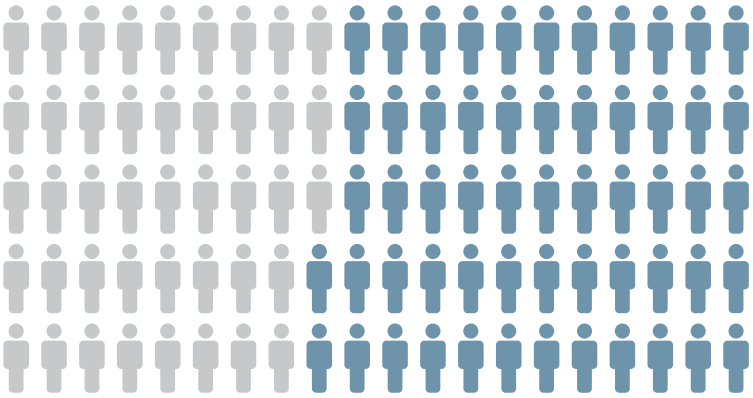
Executive Summary

Elections are fundamental to democracy, and their effective administration requires substantial data collection and sharing. However, this data handling also presents privacy risks that must be carefully managed.

This discussion paper examines current practices around electoral data in New Brunswick, compares them to other Canadian jurisdictions, and identifies multiple recommendations that could be implemented, from a comprehensive regime with maximum privacy protection to minimal steps that merely encourage participants to better protect voter privacy while maintaining electoral integrity.

Key Findings

- New Brunswick's electoral data handling practices are outdated compared to other provinces and could be improved with legislative and procedural changes.
- There is increasing public concern about data privacy, with 57% of Canadians reporting concern in 2022, up from 42% in 2012.
- Recent incidents across Canada have highlighted privacy and security risks related to voter data, including:
  - Distribution of voter lists to extremist political parties
  - Harassment of candidates, especially women and gender-diverse individuals
  - Insufficient safeguards on use of voter data by political parties
- Other provinces have implemented stronger protections, such as:
  - Allowing vulnerable voters to be removed from shared lists
  - Requiring political parties to file privacy policies before receiving voter data
  - Empowering election agencies to audit party compliance
  - Reducing unnecessary data collection and sharing
- New Brunswick could adopt many of these best practices, often with minimal cost or disruption to electoral processes.



57%

of Canadians reporting concerns about data privacy in 2022.

Recommendations Requiring Legislative Change

1. Develop a comprehensive legislative regime to manage privacy risks.
2. Reduce data gathering requirements, particularly for non-essential information like elector gender, addresses of those who printed advertisements, and candidate occupations.
3. Explore the use of fictitious data to track potential data breaches.
4. Create further legal distinction between what is gathered and what is shared, particularly for donor information.
5. Provide a mechanism for electors to be removed from the elector list or have their information concealed in versions shared with political parties/candidates.
6. Require political parties to develop privacy policies regarding data they receive or collect, make these policies public, and appoint a Privacy Officer.
7. Require political parties to develop and deploy privacy policies subject to approval by the Chief Electoral Officer before receiving any elector data.
8. Give Elections NB or the Ombud the authority to audit compliance with privacy policies.
9. Encourage a single point of contact for data sharing within political parties.
10. Require registered political parties to meet with the CEO and/or Ombud at least once annually on the subject of privacy.

Recommendations Requiring Process or Policy Change

11. Broaden the scope of the existing agreement form provided to recipients of elector data.
12. Advocate for the voluntary adoption of privacy policies by political parties.

Recommendations Requiring Funding, but Not Legislative Change

13. Work to create training programs for volunteers/campaign staff on data privacy.
14. Develop sessions, speakers, and more engagement on privacy with more senior party staff.
15. Conduct research/surveying on New Brunswickers' expectations and perspectives on data privacy.

Discussions with Political Parties

Efforts to engage political parties on these issues had limited success. When conducted, only two out of five registered political parties participated in discussions, and their input did not provide clear direction for next steps. This lack of engagement may stem from political parties' focus on other operational priorities, competitive concerns, or limited resources for implementing changes.

Evolving practices federally and in other provinces may create momentum for change. Elections NB has an ethical imperative to enhance privacy protections, even if stakeholder enthusiasm is currently muted. This discussion paper suggests that sharing examples of data breaches and harms from other jurisdictions might elevate the urgency of these recommendations.

This discussion paper also notes the financial constraints of political parties, particularly the smaller ones. It suggests exploring whether political parties would be more open to implementing better practices if financial support was available for hiring privacy expertise, similar to how they are reimbursed for auditors.

Conclusion

By adopting these recommendations, New Brunswick can modernize its approach to electoral data privacy, aligning with Canadian best practices and public expectations. This will help maintain trust in the electoral system while protecting voters' personal information. The proposed changes balance the need for electoral transparency and campaign effectiveness with the growing imperative to safeguard personal data in a digital world.

Data Privacy and Elections in 2024

Introduction—Why Privacy Matters

Data breaches, or inappropriate access to data, have impacted governments across the world, across Canada, and across all levels of government.

Democratic elections in Canada generally require substantial data to operate. Elections agencies need data to coordinate voting stations. They gather data about their own staff and from political parties on elections financing. Political parties receive data about voters from elections agencies to support their campaigns.

According to a poll conducted in 2022 by the Office of the Privacy Commissioner of Canada, 57% of Canadians are concerned or very concerned about the protection of their privacy, up from 42% in 2012. Canadians are concerned about the protection of their privacy—and the Government has an obligation to protect their privacy, especially when it is the Government collecting and distributing the data.

Elections are key to democracy, and we all benefit when elections are free, fair, and have broad and open participation from the public. This discussion paper outlines concerns that have been raised across the country relating to how elections are conducted, and some suggestions for how to resolve these concerns.

Broadly, New Brunswick has many data-handling practices which are out-of-date. Elections could be run just as well, and political parties could receive data to support their campaigns just as effectively, with fairly small adjustments to legislation. Some provinces have gone further, and this discussion paper outlines "best-practices" that would go the furthest to protect data privacy—but the focus of this discussion paper will be "easy wins" that can be done at little to no cost for government and political parties.

Many provinces have implemented processes that may reduce data privacy risk. Some of these would require legislative changes and some would not.

The Best Time was 10 Years Ago, the Next Best Time is Now

In 2021, an accused white supremacist received the names and address of every voter in the country through his registered "Canadian Nationalist Party," which was a far-right white nationalist political party that was registered with Elections Canada.

While the political party, when questioned, assured that it had no intentions to share the list outside of its own operations, there are few to no enforcement mechanisms to ensure that the list is not used for nefarious purposes.

While the government is clear that it's not in Elections Canada's mandate to judge the platforms and ideologies of political parties, stricter requirements on data sharing could alleviate the concerns around data misuse—or at least provide remedies if they should happen.

In 2021, a Calgary mayoral candidate named Kevin Johnston made inflammatory remarks about Muslims and health workers during the pandemic, including threatening to arrest employees of the Alberta Health Service. He would have received a copy of the elector list if one had been prepared, but the city council, in light of this risk, opted to not produce an elector list at all—being informed by Elections Calgary that they were capable of running an election without one.

This case raised concerns over the potential for lists to be used illegitimately. Ultimately, the city worked within its legislated capacity to run an election without producing compromising information, but this came at the cost of honest actors not receiving data they might usually expect to receive.

Women and gender-diverse candidates in the 2023 provincial election in PEI faced disproportionate harassment, mostly over the internet. Much of this harassment came from out-of-province and was directed at the gender of candidates.

After the election, there were calls to review policies around cyberbullying and harassment of candidates.

In 2015, Prince Edward Island (PEI) rolled out a system whereby political parties would receive updated lists of who has voted on election day every 15 minutes. The Privacy Commissioner, an independent office established in the province in 2002, found that this was an undue intrusion on the privacy of voters as the digital provision of the list of "who voted" was not authorized in PEI's *Election Act*. PEI's *Election Act* was subsequently amended to allow for such distribution of this information. In this case, legislation did not further restrict data production and access, but clarified its legitimate usage.

This is a small sample of cases within the last decade where questions of electoral data privacy have become matters of public concern. Every election, electoral agencies like Elections NB receive calls from concerned citizens who do not know or understand how political parties got their contact information—while exactly where the line is drawn is ultimately a decision for legislatures, there is a clear demand for both clarity in how electoral data is handled and for governments to be mindful and intentional in where lines are drawn between appropriate and inappropriate use of data.

Below is a table of cases of interest with brief summaries of the issues raised, which have occurred across Canada in recent years.

Article	Jurisdiction	Issue(s)	Risk
Calgary Isn't Giving Candidates Voters' Names And Addresses, But The Issue With Elector Lists Is A Canada-Wide Problem	Alberta	Radical candidates threatening voters on voter lists Privacy of voter lists.	Voter privacy and safety
Election law gives name and address of every Canadian voter to white nationalist party	Canada	Radical candidate receiving access to elector list with questions raised around safety of individual having access.	Voter privacy and safety
Restraining order issued against mayoral candidate threatening armed visits to Alberta health-care workers	Alberta	Radical Candidates threatening voters on voter list.	Voter privacy and safety
Female and gender-diverse candidates in 2023 P.E.I. election report being targeted online	PEI	Cyberbullying of candidates and online hate.	Threats and bullying will force some candidates to drop out of race.
Telling parties who has voted 'an unreasonable invasion' of privacy says commissioner	PEI	Practice of updating candidates through an electronic portal during an election who has voted contravenes privacy legislation.	Although the intent is to get more people out to vote by enlisting candidates, it risks the privacy of voters and who they voted for to be used against them.
Privacy commissioner finds gaps in federal party policies on personal data collection	Canada	Political parties not compliant with legislation on protecting personal information. Law is insufficient in protecting personal information.	Gaps on legislation and practise puts voter personal information at risk of exposure or abuses
Privacy concerns as only 14 per cent of candidates who used voters lists in last federal election say they secured them	Canada	Same as above.	

Article	Jurisdiction	Issue(s)	Risk
Survey of Candidates of the 43rd Federal General Election	Canada	Many topics covered, including privacy. Protection of Personal Information.	Lack of consistency in practice for protecting voter information
Trudeau government says privacy rules shouldn't apply to federal parties	Canada	Federal Privacy Commissioner indicates that proposed changes by the government do not establish "minimum privacy requirements" for parties. All parties are required to do is adhere to their own privacy policies, which they can revise whenever they wish.	Political parties will continue to collect private details about Canadians with zero oversight and almost no rules.
What's in your file? Federal political parties don't have to tell you	Canada	Lack of transparency and accountability for personal information collected by political parties.	Political parties/candidates collect much more personal information to build voter profile, and lack of auditable protections can lead to exposure of private information.
Courtenay-Alberni Riding Association Of The New Democratic Party Of Canada	Canada / BC	Federal vs Provincial purview over the collection and protection of personal information.	
https://www.cnn.com/2023/12/07/politics/threats-us-public-officials-democracy-invs/index.html	US	Security and threats to political candidates.	
https://globalnews.ca/news/9454325/canadian-mps-security-threats-rcmp/	Canada	Security and threats to political candidates.	
As Parties Build Digital Profiles of Voters, the Risk of Breaches Grows	Canada	Protection of digital information maintained by political parties.	Most parties lack policy and infrastructure to provide necessary protection.

These concerns are not theoretical. They are of increasing concern. Data privacy breaches have occurred across levels and functions of governments, and elections present a data-intensive operation where sensitive data is exchanged between the government and political entities with varying degrees of capacity and maturity in handling electoral data.

Overview of Recommendations from Previous Elections NB Publications

Modernizing New Brunswick's Electoral Legislation (2019)

In 2019, Elections NB published a discussion document, *Modernizing New Brunswick's Electoral Legislation*, outlining recommendations for modernizing the electoral process in New Brunswick, taking into consideration that a major update to legislation had not occurred for several decades; many practices have been unchanged since the mid-20th Century and deserve re-examining to ensure that New Brunswick's electoral practices continue to serve the province and are in-line with best practice in Canada.

A complete copy of those recommendations that are relevant to data privacy is included in **Appendix A**. The following is a summary of the content of each recommendation from the 2019 discussion document.

Recommendation 14: Require the recipient of a list of electors to file a privacy policy with the Chief Electoral Officer before receiving such a list.

Before receiving a list of electors, political parties or individuals should submit a privacy policy to the Chief Electoral Officer for approval. This policy must outline security measures to safeguard personal information and establish protocols for handling privacy breaches. By ensuring compliance with approved privacy policies, the risk of unauthorized access or data misuse can be minimized.

Recommendation 15: Consistently prescribe the contents of lists of electors provided to political parties and other individuals.

Standardize the contents of lists of electors provided to political parties and individuals. This entails limiting the data included in the lists to essential information such as surnames, given names, sex, civic addresses, and mailing addresses. Establishing uniformity in the information shared enhances clarity and consistency in electoral processes.

Recommendation 16: Provide a means to protect an elector's safety and to opt-out of sharing with political parties.

Introduce mechanisms to safeguard the privacy and security of vulnerable electors. Enable electors to request the redaction or anonymization of their personal information from records shared with political parties, data partners, and the public. This provision aims to protect vulnerable individuals from potential risks associated with disclosing their personal details.

Recommendation 17: Authorize the Chief Electoral Officer to provide copies of the preliminary and revised lists of electors to registered political parties during the election period.

Empower the Chief Electoral Officer to provide preliminary and revised lists of electors to registered political parties upon request during the election period. This proactive approach streamlines the distribution process, allowing parties to access relevant information promptly, even before official nominations are confirmed. Such efficiency can improve campaign planning and outreach efforts.

Recommendation 18: Clarify the distribution of lists of electors after ordinary polling day.

Clarify that preliminary and revised lists of electors are intended solely for use during the election period and should not be provided to political parties or candidates after ordinary polling day. This clarification aims to prevent misuse of elector information post-election, ensuring that sensitive data is appropriately handled and protected.

2021 Electoral Modifications and Post-Election Recommendations

In 2021, Elections NB published *Electoral Modifications and Post-Election Recommendations*, specifically addressing municipal elections and relevant updates to elections processes and legislation. The following are high-level summaries of those recommendations which are relevant to the topic of data privacy.

A complete copy of those recommendations that are relevant to data privacy is included in **Appendix A**. These recommendations were targeted at the *Municipal Elections Act*, but summaries of the two recommendations pertinent to elector data privacy are as follows:

Recommendation 2: Voters List – Protecting Vulnerable Electors

The *Municipal Elections Act* has no provisions to protect the privacy or safety of vulnerable electors contained on a voters list. Parallel to Recommendation 16 in the 2019 publication, it was recommended that a provision be introduced to provide a method for vulnerable people to vote without forcing them to expose their name and address to an unknown quantity of people.

Recommendation 3: Collection and Publication of Candidate Information

Municipal candidates have their names, addresses, and gender posted online to allow electors to identify candidates. During the 2021 municipal elections, several candidates were not comfortable having their home addresses published. A temporary workaround was implemented which used the municipal returning offices as surrogate addresses, but a longer-term solution would gather this information to determine eligibility—but not publish it.

Further, it was recommended to remove the requirement to gather the candidate's "occupation" (job) and that sex be changed to gender for information gathering and that this be gathered on a voluntary basis and not published.

Elector List Data Collection and Disclosure

Current Collection and Sharing Requirements

All Canadian provinces maintain permanent lists of electors between elections. In New Brunswick, this is known as the Register of Electors and it contains the following pieces of information:

- Name, given and surname
- Civic address
- Mailing address if different from civic address
- Sex

Electors are removed from the Register of Electors if they move out of New Brunswick or die. An elector may also request their name to be deleted from the register, but they must be added to the elector list in order to vote in any subsequent election.

Significant quantities of this data are gathered through other entities. This includes Elections Canada, New Brunswick Vital Statistics, Service New Brunswick, which all support maintaining an accurate and up-to-date picture of eligible electors within New Brunswick in addition to voter self-registration.

The elector list is important for the running of an election itself, electoral transparency, and is a key piece of information that campaigns use to support their engagement efforts. However, concerns exist around the lack of safeguards for the protection of this data.

Elections NB is required to provide the elector list to all political parties in provincial elections and nominated candidates in municipal, school board, and provincial elections.

The list of electors (or “elector list,” which will be used interchangeably throughout this paper) collects several data points from New Brunswick citizens. The list takes on several iterations as the electoral process progresses:

- The preliminary list of electors, which is created at the start of an election using information drawn from the Register of Electors.
- The revised list of electors, which are iterations of the list of electors developed after the preliminary list of electors is issued for an election.
- The final list of electors, prepared after the election has concluded representing all eligible, registered voters after the polling stations had closed.

The elector list collects the following pieces of information:

- Name, given and surname
- Civic address
- Mailing address if different from civic address
- Sex

While much of this data is commonly collected by election management bodies, collection of sex/gender data is not universal among Canadian jurisdictions.

As is the case with the Register of Electors, electors are removed from the elector list if they move out of New Brunswick or die; however, unlike the Register of Electors, there is no mechanism for an individual to voluntarily be removed from this list if they want to vote. If an eligible elector chooses not to be included in the Register of Electors, they must be included on the elector list to exercise their right to vote. As a result of being on the elector list, their information must then be shared with all political parties and nominated candidates in municipal, school board, and provincial elections.

Jurisdictional Comparison

The norm of sharing elector lists with political parties or candidates by an election management body is by no means unique to New Brunswick and is a tradition and expectation throughout most, but not all, liberal democracies. However, jurisdictions are taking measures to reduce risks to individuals while ensuring that elections are conducted fairly, accurately, and in a transparent and trustworthy fashion.

Exclusion from the Elector List

An increasing number of jurisdictions are now providing methods to opt-out of having personal information shared with candidates and political parties.

Individuals may have good reason to not want their information shared. This includes, but is not limited to, police officers, prosecutors, or individuals who have been the victims of domestic or gang violence, all of whom have good reason to not want their civic addresses and names released to a broad and difficult to trace population of elections workers and campaign volunteers. It is possible to conduct a free, open, and transparent election without compromising the safety of people whose privacy is paramount to their safety.

Elector lists that exclude individuals face a technical difficulty—the same elector list that is shared with political entities is used to verify voters at the voting booth, their names are then struck off, and this information shared with political parties.

Elections British Columbia (EBC) resolves this by flagging certain individuals as requiring elevated permissions to access their personal information on the elector list. These individuals lose the ability to vote at a standard voting booth; however, they are permitted to vote by mail or to vote at a Returning Office, where the Returning Officer can view the complete elector list and verify the voter. EBC distributes information to these individuals to ensure they are made aware of how their voting situation is unique and works with these individuals to ensure their votes count. Individual requests to be excluded from the list are evaluated, and a good reason is required to participate in this solution, but overall, the program is cited by EBC as a success.

Elections Nova Scotia (ENS) also permits individuals to request exclusion from the voter list. In Nova Scotia, these people are simply removed from the list. When the time comes to vote, they are "registered" at the polling station where they are eligible to vote. They are not included in any lists that are distributed to political parties.

Elections Canada (EC) provides the option for electors to write to EC to request exclusion from the elector list. Their website notes that out of about 28.4 million eligible electors in 2023, requests for exclusion have only been received from 321 electors.

Sharing of the Elector List

While elector lists are still broadly shared with political parties and candidates, some entities have taken measures to encourage a more limited distribution of the elector lists.

EBC has taken the measure of encouraging candidates to not exercise their right to access the list unless they feel they must. While candidates are free to access it, they are encouraged to first reach out to their political party and attempt to access the data through them. By distributing the data through political parties first, and candidates second and only if required, EBC reduces the number of points of contact that the list travels through—making tracking breaches easier and reducing the overall risk that they occur in the first place.

Data Privacy Policy

Various jurisdictions have undertaken measures to ensure that political parties and candidates are good stewards of the data they receive.

British Columbia has passed legislation that requires entities receiving electoral data to have a privacy policy that is approved by the Chief Electoral Officer of EBC. EBC also provides policy templates to support political parties, candidates, individuals, and local governments who are set to receive data. Entities are free to write their own policies, however, and the criteria for what constitutes an acceptable policy are iterated in legislation.

British Columbia's legislation reserves the right to audit political parties for compliance with these policies, but this power has yet to be deployed. EBC has so far preferred to do voluntary compliance surveys to remind political parties of their own policies and encourage compliance.

Nova Scotia does not require that political parties submit a privacy policy per British Columbia and does not give its elections agency that authority. However, ENS developed guidelines to support political parties in responsibly managing elector personal information. Political entities in Nova Scotia are strongly encouraged to adopt the comprehensive guidelines provided by Elections Nova Scotia (ENS). These guidelines serve as a framework to guide political entities in developing their own robust privacy measures, ensuring the protection and secure handling of elector personal information.

Political entities, including registered political parties, independent candidates, and Members of the Legislative Assembly, are advised to incorporate specific privacy practices that align with best practices recognized both provincially and nationally. These practices include the secure storage of personal information, limited access to sensitive data, and strict protocols for the disposal of elector information after use.

The content of the privacy policies encouraged by Nova Scotia focuses the following:

Data Minimization	Political entities are encouraged to collect only the information that is necessary for electoral purposes, such as communication with electors, campaign planning, and fundraising activities, reducing the risk of data breaches by limiting the volume of information collected.
Secure Access and Storage	The guidelines outline security measures to protect stored data, including using encrypted databases, secure servers, and restricted access protocols to ensure that only authorized personnel can access sensitive information. Physical security measures, such as locked filing cabinets for any paper records and controlled access to storage areas, are also highlighted as important aspects of a robust data security approach.
Training and Awareness	Political entities are encouraged to conduct regular training sessions for all individuals who handle elector personal information. These training programs should cover the importance of data protection, the specific measures outlined in the privacy policy, and the legal consequences of privacy breaches.
Breach Notification	Political parties should have a clear breach notification procedure. The guidelines recommend that political entities have plans in place to quickly identify and respond to any data breaches, including immediate containment and assessment of the breach, followed by appropriate reporting to Elections Nova Scotia and affected individuals if necessary.
Data Disposal and Destruction	After the electoral purpose has been served, secure and irreversible destruction of elector personal information is required. The guidelines provide specific methods for the destruction of both physical and digital records, ensuring that information cannot be reconstructed or retrieved.

Although Nova Scotia does not impose a formal requirement for political entities to submit privacy policies for review, the framework provided by ENS represents a proactive approach to privacy protection.

Nova Scotia also permits, by law, for ENS to include fictitious data in its elector list. This "junk data," which does not actually represent any real electors, is used to track potentially unauthorized use of data. While these security measures are not perfect, and a sophisticated actor could identify this data and remove it, it is a relatively easy way to track the identity of data and potentially track the source of a data breach should one occur.

Elections Canada (EC) has undergone change in its electoral data approaches in the last decade, and Parliament is reviewing potential further updates to data privacy.

In 2018, the *Elections Modernization Act* required political parties to develop their own privacy policies surrounding data that they collect. This is distinct from data that is provided by the electoral agency, but as noted in the risk analysis, this data can form a non-trivial component to data at-risk while conducting an election. The *Elections Modernization Act* (2018) requires federal political parties to post to their websites a privacy policy covering the following:

- The types of data collected, and how it is collected.
- How the political party protects personal information under its control.
- How the political party uses personal information under its control and under what circumstances that personal information may be sold to any person or entity.
- A statement indicating the training concerning the collection and use of personal information to be given to any employee of the political party who could have access to personal information under their control.
- A statement indicating the political party's practices concerning personal information created from online activity and its use of cookies.
- The name and contact of a person to whom concerns about the policy can be addressed.

While the overall impact of these policies versus British Columbia's may be less, it provides transparency to the public and can be viewed as a steppingstone in preparing political parties for more developed discussions around data privacy. In 2019, as noted in the earlier section in this paper reviewing incidents surrounding privacy, the Privacy Commissioner reviewed the privacy policies developed by the political parties and provided criticism. In the opinion of the Privacy Commissioner, the policies failed to sufficiently outline specific limitations on the use of data, detailed information on how long information is kept, security safeguards to protect data, and the ability for individuals to check if data kept on them by political parties is accurate. The Privacy Commissioner noted that privacy policies should be in keeping with the Ten Principles of Fair Information, as outlined in the *Personal Information Protection and Electronic Documents Act (2002)*.

Bill C-65, the *Electoral Participation Act*, is a piece of federal legislation that as of this report's writing, has completed its second reading (June 2024) and is under review by committee. It would provide a framework much closer, but different, than the one presently deployed in British Columbia. There is presently controversy surrounding some aspects of the bill, including changing the elections date and updates to how the law would interpret voter's intent in incorrectly completed ballots; however, political parties have not appeared to publicly dispute (in either the press or House of Commons) the aspects surrounding data privacy.

The *Electoral Participation Act* would require political parties to develop a publicly available privacy policy that would:

- Designate a privacy officer and sharing their name and contact information.
- Share the types of personal information that the political party collects, retains, uses, discloses and disposes of. These must be explained via illustrative examples.
- Outline training that staff undertake to comply with the privacy policy.
- Outline security measures, both physical and digital, that will be used to secure data.
- Require the political party to, in the case of a breach, respond to that breach by ensuring individuals whose data are compromised are informed if there is reason to believe there may be any harms or risk generated by the breach.
- Ensure that anybody who receives data covered by the policy agrees to follow, at a minimum, the privacy requirements of their privacy policy.
- Require the political party to meet once a year with the Chief Electoral Officer on the subject of data privacy.
- Require the political party to not mislead the public about the collection of personal information, sell information, or cause harm by disseminating information.

Overall, the proposed federal legislation is of a slightly different scope than the legislation enacted in British Columbia. The list of electors is not an explicit component of this legislation. However, given how political parties connect data received from the elector list to data they have collected themselves, this policy covers the broad datasets that political parties operate on rather than simply the original list[1].

Elections Ontario (EO) also requires that a privacy policy be developed and approved by its CEO. The privacy policy must comply with the "Guidelines for the Use of Electoral Products," which is a 32-page document provided to political parties (and the public) that outlines the appropriate use of the elector list.

[1]Note that British Columbia has other privacy legislation relating to information that is gathered on individuals that apply broadly to entities who operate there, including political parties. The provincial and federal jurisdictions are not a 1:1 comparison, and the different scope of the BC framework can be interpreted as focusing on the elector list more closely, at least in part because other legislation already covers data that is collected by the parties themselves.

The guidelines consist of two parts. First, political parties and their agents receiving elector lists must attest to the following:

- Understanding that data is for electoral and not commercial purposes
- Understanding of importance of protecting elector data
- Understanding of safeguard measures to protect electors' personal information and confirm compliance with privacy policies.
- Confirm intention to destroy elector list after election.

Second, they must complete a signed form (called an F0101) that is filed with EO and kept on record. This is not dissimilar from the present practice of New Brunswick.

Where EO goes further, is that the privacy policy requires:

- F0101s to be collected from every individual to whom the list is subsequently distributed.
- Specifics as to how the elector data is to be reproduced, stored, or transmitted, restricting these cases to only those specifically related to electoral activities.
- Details on how data is to be destroyed after use such that it cannot be reconstructed.
- The appointment of a Chief Privacy Officer within the political party.
- Limitations on access to electors' personal information as much as possible and ensuring that all who have access to it comply with the agreement (F0101).
- Guidelines on appropriate password creation and management.
- Securing and encrypting electronic records and avoiding transmitting elector data by email when not on a secured network.
- Processes and measures in case of a privacy breach, including documenting the circumstances, review of policies, and informing the Chief Electoral Officer of Ontario.

Overall, Ontario's requirements are slightly less onerous than British Columbia's, in large part because of a lack of audit mechanism. However, the requirements imposed in Ontario are a substantial step in the right direction for the protection of elector's data privacy.

The **European Union** (EU) has put in place the General Data Protection Regulation (GDPR), a comprehensive data privacy law that came into effect on May 25, 2018. It aims to protect individuals' personal data by establishing strict guidelines on data processing, storage, and sharing. GDPR applies to any organization handling the personal data of EU citizens, regardless of the organization's location.

Regarding political parties, GDPR covers how they collect, process, and store personal data, including information about political opinions, which is classified as "special category data." Political parties must have a valid legal basis (e.g., explicit consent or legitimate interest) to process such data and must implement safeguards to protect individuals' privacy and rights.

Areas for Improvement & Risk Mitigation

Based on the jurisdictional findings across Canada, there are multiple areas where improvements can be made to better mitigate the risks that inappropriate data handling or breaches could pose to both voters themselves and public trust in the electoral system.

Areas for Improvement

Training. The current training provided to candidates and political parties on the election process could be enhanced with further and more thorough privacy awareness training. Feedback from political parties indicate that although the current training provided is appreciated and necessary, more training on privacy awareness would be helpful.

Alternatives include outsourcing this training or developing this as a competency within Elections NB. Given that other provinces share similar concerns and are facing similar issues, in the context of non-legislative-specific training about handling elector's data, there may be an opportunity to co-develop something with another jurisdiction.

With the cooperation of political parties, this training could be distributed to political parties, achieving a more standardized result. Sessions could be combined with other relevant training on cyber-security.

Information Sharing.

- Elections NB produces an information flyer in advance of elections that is mailed to every household. It could include a section on protection of personal information. Raising awareness around data privacy with the public could reduce concerns or clarify how political parties get their data, ensuring that individuals know exactly what information (which is relatively limited) is actually distributed by Elections NB versus bought or produced privately.
- Elections NB could host a speaker series/bring in keynote speakers to raise awareness of the topic, inviting political party representatives to raise awareness and start conversations around privacy.
- Elections NB could make it a standing item on the agenda for their advisory committees that include registered political parties.
- This could be an area to partner with the Office of the Ombud and leverage their mandate and expertise Under the *Right to Information and Protection of Privacy Act*.

Public Engagement.

- Elections NB could survey voters and get their opinions on privacy and protection of personal information, then publish the results.

Risks to Candidates

Threats. Threats (vandalism, email and phone threats, cyber-bullying) to candidates present risks to their safety and will force potential candidates to reconsider running for public office. These threats have a personal impact to candidate safety, privacy and security. There have been several instances in the media regarding cyber-bullying, and threatening phone messages and email to a variety of political candidates at the federal and provincial level, resulting in candidates and elected officials choosing not to run in an election. The overall result limits effective representation of the population and degrades the democratic process.

Mitigating this threat comes by protecting candidates by providing effective legal deterrents with severe consequences to perpetrators, and by providing security where needed to candidates or elected officials receiving threats.

Risks to Electors

Lack of Accountability and Oversight. Current legislation does not provide sufficient accountability and oversight for users of elector lists to ensure they use them appropriately and respect voter privacy. Political parties are not currently required by law to have a privacy policy and as such Elections NB has no way to enforce privacy legislation once the voter lists are provided to them. The lack of accountability and oversight puts elector data at much greater risk of exposure without safeguards in place.

The lack of accountability and oversight expands beyond elector lists provided by Elections NB. It must be pointed out that elector lists are only one input into the elector profiles created by candidates and political parties. A much larger set of data points are collected and stored in their databases and software applications for analysis and voter predictions. Recent federal legislation has highlighted the need for more accountability by political parties.

This was an issue identified in the 2019 paper on *Modernizing New Brunswick's Electoral Legislation* where it was noted that the Chief Electoral Officer does not have the authority to enforce voter privacy, and there is no legislation which governs the custody or care of elector's personal information once it is passed on to candidates and the political parties.

Mitigating this threat can be performed using combinations of several possible actions of different degrees of commitment and difficulty of implementation:

- Develop a comprehensive privacy regime in legislation that addresses all the risks identified in this document, clearly establishing oversight rules and actions, such as those that are identified later in this document.
- Revise the *Elections Act* to empower the CEO to require a privacy policy be submitted by political parties for approval. This update should outline in legislation clear requirements and standards for what qualifies as a sufficient privacy policy to address the issues outlined in this paper. British Columbia's legislation would serve as a starting point and provide precedent for such updates.
- Include the capacity for the Ombud to perform audits, a minimum in the case of a privacy breach, but ideally at the Ombud's discretion or at the request of the CEO. British Columbia empowers their CEO to initiate an audit of privacy policy compliance.
- Similar to section 20.14 of the *Elections Act*, require political parties to respond to requests from individuals to send that person all of the information in the political party's possession relating to that person, regardless of how the data was acquired.
- At a minimum, political parties could engage with Elections NB to voluntarily undertake privacy policies guided by Elections NB to ensure that the issues raised here are addressed. This could avoid the more stringent requirements of British Columbia if stakeholders do not feel prepared to comply to a higher standard, while reducing the aggregate risk and serving as a potential steppingstone to mutually beneficial, stronger policies later when political parties feel prepared to deploy more stringent measures.
- Update the forms presently given to candidates requesting access to elector lists to include agreement to further measures to protect elector privacy, including but not limited to:
    - Informing Elections NB of any breaches that occur.
    - Agreeing to training for any staff in possession of the list for the correct handling of sensitive data, or attestation that these individuals will have already received training.
    - Agreeing to form "chain of custody" records to track who has received data, for what purposes, and requiring that these individuals also complete a copy of the form and file it with Elections NB.

- At a minimum, ensure that the individuals who will receive the elector list are informed of their responsibilities, and that a signed attestation to that effect is filed with Elections NB. This is technically required by the present Elections NB agreement that receivers of elector lists must sign, but there is no clear enforcement mechanism or requirement that the form completed by those subsequently handling the data is filed with Elections NB.
- Encouraging political parties (where applicable) to voluntarily suggest that candidates not individually pursue elector lists, instead acting as a single point of contact for the list and distributing it, per the requirements outlined above, to their candidates.
- Review the *Elections Act* to make the collection of gender data voluntary for electors. Review all data that is collected and ensure that it constitutes the minimum required data for elections to be conducted and for political parties and candidates to be supported in engaging with the electorate.
- Ensuring that all above recommendations, to the degree to which they are implemented, are equally reflected in the *Municipal Elections Act*.

Threats to voter privacy and possible risk to safety. Voters who feel at risk of attack or violation of privacy have few options to keep their information private without removing themselves from the voters list. This is being done effectively in BC by screening 'at risk' voters from the elector lists while still allowing them to vote through an alternative method. At risk voters could include law enforcement, judges, and others who, due to the sensitivity of their profession or legal circumstances, wish to remain off the electors list.

Several methods can be implemented to mitigate this risk:

- Engage tools such as data redaction software to block out private information on elector lists and other reports containing personal information of those who wish to have their information protected.
- Flag voter records that are to be made private and leave private records off the polling station lists but allow senior staff access to the complete list. Allow these flagged voters to vote by another method such as vote by mail, or directly with the Returning Officer (RO), who will have access to their data. Technical changes will be required to implement this, but Elections BC has demonstrated one of multiple possible approaches.

Other Personal Data Collected By Elections NB

Current Requirements

Information from Donors: It is a requirement for political parties to collect information from individuals who make donations. Subsequently, political parties submit financial returns to Elections NB who publishes the returns. The returns include the amount that was donated, the name of the individual who made the donation, and their civic address (if they donated over $100.)

Information on Political Advertisement Printer(s): In addition to the name of the registered political party or the candidate on whose behalf it was ordered, every printed political advertisement must include the name and address of its printer.

Information on Ballot Printer(s): Elections NB is required to collect the name of everyone who has a hand in developing and printing the provincial election ballots.

Information on Candidates, Agents and Nominators: Elections NB collects the name, address, gender, and occupation of candidates. This is collected at the nomination stage, along with information for contacting a candidate's agents, as well as all of their nominators' names and addresses. Nomination paper information is sometimes requested by candidates' opponents; however, the *Elections Act* does not clearly address if such papers are election documents that may be inspected as public records or if they may only be inspected by an order of a judge.

Information on Returning Officers and Election Officers: Elections NB is required by law to annually publish in The Royal Gazette the names, occupations, and residential addresses of all appointed Returning Officers. Elections NB is also required to post a list of the names and addresses of the election officers and where they are working and provide full opportunity for inspection of the list by candidates, their agents or the public.

Jurisdictional Comparison

Information from Donors: Elections Nova Scotia (ENS) collects similar information to what is legislated in New Brunswick. Of note however, is that there is no requirement to publish the specific civic address of donors. Instead, ENS publishes the name of the community, but not the civic address, of the donor. Donors to provincial political parties in Nova Scotia are traceable if need-be, but do not automatically have their civic address published in a way accessible to the entire internet when they support the political party or candidate of their choice.

Elections British Columbia similarly does not publish the addresses of donors.

Information from Printers of Political Advertisements: Other jurisdictions do not require that "printer" information be published. This requirement appears outdated but is also low risk.

Information on Candidates: Information collected on candidates varies widely but has trended towards revealing less information due to concerns over safety and privacy. Nova Scotia collects the name and address of candidates and their agents but does not publish their addresses to the public.

Information on Returning Officers: The Federal Government releases the names, occupations, and civic addresses of Returning Officers, similarly to New Brunswick. Nova Scotia, however, validates that a Returning Officer resides in the electoral district they are representing, but does not appear to publish their civic address.

Areas for Improvement & Risk Mitigation

Areas for Improvement

Training: Developing or acquiring a general training package on privacy awareness and making it available to political parties, candidates and election workers would benefit all involved in appropriately handling privacy information during the elections process. This could be combined with other relevant training on cyber-security.

Brochures and Information Packages: Developing written materials on handling privacy information and distributing it to political parties, candidates and election workers can help build privacy awareness. This could be an area to partner with the Office of the Ombud and leverage their mandate and expertise under the *Right to Information and Protection of Privacy Act.*

Risks to Donors

Publishing of Civic Address: The current practise of including donors' civic addresses on financial returns published by Elections NB makes donors potential targets for retribution through threats, vandalism and bullying.

Mitigation of this risk can be accomplished by amending current legislation to withhold contact details from published donor lists.

It is recommended that legislation in New Brunswick be adjusted to reflect the same requirement as is the law in Nova Scotia. Nova Scotia has no on-going concerns on account of publishing less information with regard to civic addresses of donors. The information is still collected and could be audited should there be a reason for concern. Transparency of the nature of donations remains something that can be used by journalists, analysts, commentators, and political parties to hone their campaigns (e.g., the average size of donation or where donors tend to be from geographically.)

It is further recommended to explore options under section 63(1.1) of the *Political Process Financing Act* to determine whether addresses of political donors could be deemed "supporting documents" and are therefore at the prerogative of Elections NB to release or redact. While this is more ambiguous than changing the legislation, and should be examined with reference to precedent in any jurisdictions where similar cases have occurred, the wording of the legislation does not make it completely clear if the present practice is necessary for fulfillment of the law.

Risks to Candidates (including nominees and their agents)

Collecting Unnecessary Information on Candidates. Gender information is unnecessary and could be contentious. While a relatively small point of data, publicizing gender provides no obvious benefits to the electoral process. Candidates can, and almost certainly will, disclose their gender in some format via their campaigns. The method and format of doing so should principally be the candidate's choice—which reduces slightly the risk that Elections NB carries in managing data related to candidates. By the same logic, the requirement to collect "occupation" is unnecessary. Candidates will likely be public and candid in how they disclose their professional history, but their approach to doing so can be easily handled by the campaigns, the media, and the inquiring public.

To mitigate this risk, the information collected for candidates should be reviewed and stripped down to require only the data points essential to identify the candidate. For the vast majority of cases in provincial elections, this is simply their name and their party. However, the *Political Process Financing Act* requires that political parties' annual allowances are determined using a calculation including the proportion of male and female candidates in the previous general election.

Additional data such as the address of candidates is required by returning officers in municipal and school district elections to ensure the candidate is eligible to run in a particular municipality, ward, or school subdistrict. It may be possible only to publicly publish the general neighbourhood, or first three digits of the candidate's postal code, but this is not always adequately accurate. Nevertheless, not publishing a candidate's address would not expose them to unwanted public attention at their private residence.

Risks to Elections NB Staff

Public Availability of Election Worker Personal Information. Election workers, and specifically Returning Officers, are required to make their personal information public, such as home address. When the legislation was created, ROs were political appointees and subject to public scrutiny. Election workers needed to be supplied by and work as a pair, from lists supplied by the former government and opposition political parties. However, all election workers are now appointed by Elections NB, and are private citizens. The current legislation should be re-examined, as releasing this information publicly could make Elections NB staff targets of violence, threats and bullying.

To mitigate this risk, the legislation should be changed to remove requirement of publishing or posting personal information of Elections NB staff members to the public. If there was deemed a benefit to the public being able to send mail to a Returning Officer outside of an election period, this could be replaced with a mailing address or simply the address of the head office of Elections NB.

Discussions with Political Parties

Registered Political Parties Engagement

In preparing this discussion paper, attempts were made in the spring of 2024 to engage the five political parties registered at the time. The goal was to have input from the parties to better understand if they had concerns or suggestions that could be taken under consideration by Elections NB.

Unfortunately, only two political parties participated, and the input received did not give an obvious direction for next steps or implementation. Two other political parties acknowledged the request but did not respond to attempts to book time for providing feedback. One party never acknowledged the request or responded in any way.

The initial outreach consisted of an email request from the Chief Electoral Officer directly to the main contacts for each party. The CEO explained the nature of the project and asked for their participation in a confidential discussion with our consultants that would be based on a standard set of questions.

Our consultants followed up within 24 hours to explain the logistics and reiterate the confidential nature of the conversations. When the emails went unanswered or acknowledged, the consultants followed up with phone calls to each registered party office or via a party contact person.

These additional activities resulted in two meetings being booked and completed. Each meeting was attended by one registered party representative (staff or volunteer) and two consultants.

In one case, a registered party representative demonstrated awareness of operational privacy and data handling practices but could not provide detailed feedback on current affairs as they were new to the role. The other discussion made it obvious there was limited operational capacity to address these topics but neither had issues or concerns been raised internally in the past.

In addition to raising issues related to privacy and handling of personal information in published reports in 2019 and 2021, in April 2024 an information session was held with representatives of all five registered political parties in advance of the provincial general. At the session, the CEO discussed the previous recommendations and advised party representatives of this project. She alerted them there would be a request to participate and provide feedback. No one indicated concern, time constraints, or opposition to participating.

Discussion

Regardless of the level of engagement of the political parties, Elections NB has an organizational and ethical imperative to handle personal information appropriately and to recognize that legislation, regulations, and standards are evolving in this field. We have obligations as the stewards of data that voters and donors must provide to us under law.

For the past five years, Elections NB has been researching and sharing information related to protection of personal information and safe data handling practices. We have also advocated for legislative changes that would enhance requirements of the political parties in their treatment of the data that is provided to them under law. Additional attempts to raise these issues could be made using the tools of communications and advocacy.

It can be difficult for organizations to change in response to risks that have not been experienced but are only seen as being possibilities. Sharing examples of data breaches and harms that have occurred in New Brunswick and across the country might elevate the previous recommendations as a priority for future legislative amendments.

Another unknown is the capacity of the registered political parties to implement changes (if required) to their operational handling of data. The financial capacity of the political parties is public information and indicates limited resources for regular staffing or contract expertise. The three smallest political parties are particularly limited in resources.

In 2021, the most recent non-election year for which there is a published report, the political parties had the following net revenues, a significant part of which comes from legislated financing (annual allowances) based on voter support:

Party	Net Revenue	Annual Allowance
Progressive Conservative	$ 476,193	$ 237,813
Liberal	$ 319,215	$ 215,746
Green Party	$ 210,303	$ 100,536
People's Alliance	$ 85,308	$ 61,950
New Democratic Party	$ 63,383	$ 17,131

An untested option is whether political parties are open to implementing better practices if financial support was available to allow them to contract a person or firm to provide them with privacy expertise. This is not a novel suggestion. Political parties are currently reimbursed funds for hiring independent financial expertise (auditors) every year.

Recommendations

Depending on what the members of the Legislative Assembly determine is appropriate, there are multiple recommendations listed below that could be implemented, from a comprehensive regime with maximum privacy protection to minimal steps that merely encourage participants to better protect voter privacy while maintaining electoral integrity.

There are a number of changes with precedent across many jurisdictions which could alleviate concerns around data privacy in New Brunswick. Some will require buy-in sufficient to trigger legislative change, others may be achievable with either a policy or process change within Elections NB, or with voluntary engagement by political parties. Some recommendations may require establishing new programming and therefore require budget.

All recommendations should be interpreted, where applicable, as extending to municipal elections equally as to provincial elections.

Recommendations Requiring Legislative Change

Recommendations requiring legislative change will require more momentum, interest from stakeholders, and engagement to ensure that changes are sufficient and relevant to address privacy concerns raised by the status quo.

Recommendation	Description
Develop a comprehensive legislative regime to manage privacy risks	While having the benefit of addressing all issues in clear rules, the likelihood of having such legislation written and introduced is small, considering the effort and analysis needed, and the willingness of political parties to limit their own privacy practices.
Reduce data gathering requirements	Reduce legislated requirements to gather and/or publish data where not necessary. Many cases of this exist. Of note are: • Elector gender • Addresses of ballot printer and printers of political advertisements • Occupations of candidates Candidate gender, while it is collected by Elections NB for legitimate reasons surrounding PPFA allocations, may fall into the category of things which may be collected but not published. The collection of gender could also be made optional.

Recommendation	Description
Explore the use of fictitious data to track potential data breaches	While a measure that may not catch sophisticated actors, including fictitious data unique to each point of distribution is a practice in Nova Scotia which could support enforcement in the case of misuse of elector data. Knowledge that this is a practice may discourage handlers of the data from being loose with their storage of it.
Create further legal distinction between what is gathered and what is shared.	Some data points may be suitable to be collected but should not necessarily be shared automatically with the public, even if they remain available for scrutiny. For example, the *Political Process Financing Act* requires financial returns show the address of individuals making political contributions. The Act requires Elections NB to publish to their website all returns within 30 days of receiving them. This is more strenuous than what is expected in jurisdictions like British Columbia and Nova Scotia. This information could be either excluded completely or replaced with a neighbourhood or first three digits of the postal code associated with the contribution. Full addresses could be kept on record for audit as needed.
Provide a mechanism for electors to be either removed from the elector list or have their information concealed in versions of the list that reach political parties/candidates.	As has been recommended before, electors should have the ability to remove themselves from the elector list—this should be doable while retaining the ability to vote as multiple jurisdictions manage to accomplish. It is an additional policy decision what the standard ought to be in order to be removed. Given the potential complexity in managing systems to generate multiple levels of access privileges to listed electors, such a system could be fairly conservative in who is afforded access to it—at least to trial a solution, while providing protection to individuals for whom their address is potentially compromising information.
Require political parties to develop privacy policies regarding data they receive or collect, make these policies public, and appoint a Privacy Officer to field public questions or concerns about a party's collection of data.	Political parties are being expected to produce privacy policies in other jurisdictions, including at a federal level. Policies ideally cover both elector lists and Elections NB-related data and data that political parties procure or create themselves.

Recommendation	Description
Require political parties to develop and deploy privacy policies subject to approval by the CEO before receiving any elector data	At a minimum, political parties should be required to publicly post policies that can then be publicly scrutinized. Electors are then, in theory, better equipped to manage their relationships with political parties. However, ideally, political parties would submit their privacy policies to the CEO of Elections NB for approval. The standards for this approval would be outlined in legislation, similar to British Columbia.
Give Elections NB and/or Ombud the authority and necessary funding resources to audit compliance with privacy policies.	In addition to the policies being approved by the CEO, Elections NB should be empowered to audit compliance with policies that they approve. This power could be within the job of the Ombud and ideally is triggered at the prerogative of the CEO. While this power is relatively new to British Columbia, it shows promise in encouraging compliance with policies. This can be augmented with other, less punitive measures to encourage compliance and self-regulation. Any increase in oversight or audit duties must also be accompanied by an increase in resources provided to the agency in order to permit the work to be done.
Encourage single point of contact for data	Following the practice of Elections British Columbia, Elections NB can encourage political parties to act as a single point of distribution for data sharing with candidates. While candidates could retain the right to request the data should they so choose, restricting the number of points of access wherever possible is a solid first step. This in turn reduces the points of contact for establishing new data handling protocols. Applying additional recommendations to data practices will be easier if fewer stakeholders are directly engaged with the elector list.
Require registered political parties to meet with the CEO and/or Ombud at least once annually on the subject of privacy.	Mirroring potential future federal legislation, requiring political parties to devote one meeting per year to discussing data privacy with the CEO or Ombud helps ensure that these issues are addressed in a timely fashion and respond to new developments and risks. Ideally, this is done in conjunction with political parties having Privacy Officers who are authorized to speak and enact party policy on the subject of data privacy.

Recommendations Requiring Process or Policy Change

While they are the minority, some changes can likely be made without legislative adjustment. These also can serve as useful steppingstones to socializing the political culture in New Brunswick towards considering privacy in operations and potentially future legislative changes.

Recommendation	Description
Broaden the scope of the existing agreement form provided to recipients of elector data	Recipients of elector data in New Brunswick already agree to a number of conditions when they receive data. Without imposing conditions that might be challenged, this document can be expanded to cover additional stipulations, such as: • Attest that original documents will be deleted/destroyed after the election period. • Request, at a minimum, a short outline of data security practices, both digital and physical, that the person requesting the data will deploy to safeguard elector data. This could be in the style of a form that each party completes.
Advocate for the voluntary adoption of privacy policies by parties	Nova Scotia has successfully convinced political parties to voluntarily abide by self-imposed privacy policies. While Elections Nova Scotia is not equipped to audit or enforce these policies, this represents a step towards socializing political parties into considering privacy. Political parties seem more likely to accept taking on legislated requirements for privacy if they are already completely or mostly compliant due to voluntary adoption. If political parties are willing to voluntarily adopt policies covering, but are not necessarily limited to: • Physical and digital security measures around elector data • Training for all staff who handle data • Publishing a privacy policy on their website • Appointing an individual to field public questions about a party's privacy policy

Recommendations Requiring Funding, but not Legislative Change

Recommendation	Description
Work to create training program for volunteers/ campaign staff	Providing easily usable and available resources for party staff and volunteers to complete, which they can then attest to completing, would make it easier for political parties to adopt better privacy practices. Given that this is of interest to other provincial election management bodies, and that many if not most data handling best practices are common rather than specific to NB legislation, this could potentially be developed jointly with other jurisdictions. If deployable online, the cost to scale to more people would not be great.
Develop sessions, speakers, and more engagement on privacy with more senior party staff	With the goal being socializing political parties towards being willing interlocuters on privacy matters with Elections NB, organized sessions with external experts from other jurisdictions may be an effective method to encourage voluntary compliance with more stringent data privacy methods.
Conduct research/surveying on New Brunswicker's expectations and perspectives on data privacy	While national data exists, some data demonstrating that New Brunswickers care about how their data is treated may spur action. Tracking and potentially publishing correspondence related to elector's expressing concern over how their data has been shared with political parties without their knowledge may be a first start to measuring the weight of this issue to New Brunswickers.

Conclusion

This discussion paper builds upon previous insights and recommendations made by Elections NB to strengthen the handling of personal information. It presents updated information from other jurisdictions that are moving forward with policies and operational mechanisms for addressing modern privacy concerns.

We also wish to state our appreciation for the open and transparent conversations with elections officials in other Canadian jurisdictions who are attempting to work with political parties to de-risk the management of elector and donor data.

New Brunswick political parties will necessarily have to be part of the effort if these recommendations are to be implemented. There was limited engagement from them during the development of this discussion paper. Just as there was limited reaction to the recommendations offered by Elections NB in previous reports in 2019 and 2021, it may be that progress in adopting policies and approaches to strengthen data handling at the federal level, and in other provinces, may help to support change in New Brunswick.

Elections NB presents this discussion paper to the members of the Legislative Assembly for their consideration and debate to determine how robustly they wish to protect voter privacy. We call on the members to advocate for and support the efforts that they determine are appropriate in this province, and that will need to be undertaken by Elections NB and other political party participants to strengthen privacy protections for voters, political donors, election workers and candidates in response to this document.

Appendix A: Original Recommendations Related to Data Privacy

Modernizing New Brunswick's Electoral Legislation (2019)

The following is a verbatim repetition of the recommendations related to the general topic of elector data privacy and protection of data made in 2019, included here for reference.

Recommendation 14: Require the recipient of a list of electors to file a privacy policy with the Chief Electoral Officer before receiving such a list.

Amend the *Elections Act* to provide as follows:

i. require a person who is entitled to receive a list of electors under section 20, 20.5, 41 or 42.1 to file with the Chief Electoral Officer a privacy policy for approval before receiving such a list;

ii. the privacy policy shall be in the form prescribed by the Chief Electoral Officer and shall set out, to the satisfaction of the Chief Electoral Officer, those reasonable security arrangements as are necessary to protect the personal information contained in the list from the risk of unauthorized access, collection, use, disclosure or disposal;

iii. authorize the Chief Electoral Officer to waive the requirement to file a privacy policy if a privacy policy has been previously filed by the same person;

iv. authorize the Integrity Commissioner to receive and investigate complaints from the public related to the collection, use and disclosure of personal information contained in a list of electors by a recipient of the list;

v. authorize the Integrity Commissioner to conduct an audit in order to evaluate the level of conformity with a privacy policy, which could be conducted on the Commissioner's own initiative or on request of the Chief Electoral Officer; and

vi. in the event of a breach or a suspected breach of privacy with respect to personal information contained in a list of electors provided to a person under those sections:

a) require the person to immediately advise the Chief Electoral Officer of the breach or suspected breach and to take any measures that the Chief Electoral Officer directs to rectify the breach;

b) authorize the Chief Electoral Officer to take such measures as are considered necessary to rectify the breach, including advising affected electors; and

c) require the Chief Electoral Officer to refer a reported breach or suspected breach to the Integrity Commissioner for investigation and to make recommendations.

ii. Content of lists of electors

As indicated above, the requirement to provide lists of electors to various political parties and individuals is found in sections 20, 20.5, 41 and 42.1 of the *Elections Act*. The Act prescribes which personal information is to be included in this list in only two of these instances – subsections 20.5(2) and 42.1(1). The Chief Electoral Officer has provided the other lists in accordance with the requirements of subsections 20.5(2) and 42.1(1), but it would be preferable that all four provisions were consistent.

Recommendation 15: Consistently prescribe the contents of lists of electors provided to political parties and other individuals.

Amend subsection 20(3) and paragraph 41(b) of the *Elections Act* to limit the data included in the lists of electors provided under those provisions to the following personal information of electors – surnames, given names, sex, civic addresses and mailing addresses.

iii. Protecting the personal information of vulnerable electors

The *Elections Act* has no provision to protect the privacy or safety of vulnerable electors contained on a list of electors. All electors must appear on a list of electors in order to vote and the lists of electors must be shared with registered political parties and candidates, therefore, a vulnerable elector cannot vote without sharing his or her name and current address with an unknown number of persons. A number of jurisdictions across the country have taken measures to address this serious concern. The Chief Electoral Officer of Ontario, on the written request of a voter, may redact from any record made available to political entities, data partners and to the public, any information that the Chief Electoral Officer reasonably believes would, if made available, endanger the life, health or security of the elector. An elector in Manitoba may request that the Chief Electoral Officer not include the elector's information in the register of voters or a voters list in order to protect the voter's personal security. In British Columbia, the Chief Electoral Officer may prepare a list of voters, including a list of voters used for election purposes, which omits or obscures the address of a voter or other information about a voter in order to protect the privacy or security of the voter.

Recommendation 16: Provide a means to protect an elector's safety and to opt-out of sharing with political parties.

Amend the *Elections Act* to permit the Chief Electoral Officer, on the request of an elector, to redact any record made available to political entities, data partners and to the public, any information that the Chief Electoral Officer reasonably believes would, if made available, endanger the life, health or security of the elector. This includes the anonymization of personal information included on a list of electors provided to candidates and registered political parties during an election period.

iv. Provision of a list of electors to registered political parties during an election period

Subsection 20(3) of the *Elections Act* authorizes a returning officer to provide the preliminary list of electors for his or her electoral district to each "recognized party which has an officially nominated candidate in the electoral district." A person's nomination papers must be accepted by a returning officer prior to becoming an officially nominated candidate. Similarly, section 41 of the Act authorizes a returning officer to provide a copy of the revised list of electors for his or her electoral district to each party and candidate who received a copy of the preliminary list of electors. These provisions mean that a recognized party cannot receive a preliminary list of electors for an electoral district until their candidate's nomination has been officially accepted by the local returning officer. Further, those political parties that choose to centrally manage campaigns must work with 49 separate lists of electors that have been picked up locally by a candidate's agent, who then must ship them to a central point from around the Province. This is a cumbersome process and makes personal information vulnerable to loss.

It is therefore recommended that, at the start of the election period, the Chief Electoral Officer be authorized to send the preliminary list of electors for each electoral district to the headquarters of each registered political party on request, notwithstanding there may not yet be an officially nominated candidate in each electoral district. This is similar to the process to supply an annual extract from the register of electors to members of the Legislative Assembly. On request, the Chief Electoral Officer should also be authorized to send the revised lists of electors to the headquarters of each registered political parties before advance and ordinary polling days.

As this service would only be on the request of the registered political parties, those parties that continue to use decentralized campaigns could continue to obtain information from the local returning officers, as is the case now.

Recommendation 17: Authorize the Chief Electoral Officer to provide copies of the preliminary and revised lists of electors to registered political parties during the election period.

a) Amend section 20 of the *Elections Act* to authorize the Chief Electoral Officer, when the preliminary lists of electors have been created, to send them to the headquarters of each registered political party on request, notwithstanding that there may not yet be an officially nominated candidate in each electoral district.

b) Amend section 41 of the *Elections Act* to authorize the Chief Electoral Officer, on request, to send the revised lists of electors to the headquarters of each registered political party when those lists are required to be provided to a candidate during an election.

v. Provision of a list of electors following the close of polls on Election Day

As referred to above, subsection 20(3) of the *Elections Act* requires a returning officer to provide a copy of the list of electors to each recognized party which has an officially nominated candidate in the electoral district and to each independent candidate who has been officially nominated in the electoral district. Further, section 41 of the E*lections Act* requires a returning officer to provide a copy of the revised list of electors to each party and candidate who was provided with a copy of the preliminary lists of electors prior to the advance and ordinary polls.

Subsection 42(2) of the *Elections Act* provides as follows:

> **42**(2) A political party or a candidate who has been furnished with copies of the preliminary and official lists of electors may use the lists for communicating with electors during the election period, including communications for the purpose of soliciting contributions and recruiting party members, but for no other purpose.

Section 42.1 requires the Chief Electoral Officer to complete all revisions after Election Day, and to prepare a final list of electors of all electors whose names have been included in or added to the official list of electors by the close of polls on ordinary polling day. The final list is provided to the elected member in respect of his or her electoral district and, on request, one copy of the list is provided to each registered political party.

Elections NB often receives requests from candidates following the election asking for the list of electors, particularly with information as to who voted. This information is relevant during the electoral period, and is readily available to scrutineers in the polling stations while they are open, but has no relevance after the polls close. Although there is no authority to provide lists of electors with this information after ordinary polling day, it would be beneficial to Elections NB if it were clearly stated that this was not permissible. In comparison, the provision of a list of electors to candidates in municipal elections after Election Day is prohibited under subsection 12.1(3) of the *Municipal Elections Act*.

Recommendation 18: Clarify the distribution of lists of electors after ordinary polling day.

Amend the *Elections Act* to provide that preliminary lists of electors prepared under section 20 and revised lists of electors prepared under section 36 are intended to be used only during the election period and will not be provided to a political party or candidate after the close of the polls on ordinary polling day.

2021 Electoral Modifications and Post-Election Recommendations

The following is a verbatim repetition of the recommendations related to the general topic of elector data privacy and protection of data made in 2021, included here for reference.

Recommendation 2: Voters List – Protecting Vulnerable Electors: The Municipal Electoral Officer recommends that a means be provided to protect an elector's safety by permitting the Municipal Electoral Officer, on the request of the elector, to redact the elector's personal information included on a voters list provided to a candidate during an election.

In *Modernizing New Brunswick's Electoral Legislation*, the Chief Electoral Officer recommended the *Elections Act* be amended as follows:

> Amend the *Elections Act* to permit the Chief Electoral Officer, on the request of an elector, to redact any record made available to political entities, data partners and to the public, any information that the Chief Electoral Officer reasonably believes would, if made available, endanger the life, health or security of the elector. This includes the anonymization of personal information included on a list of electors provided to candidates and registered political parties during an election period.

Like the *Elections Act*, the *Municipal Elections Act* has no provision to protect the privacy or safety of vulnerable electors contained on a voters list. All electors must appear on a voters list in order to vote and the voters list must be shared with candidates on request. Therefore, a vulnerable elector cannot vote without sharing their name and current address with an unknown number of persons.

It is important to be aware that protecting electors from the improper use of the voters list is not just a theoretical concern. In the context of Calgary, Alberta's fall 2021 mayoral race, the Calgary Police raised significant security concerns with all candidates having access to voters' personal information due to a candidate harassing and threatening some voters.

A number of jurisdictions across the country have taken measures to address this serious concern. The Chief Electoral Officer of Ontario, on the written request of a voter, may redact from any record made available to political entities, data sharing partners and to the public, any information that the Chief Electoral Officer reasonably believes would, if made available, endanger the life, health or security of the elector. An elector in Manitoba may request that the Chief Electoral Officer not include the elector's information in the register of voters or a voters list in order to protect the voter's personal security. In British Columbia, the Chief Electoral Officer may prepare a list of voters, including a list of voters used for election purposes, which omits or obscures the address of a voter or other information about a voter in order to protect the privacy or security of the voter.

It is the opinion of the Municipal Electoral Officer that a similar amendment should be made to the *Municipal Elections Act* to protect electors on their request.

Recommendation 3: Collection and Publication of Candidate Information: The Municipal Electoral Officer recommends that candidates be provided the option to determine what additional information about them appears along with their name on the list of candidates posted to the Elections NB website or published in reports. For two decades, each candidate's name, address and gender have been posted online to allow electors to identify the candidates, while 30 years ago, each candidate's name, address and occupation were printed on the ballots.

In the 2021 local elections, a handful of candidates requested that their home addresses not be included on the Elections New Brunswick website. In three instances, these were young, female candidates who were not comfortable having their personal address displayed publicly. A temporary programming change was made to allow the address of the municipal returning office to be used as the default service address of these candidates.

The Municipal Electoral Officer recommends that candidates still be required to include their civic address on the nomination papers as this is needed for the municipal returning officer to confirm a candidate's eligibility.

The Municipal Electoral Officer also recommends that the format for presenting a candidate's name posted on Elections New Brunswick's website be revised to exclude gender. Further, on candidate nomination papers, the term "gender" will replace references to "sex". There is no legislated requirement to include this information on the public website, but simply continued past practice when Elections New Brunswick began providing candidate information on the internet. Members of the public have questioned why the sex of candidates are included on the Elections New Brunswick website with the list of candidates.

Although a candidate's gender will no longer appear on the candidate information webpage, Elections New Brunswick will continue to collect this information from candidates on a voluntary basis. This data is often requested by social science researchers and groups advocating for greater participation by female candidate; therefore, the aggregate data will continue to be published in final election reports. It should be noted, however, that advocacy groups will not have access to this information on the public website during an election. If they wish to have this information during the election, they will have to contact Elections New Brunswick directly or contact candidates individually.

In addition, it is recommended that the requirement for a candidate to provide their occupation on their nomination papers be eliminated. There is no current relevance to the collection of this particular information, no historical context available to explain the original rationale for its collection, and it is not published in any election report.