
INVESTIGATION REPORT

P19-03

PIPEDA-035913

AggregatIQ Data Services Ltd.

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

Daniel Therrien
Privacy Commissioner of Canada

November 26, 2019

CanLII Cite: 2019 BCIPC 48
Quicklaw Cite: [2019] B.C.I.P.C.D. No. 48

TABLE OF CONTENTS

Table of Contents.....	1
Commissioners' message.....	2
Executive summary.....	3
1 Background & methodology.....	5
Background.....	5
Methodology.....	6
2 Legislation.....	7
2.1 PIPA and PIPEDA.....	7
3 Issues.....	9
4 Investigation and findings.....	10
Issue 1: What personal information did AIQ collect, use, and disclose to do work on behalf of its clients?.....	10
4.1 SCL Elections and Cambridge Analytica.....	10
4.2 Brexit campaigns.....	12
4.3 Canadian clients.....	16
Issue 2: Was AIQ compliant with consent requirements for the collection, use, or disclosure of personal information?.....	18
4.4 Findings and recommendations.....	23
Issue 3: Did AIQ take reasonable security measures to protect the personal information in its custody or control?.....	24
4.5 Findings and recommendations.....	26
5 Conclusion.....	26

COMMISSIONERS' MESSAGE

AggregateIQ Data Services, Ltd.'s ("AIQ") work for high-profile political campaigns in the United States and the United Kingdom draws domestic and international attention and scrutiny. Our investigation into AIQ's activities illustrates how cross-jurisdictional digital data practices associated with internationally active companies like AIQ create significant privacy implications for businesses, regulators and, most importantly, citizens around the globe.

As our digital presence grows, it becomes more and more imperative that the activities of tech companies operating across borders respect privacy obligations in all jurisdictions in which they operate. This is especially so in the case of handling sensitive information such as that which could reveal political opinions and personal beliefs, as described in this investigation report.

The public has a general sense that there are rules governing the collection, use and disclosure of their personal information. Citizens expect that these rules protect them – and their data. But when personal information is being used in a truly global digital world, questions arise: which privacy rules apply, who enforces them, and how? An organization across the world might collect and use individuals' information, or a local organization might collect it but use it in another jurisdiction. In either case, which rules apply and how?

This is obviously of more than academic interest. Canadian businesses increasingly work across provincial and international boundaries in search of markets and opportunity. Online commerce has contributed significantly to this market expansion. Part and parcel of these developments is the exponential increase in the collection and processing of personal information.

AIQ illustrates the point. The British Columbia-based company specializes in data-related services for political campaigns, with clients in many jurisdictions. AIQ works with clients across the globe, including in BC, other parts of Canada, the US and the UK, using and disclosing personal information of citizens from those jurisdictions. The global nature of AIQ's business activities is reinforced by the fact that we are not the only privacy regulators to look into AIQ's activities in relation to the 2016 UK referendum on membership of the European Union—the Brexit referendum. The UK Information Commissioner has examined AIQ's activities related to the Brexit referendum, as have parliamentary committees in the UK and Canada.

Our report underscores that an organization must ensure that it understands, and complies with, its legal responsibilities in Canada, even when it is also operating in other jurisdictions. This is what the public expects. It is what we, as regulators, expect.

Privacy regulators are increasingly communicating and collaborating to ensure that practices affecting privacy in multiple jurisdictions are appropriately monitored and investigated.

This is the spirit in which our two Offices consider whether, consistent with Canadian laws, AIQ took measures required to ensure it had the legal authority to use and disclose UK voter information in the way it did.

We have found that, in the context of certain of its work related to the Brexit referendum, it did not.

We reach the same conclusion regarding AIQ's work in support of a United States political campaign. It is widely known, and we have found, that AIQ worked with psychographic profile information derived from Facebook data that was obtained by Cambridge Analytica and SCL Elections, via a third-party app, from millions of Americans.

Even where the information was collected in a different jurisdiction, whether that be the UK or the US, AIQ is still required to meet its obligations under Canadian law with respect to its handling of that information in Canada.

This joint investigation, the second completed this year between our Offices, is a further illustration of the collaborative reality on the privacy enforcement front – not just between our two Offices, but also among privacy regulators globally. Although privacy laws across the world are not, and never will be identical, they are generally rooted in common fair information principles that, as was relevant in this case, place great emphasis on the knowledge and consent of individuals for the collection, use or disclosure of their personal information, and on the safeguarding of that information.

Regulators will, therefore, increasingly co-operate on both a domestic and international level to ensure that individuals' privacy rights, including those relating to consent and safeguards, as we examine in this case, are respected across jurisdictions. Our two Offices are committed to doing our part in meeting that challenge.

EXECUTIVE SUMMARY

This report focuses on AggregateIQ Data Services Ltd.'s ("AIQ") compliance with the *Personal Information Protection Act* ("PIPA") and the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") in respect of its collection, use and disclosure of personal information in the provision of services to various political campaigns in the United Kingdom, the United States, and here in Canada.

It is the culmination of a joint investigation conducted by the Office of the Information and Privacy Commissioner for British Columbia and the Office of the Privacy Commissioner of Canada.

The report's findings and recommendations focus on two issues. The first is AIQ's compliance with the consent requirements in PIPA and PIPEDA relating to the collection, use and disclosure of personal information. The second is their compliance with the data security requirements set out in each of those laws.

PIPA and PIPEDA allow organizations to process personal information on behalf of other organizations based on the consent given by the individual when their information was first collected. This creates an obligation on the organizations that perform these services to exercise due diligence in terms of determining whether consent has in fact been acquired for how they use personal information.

The investigation finds that for some campaigns, AIQ was aware of the purpose for which individuals had consented to the use of their personal information and AIQ's use of that data appeared to align with those purposes. However, for most campaigns, the investigation finds that: (i) the consent relied on by AIQ did not address all of the work performed by AIQ; or (ii) AIQ was unaware of how, or whether, individuals had consented to the use of their personal information.

We examine the services AIQ provided to two campaigns in the 2016 United Kingdom European Union membership referendum ("Brexit"). The investigation finds that AIQ's use of phone numbers to send SMS messages for the BeLeave campaign is authorized by the consent provided by individuals who gave their information to that campaign. However, the same cannot be said for AIQ's work for Vote Leave.

In respect of AIQ's work for that campaign, the investigation finds the consent that AIQ relied on for its activities had not been adequate under Canadian or BC privacy law to address certain ways in which AIQ processed the personal information of Vote Leave supporters. In particular, the investigation finds that there is not adequate consent to cover AIQ's disclosure of personal information to Facebook either for the purpose of advertising to those individuals (via "custom audiences") or for the purpose of analyzing their traits and characteristics in order to locate and target others like them (via "lookalike audiences").

The investigation also examines the work AIQ performed for various US campaigns through its contractual relationship with SCL Elections. This includes work undertaken for a political action committee, a presidential primary campaign and various campaigns in the 2014 midterm elections. The investigation finds that the personal information provided to and used by AIQ comes from disparate sources. This includes psychographic profiles derived from personal information Facebook disclosed to Dr. Aleksandr Kogan, and onward to Cambridge Analytica.

In the case of their work for US campaigns that the investigation examines, AIQ did not attempt to determine whether there was consent it could rely on for its use and disclosure of personal information.

Finally, with respect to AIQ's work for Canadian campaigns, the investigation finds that AIQ is, for the most part, aware of the notice and consent obtained by its clients. However, in certain cases, the purposes for which individuals are informed, or could reasonably assume their personal information is being collected, do not extend to social media advertising and analytics.

The second issue being examined in the investigation looks at whether AIQ took reasonable security measures to protect personal information in its custody or under its control. This aspect of the investigation arose in response to a data breach AIQ reported to the OIPC. The breach involved unauthorized access to an unsecure GitLab repository holding substantial personal information as described in this report, as well as encryption keys and login credentials that put the personal information of over 35 million people at risk. The investigation determined that AIQ failed to take reasonable security measures to ensure that personal information under its control was secure from unauthorized access or disclosure.

The investigation results in a series of recommendations by our Offices. These include that AIQ take reasonable measures to ensure that any third-party consent it relies on for its collection, use or disclosure of personal information on behalf of its clients is adequate under PIPA or PIPEDA, as appropriate. These measures should include both contractual measures and other measures, such as reviewing the consent language used by the client. Where the information is sensitive, as with political opinions, AIQ should ensure there is express consent, rather than implied. In terms of security, we recommended that AIQ adopt and maintain reasonable security measures to protect personal information, and that it delete personal information that is no longer necessary for business or legal purposes.

During the investigation, AIQ took steps to remedy its security breach. AIQ has agreed to implement the Offices' recommendations.

1 BACKGROUND & METHODOLOGY

Background

1. This report examines AggregateIQ Data Services Ltd.'s ("AIQ") compliance with the *Personal Information Protection Act* ("PIPA") and the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") in respect of certain collections, uses, and disclosures of personal information on behalf of other organizations in order to provide targeted advertising, data processing, and database management services in political campaigns. Specifically, this report focuses on whether AIQ met its legal obligations relating to consent and safeguarding of personal information.
2. AIQ is a commercial organization that provides election and campaign-oriented software, website development and digital advertising services. It was incorporated in British Columbia on November 19, 2013, and is located in Victoria, British Columbia.

3. This investigation was launched in the wake of concerns raised by the media and by the United Kingdom's Information Commissioner about the collection of personal information of UK citizens by AIQ in the course of providing services to campaigns in the 2016 United Kingdom European Union membership referendum ("Brexit").
4. Subsequently, AIQ was reported to be linked to: (i) Cambridge Analytica and its parent SCL Elections Ltd ("SCL"); and (ii) the potential unauthorized receipt and use of data that had been originally obtained from Facebook. Our Offices jointly investigated Facebook's disclosure of personal information to third-party apps, including at least one such app that obtained information and subsequently disclosed that information to SCL.¹
5. Satisfied that reasonable grounds existed to investigate this matter, the Privacy Commissioners for BC and of Canada each initiated investigations pursuant to s. 36(1)(a) of PIPA and s. 11(2) of PIPEDA, respectively. In April 2018, the Office of the Information and Privacy Commissioner for British Columbia ("OIPC BC") and Office of the Privacy Commissioner of Canada ("OPC") decided to conduct these investigations jointly.

Methodology

6. The OIPC BC and the OPC sought records related to the collection, use, or disclosure by AIQ of personal information in providing services to various clients, including SCL, Brexit campaigns, and Canadian political campaigns/parties. After reviewing the produced records, investigators from both Offices interviewed the principals of AIQ under oath. Investigators also conducted a site visit at AIQ's office, where information technology analysts conducted a forensic search of devices for additional records related to the investigation and obtained copies of software applications and relevant records.
7. In addition to the evidence gathered during the site visit and through oral examinations of the principals of the organization, the investigation drew on public testimony from AIQ and others in front of the House of Commons' *Standing Committee on Access to Information, Privacy and Ethics*, as well as the UK *Digital, Cultural, Media & Sport Select Committee*.
8. The investigation and findings focus on AIQ's legal obligations under PIPA and PIPEDA. This report does not otherwise examine the practices of AIQ's clients or any other organization or individual referred to in this report, nor does it draw any conclusions about the activities or legal obligations of these other parties under PIPA or PIPEDA.

¹ Our report of findings in that investigation can be found at: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>.

2 LEGISLATION

9. PIPA and PIPEDA regulate the collection, use, and disclosure of personal information by organisations, as described below. Their rules are consistent with internationally recognized fair information practices.

2.1 PIPA and PIPEDA

10. Section 3(1) of PIPA states that it applies to every organization and defines “organization” broadly to include a person, an unincorporated association, a trade union, a trust or a “not for profit” organization.
11. PIPEDA applies to every organization in respect of personal information that the organization collects, uses, or discloses in the course of its commercial activities. Subsection 2(1) of PIPEDA defines “organization” to include an association, a partnership, a person, and a trade union.

Consent

12. Section 6 of PIPA and Principle 4.3 of Schedule 1 of PIPEDA each set out a general requirement that an organization must only collect, use, or disclose personal information about an individual where the individual has consented. PIPA and PIPEDA each contain exceptions to the general requirement to obtain consent that allow for certain instances where personal information may be collected, used, and disclosed without consent.
13. Principle 4.3 of PIPEDA states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information. Principle 4.3.2 further specifies that an organization must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. In addition, s. 6.1 requires that for consent to be valid, it must be reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.
14. Principle 4.3.4 states, in part, that the form of consent sought by the organization may vary, depending on the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information, noting that any information can be sensitive, depending on the context. Principle 4.3.5 states in part that in obtaining consent, the reasonable expectations of the individual are also relevant. Principle 4.3.6 of PIPEDA further states, in part, that an

organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

15. Under PIPA, an organization also needs to obtain meaningful consent by first ensuring that individuals are aware of how the organization plans to collect, use, or disclose personal information. Express consent is achieved when the individual receives notice and agrees to provide their information for the purpose(s) described in the notice. PIPA also allows for implied or implicit consent when an individual volunteers information for an obvious purpose and it is appropriate for the individual to volunteer that information in those circumstances. Such circumstances generally do not include situations where the organization is seeking sensitive personal information.
16. PIPA addresses a number of circumstances in which an organization may collect, use, or disclose personal information without consent. However, the Act also specifically contemplates circumstances in which an organization works on behalf of another organization. These provisions, as set out below, rely solely on the consent obtained by the original organization.
17. Section 12(2) of PIPA sets out when an organization or service provider can collect personal information from or on behalf of another organization without the consent of the individual to whom the information relates. This is allowed when the other organization obtained consent and the personal information is collected by the service provider for purposes that align to the consent and for the provision of services to the other organization.
18. Similarly, s. 15(2) of PIPA authorizes an organization to use personal information to do work on behalf of another organization for the sole purpose that the first organization received consent at the time of collection of the personal information from the individual.
19. In addition, s. 18(2) of PIPA authorizes disclosure to another organization where the individual consented to the collection of the information by the original organization and the disclosure is for the same purpose that the information was originally collected.
20. PIPEDA does not contain equivalent exceptions to consent to those in PIPA noted above, nor does PIPEDA set out any specific exceptions to consent for an organization that is doing work on another organization's behalf (e.g., as a service provider). However, in previous cases, the OPC has accepted that under PIPEDA, an organization can rely on consent obtained by another party for the organization's collection and use of personal information. In so doing, however, the OPC takes the position, and has found, that the organization must take reasonable measures to ensure that the requirement for consent has been met, ensuring that their use and disclosure of the information is carried out with the consent of the individuals implicated.

Security safeguards

21. Section 34 of PIPA requires an organization to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, or disposal or similar risks.
22. Principle 4.7 of PIPEDA requires that personal information be protected by safeguards appropriate to the sensitivity of the information. Principle 4.7.1 requires security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

3 ISSUES

23. The issues in this investigation are:
 1. What personal information did AIQ collect, use, and disclose to do work on behalf of its clients?
 2. Was AIQ compliant with consent requirements for the collection, use, or disclosure of personal information?
 3. Did AIQ take reasonable security measures to protect the personal information in its custody or control?

4 INVESTIGATION AND FINDINGS

Issue 1: What personal information did AIQ collect, use, and disclose to do work on behalf of its clients?

24. This report focuses on AIQ's collection, use, and disclosure of personal information in connection with work it performed on behalf of the following clients: (i) SCL, in respect of US political campaigns; (ii) Brexit campaigns; and (iii) various provincial or municipal political campaigns in Canada, including several in British Columbia.

4.1 SCL Elections and Cambridge Analytica

25. From 2014 to 2016, AIQ worked with SCL Elections Ltd. ("SCL") on various US political campaigns, including several 2014 midterm elections, a political action committee, and a presidential primary campaign.

26. In general, AIQ provided SCL with the following types of services: software development; data base management and processing; and digital advertising.

27. In respect of software development, AIQ stated that it was contracted to develop and deliver a campaign support tool in the form of a customer relationship management ("CRM") tool, for SCL to use in its clients' campaigns. The CRM tool, which would become known as "Ripon," would allow the user to view profiles of individuals populated with data held by SCL. Ripon was also a canvassing support tool that allowed a user to plan walking routes if undertaking a door-to-door campaign, receive talking points or questions to ask (e.g. for door-to-door or for phone calls), or update profiles from within Ripon as supporters (or those who oppose the candidate) were identified.

28. In respect of data base management and processing and digital advertising, AIQ used personal information provided to it by SCL (and, in at least one case, directly from Cambridge Analytica) to carry out the following for SCL: (i) load it into Ripon; (ii) test Ripon's functionality; (iii) provide product support to SCL; (iv) identify and segment individuals into datasets for particular campaigns; (v) deliver targeted digital advertising; and (vi) report back on advertising campaign results.

29. To populate the CRM tool, AIQ was provided with a significant amount of personal information from many different sources. This included information available to all political parties and candidates in the US, such as name and address (typically included in an electoral roll or registry) as well as information that political parties typically keep about their membership (e.g. donation history, birthdate, and email address).

30. AIQ was also provided with personal information from various data vendors, including those that focus on political customers. This data included magazine subscriptions, association memberships, inferred incomes, home ownership, vehicle ownership, and other consumer and behavioural information, including but not limited to: gun ownership, marital and parental status, religion, and ethnicity. AIQ was also provided with psychographic profiles or scores for millions of US voters, which were derived, at least in part, from Facebook users' data collected by Aleksandr Kogan². Kogan used the data to categorize voters using the "OCEAN" model of personality traits.³ AIQ stated that it never received the raw Facebook user data collected by Kogan. However, documents uncovered during our investigation demonstrate that AIQ was made aware that SCL was using data collected from Kogan. The documents also disclose that AIQ was fully aware they were using voters' OCEAN scores.
31. During the investigation, AIQ took the position that the information used was, in its experience, typical of the types of information US political parties hold about individuals, and is widely available for purchase from data vendors in the US.
32. Ripon allowed segmentation of individuals into narrow groups based on psychographic and socio-demographic information, and other characteristics. It enabled SCL to generate lists of individuals with specified characteristics and associated contact information for micro-targeted advertising campaigns.
33. In certain circumstances, AIQ also ran queries for SCL in Ripon, based on criteria supplied by SCL, to create such lists of individuals to receive targeted ads.
34. With names and email addresses provided by SCL, or those generated through queries it ran on SCL's behalf, AIQ delivered targeted ads on Facebook via: (i) the "custom audience" feature, which allows an advertiser to show an ad to individuals in the custom audience that has been matched by Facebook to Facebook users; and (ii) the "lookalike audience" feature, which allows an advertiser to target individuals who Facebook believes "look like" individuals previously targeted by the advertiser. The latter is accomplished via Facebook's use of the information it collects about its users and their friends, including those previously targeted through a custom audience.

² SCL worked with a research professor from the University of Cambridge, Dr. Aleksandr Kogan, to acquire information on 30 million American Facebook users through his survey app, called "thisisyourdigitallife," that gathered such information via Facebook. The survey took the form of a personality quiz that was added to the Facebook platform in 2013. According to public testimony by several individuals in various parliamentary hearings in Canada and the UK, Dr. Kogan used the information obtained from survey respondents and their Facebook friends to create and model psychographic profiles.

³ The model identified personality traits based on Openness, Conscientiousness, Extroversion, Agreeableness and Neuroticism.

35. AIQ also monitored and reported to SCL on the relative success of each advertisement, vis à vis the custom audience to which it was targeted, based on aggregate information provided to them by Facebook. More specifically, AIQ asserted that Facebook did not provide data to AIQ about who specifically had clicked on an advertisement; rather, Facebook provided aggregated metrics, including the number of impressions and clicks an ad received and the proportion of the custom audience that Facebook successfully had matched to Facebook users.
36. AIQ represented that it did not seek consent or assurance from SCL that consent had been obtained from the individuals whose personal information AIQ collected, used, or disclosed. AIQ stated that it did not think consent was required because its understanding was that the privacy laws in the US did not require consent and the types of information being amassed and used are widely available for purchase in the US.
37. We note that AIQ's contracts with SCL did include a general provision that "the parties ... have complied with and would continue to comply with the provisions of all applicable laws ... related to the collection, processing, disclosure and transfer of personal data."
38. Finally, we note that AIQ also contractually committed to:

Social Integration. Connect to Facebook/LinkedIn to gather information about friends/contacts of volunteers and offer messages to volunteers to post on their profiles.

AIQ claimed that it did not, in fact, carry out this activity for SCL. We found no evidence to corroborate or refute this statement.

4.2 Brexit campaigns

39. During the 2016 UK referendum on European Union membership, AIQ provided targeted advertising, website development, and database management services to various Brexit campaigns on the "leave" side—Vote Leave, BeLeave, Veterans for Britain, and the Democratic Unionist Party. Our Offices examined AIQ's activities with respect to two of those campaigns—Vote Leave and BeLeave—as the evidence suggests that personal information was not used in AIQ's delivery of services to Veterans for Britain or the Democratic Unionist Party.

Vote Leave

Targeted advertising

40. AIQ began working for Vote Leave in mid-April 2016, providing online advertising and database administration services. To facilitate the placement of advertising, *Vote Leave* originally provided AIQ with demographic descriptions of the type of individuals it

thought were likely to vote in favour of Brexit. Vote Leave subsequently provided AIQ with a list of names and email addresses for individuals who had signed up as supporters on various Vote Leave websites.

41. AIQ disclosed this list of names and email addresses to Facebook in order to target Vote Leave ads using Facebook's "custom audience" tool described above under s. 4.1.
42. AIQ also disclosed this information to Facebook to facilitate expansion of Vote Leave's advertising audience using Facebook's "lookalike audience" tool described above under s. 4.1.
43. AIQ used Facebook to test messages for Vote Leave by advertising to various custom audiences and measuring the success of those messages, as it did for SCL, as described above under s. 4.1.
44. AIQ also used Google to target advertisements at general demographic groups. In our understanding, this activity did not involve personal information.

Database administration

45. AIQ provided other services to Vote Leave as needed, primarily to organize and "cleanse"⁴ Vote Leave's database. AIQ explained that Vote Leave was having difficulty using its Voting Intention Collection System ("VICS") database, where it collected personal information about voters from UK local government councils and from door-to-door and phone canvassing. AIQ cleansed the VICS database to correct personal information and terminology that had been improperly or inconsistently entered and formatted across multiple data sources.
46. Vote Leave also used NationBuilder⁵, a voter engagement management service, to organize and use personal information. AIQ wrote an application programming interface to automatically update Vote Leave's NationBuilder database when an individual entered information on Vote Leave's website. Once in the NationBuilder database, Vote Leave campaign staff could append additional information and data points from time to time,

⁴ Data cleansing or data cleaning is the process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database. It refers to identifying incomplete, incorrect, inaccurate, or irrelevant parts of the data and then replacing, modifying, or deleting the dirty or coarse data (Wu, S. (2013), "A review on coarse warranty data and analysis," Reliability Engineering and System, 114: 1–11). Data cleansing also refers to the practice of standardizing input fields (e.g. that postal codes be written in all caps, with a space, or ensuring that "road" is always abbreviated "Rd."), and generally ensuring that disparate datasets take the same form and order of variables within the dataset. - https://en.wikipedia.org/wiki/Data_cleansing.

⁵ Nation Builder is an online service that allows campaign organizers to store and organize data, recruit volunteers, deliver mass-messaging, create canvassing plans, and conduct other data-driven campaign activities.

including whether the individual made a donation, which issues they were concerned about, and whether they would volunteer to campaign.

47. When Vote Leave collected the personal information that it provided to AIQ (i.e., names and email addresses of individuals), its privacy notice—accessible via a link at the bottom of the Vote Leave website, from which individuals could enter their information into a form—stated the following:

What information do we collect?

We may collect, store and use two kinds of data: personal and log information.

Personal data is any information you provide that enables you to partake in the campaign and includes your name, address, email address and post code. This also includes information about any donations you might make or advocacy actions you may take part in.

This includes where you might "follow", "like" or otherwise link your social media accounts to the campaign via a third-party website. Any correspondence you send electronically may be retained, such as the content of your email messages, your email address and our response. We may also retain any information you upload or post on the Vote Leave website such as profile pictures and comments.

Your personal log information relates to information about your visit to, and any actions on, this website. This includes your IP address, referrer, length of visit and number of page views. This information is required for the website to work correctly and allows us to improve the performance and functionality of the site.

Vote Leave uses the Vote Leave Android and iPhone App to allow supporters to communicate with their contacts and friends on behalf of Vote Leave. If you use the App it will run on your device and search your contacts for friends that may be interested in joining the Vote Leave campaign, the App will highlight those of your contacts you might like to phone, SMS or email as potential supporters. At no time will your contact lists be sent to Vote Leave. [updated as of 30 May 2016]

We only collect the information that we need to fulfil the purposes set out at collection. You can update this information at any time.

How will we use your data?

The information you provide may be used to:

- keep you up to date with the campaign;*
- offer you opportunities to engage with our activities;*
- respond to your queries;*
- process your application to volunteer;*
- administer supporter records;*
- conduct fundraising activities; and,*
- operate, maintain, and provide to you the features and functionality of this website.*

You may opt out from receiving such information at any time.

Your personal data may be shared within the campaign (i.e. between local, regional and national branches of the campaign), and with organisations and partners we have a strategic relationship with as part of the campaign, or that perform work for our campaign to provide services on your behalf. This is normal practice for political campaigns in the UK. In every instance these organisations and partners will only be supplied with the minimum amount of personal data they need to fulfil the services we request. They are obligated to protect your data in accordance with our policies. As part of that sharing we require our partners to never publish your personal details without your consent, and we do not pass your personal details to political parties (referendum campaign partners may include people that otherwise work in known political parties but their parties do not get access to your data).

Vote Leave uses the NationBuilder platform to organise our community of supporters and volunteers. You can read more about that company and its features and policies at nationbuilder.com, and how the NationBuilder service interacts with and protects your information at nationbuilder.com/privacy and nationbuilder.com/confidentiality.

48. During the investigation, AIQ stated that it believed Vote Leave’s privacy language to be “quite good,” and understood from Vote Leave that it was sufficient to meet the consent standards in UK law. Indeed, under oath, AIQ stated that they worked with Vote Leave’s compliance officer and lawyers to ensure appropriate consent to collect and use the personal information in the Vote Leave context.

BeLeave

49. AIQ began working for BeLeave in early June 2016, providing online advertising. BeLeave provided AIQ with general demographic characteristics of their target audience for AIQ to execute BeLeave’s internet advertising campaign. AIQ stated that BeLeave did not provide AIQ with any personal information, nor did AIQ collect or use any personal information to perform these services (digital advertising).
50. In records submitted by AIQ to our Offices, it is evident that AIQ used individuals’ phone numbers provided by the BeLeave campaign to send individuals mass text messages on BeLeave’s behalf. This constitutes a use of personal information.
51. BeLeave included a privacy statement, accessible by a link at the bottom of each page on the website, where personal information was solicited (via a form on the website, into which individuals could choose to enter their information). The privacy statement read, in part:

What information do we collect?

We may collect, store and use two kinds of data, personal and behavioural. Personal data relates to the information you provide to us in order to partake in the campaign, and includes your name, address, email address and post code.

Behavioural data relates to information about your visit to and actions on this website, and includes your IP address, referrer, length of visit and number of page views. This information is essential for the website to work correctly, and allows us to improve the performance and functionality of the site.

How will we use your data?

The information you provide will be used to keep you up to date with our campaign, in particular to offer opportunities to engage with our activities. You may opt out from receiving such information at any time.

There are times when it may be advantageous for us to make certain information available to organisations and partners we have a strategic relationship with, or that perform work for our campaign to provide services on your behalf. In every instance, these organisations and partners are obligated to protect your data in accordance with our policies.

Your personal details will never be published on this site, though we may determine that for national security, law enforcement or other issues of public importance, disclosure is necessary. Issues of public importance include, but are not limited to, the delivery of campaign petitions and signatories to any relevant Government department.

4.3 Canadian clients

52. AIQ provided a range of services to a variety of BC political clients at the municipal and provincial levels. In general, these services included website development, digital advertising delivery (including some targeted advertising using “custom audiences” and “lookalike audiences”), support or administration of clients’ CRM tools (namely, NationBuilder) and, in at least one instance, piloting a proprietary CRM tool for a client.
53. In respect of website development, the services provided by AIQ varied slightly, from developing a donation portal for one client to full web development for others. On each of these sites, which were operated by the campaigns, visitors were invited to provide personal information (such as name, email address and postal codes) and in some cases payment information (to process donations). When submitted, the information would flow directly into the campaign’s database (for example, NationBuilder).

54. From there, the campaigns could either: (i) export the database and provide it to AIQ for advertising (where AIQ was also providing advertising services); or (ii) provide AIQ with direct access to the database to organize and manage it and ultimately advertise based on the personal information collected by the campaigns. AIQ would have had access to various types and categories of personal information contained in the clients' databases. However, unlike with AIQ's work for SCL, we have not uncovered evidence to suggest that AIQ: (i) used anything other than contact information and donations history; or (ii) used that information for purposes other than sending messages (including email) or conducting digital advertising campaigns on behalf of the relevant campaign.
55. We have reviewed the campaign websites in question and the code associated with them. In each instance, the website included a privacy statement that stated, explicitly or implicitly, that the use of personal information was to keep the individuals who provided their information updated with respect to the campaign, volunteering opportunities, or events associated with the relevant candidate or campaign.
56. For the client to whom AIQ was pitching a proprietary digital CRM tool, AIQ was provided with the client's internal party membership list, which would have included personal information such as name, contact information, donation history, and other information.
57. Our investigation also found that AIQ provided services to a Canadian political client outside of BC, in respect of a mayoral election campaign in St. John's, NL. These services included the collection and use of personal information on behalf of the client and at the client's request.
58. AIQ provided website development, digital advertising, telephone interactive voice response surveys ("robo-calls"), and email mass-messaging services to the campaign.
59. Through the website AIQ developed for the campaign, the campaign gathered names, email addresses and postal codes from individuals who provided such information (via a form on the website). The campaign then provided this information to AIQ who used it to send individuals emails on behalf of the campaign. AIQ also provided demographic- and geographic-based advertising through Facebook on behalf of the campaign. AIQ represented that it did not use the email addresses to deliver ads to "custom audiences" on Facebook, and we have not uncovered any evidence that it did so.
60. Finally, AIQ represented that it also used phone numbers collected from the public telephone directory (phone book) to conduct telephone surveys, track respondents who indicated support, and report this to the campaign.
61. AIQ provided us with the content of the mayoral campaign website and the web form wherein an individual would enter the information that AIQ ultimately used to deliver emails on the campaign's behalf. The web form included the following language: "[b]y

submitting this form you agree to receive communications from [candidate's name] regarding this and future campaigns, including by email, sms, and phone unless you have indicated otherwise and to the use of your contact details in any of our current and future campaigns. You can opt out at any time."

Issue 2: Was AIQ compliant with consent requirements for the collection, use, or disclosure of personal information?

62. Our investigation revealed that AIQ used and/or disclosed individuals' personal information provided to it by its clients, in the provision of various services to its clients, namely:
- a. AIQ used names and email addresses of individuals provided by its clients and shared them with Facebook to: (i) deliver targeted advertising to those individuals through "custom audiences"; and (ii) deliver advertising to other Facebook users via "lookalike audiences";
 - b. AIQ used individuals' personal information from its clients' databases for the purposes of: (i) loading that information into software it developed for its clients' use; (ii) testing the functionality of that software; (iii) database management; and in certain cases, (iv) running queries to develop lists of individuals to receive targeted advertising; and
 - c. AIQ used individuals' names, email addresses, and telephone numbers provided by its clients to deliver emails and text messages to individuals on behalf of its clients.
63. With respect to the activities we looked at, AIQ did not have any direct relationships with the individuals whose personal information it used or disclosed. Rather, all of the personal information involved had been originally obtained by AIQ's clients or by other third parties on those clients' behalf. Our investigation did not uncover any evidence that AIQ collected, used, or disclosed the personal information at issue for any purposes other than to perform the above-noted functions on behalf of its clients.
64. Under PIPA, AIQ's authority to collect, use, and disclose personal information originally collected by another organization is limited to being for the purpose set out by the original organization at the time the information was originally collected from the individual.
65. As noted above, PIPEDA does not set out any specific exceptions to consent for an organization that collects, uses or discloses personal information on behalf of another party, for that party's purposes (for example, as a service provider or processor). Rather, PIPEDA applies to "organizations" that collect, use or disclose personal information in the course of commercial activities, more generally.

66. We are of the view that AIQ can rely on consent obtained by its client, for its uses or disclosures on behalf of that client, of personal information provided to it by the client. However, in so doing, AIQ must take reasonable measures to ensure the consent it relies on is in line with consent requirements under PIPA and PIPEDA.

67. In the present matter, we observed a range of practices with respect to consent:

1. SCL

68. Our investigation revealed that AIQ did not take any steps, other than agreeing to a broad contractual clause requiring the parties to comply with data protection laws, to ensure SCL had obtained consent from the individuals whose personal information AIQ collected (from SCL), used, or disclosed in its work for SCL. AIQ stated that it did not think it needed consent, based on its understanding that privacy laws in the US did not require consent.

69. On the above point, we highlight that AIQ remains responsible for complying with consent requirements for its personal information handling practices in accordance with applicable Canadian or BC privacy laws, even where its clients are located in another jurisdiction.

70. In the circumstances, we would have expected AIQ to have ensured that there was adequate consent for its collection, use, or disclosure of personal information on behalf of SCL. The fact that it did not do so is particularly concerning since certain information used to target individuals would have been sensitive (e.g., ethnicity or psychographic profiles), which would generally require express consent.

71. To be clear, we are not finding, in this section or below, that AIQ's foreign clients were required to comply with Canadian and BC privacy laws. The practices of those political organizations would generally fall outside the scope of PIPA and PIPEDA, and in any event, were not the subject of this investigation. That said, to the extent that AIQ wished to rely on the consent obtained by those foreign clients for its own collection, use, and disclosure of personal information on their behalf, it would need to ensure that such consent was sufficient, under Canadian or BC law as the case may be, for its purposes.

2. Vote Leave campaign

72. With respect to the Vote Leave campaign, AIQ collected email addresses and names of Vote Leave supporters from Vote Leave. That personal information was originally collected by Vote Leave, including through advertising campaigns that directed individuals to the Vote Leave website, where they could provide their personal information.

73. Vote Leave's privacy notice set out the purposes for which it received consent to collect, use, and disclose the personal information of individuals. We note that this language did

not explain that users' personal information collected via the website would be used or disclosed to Facebook for the purpose of delivering ads to individuals on Facebook and building "lookalike audiences" via Facebook. In our view, therefore, this privacy notice would not have been sufficient as a basis for AIQ to establish it had meaningful consent under PIPA and PIPEDA.

74. It is also the case that the privacy notice largely speaks to collecting and using personal information for the purpose of engaging supporters in the campaign and performing services on their behalf. The disclosure of individuals' personal information to Facebook for data analytics, via its "lookalike audience" feature, does not achieve or relate to either of those objectives. Instead, this disclosure is made to allow Facebook to link supporters to their Facebook profiles and analyze those profiles in order to identify, target, and persuade other similar or like-minded individuals. This is for Vote Leave's benefit and can certainly not be viewed, in any way, as performing a service on behalf of the voter whose information was processed.
75. We are further of the view that sharing individuals' email addresses (potentially with other contact information) with Facebook for purposes of delivering political communications to them could potentially reveal to Facebook an individual's political leanings or affiliations, which is sensitive personal information.
76. AIQ asserted that Facebook is simply another way of communicating with individuals, not materially different from email. We respectfully disagree. In our view, an individual who had initially provided their email address for purposes of being kept "up to date" or providing "opportunities to engage" with a campaign may expect to be contacted via email. They would not expect their email address to be used and disclosed to a social media company for advertising on their platform or any other unknown purposes. In other words, the use and disclosure of personal information for this purpose were neither stated in the notice nor would it have been obvious to individuals who provided their information to the campaign.
77. Accordingly, AIQ had the responsibility, under PIPA and PIPEDA, to ensure that it was relying on express consent for the work it was performing on behalf of Vote Leave. However, AIQ did not demonstrate that it sought such assurances from Vote Leave and it is otherwise clear that the privacy notice did not extend to much of the work AIQ was conducting for the Vote Leave campaign.

3. BeLeave campaign

78. The BeLeave privacy statement did not specifically mention the delivery of mass text messages using mobile phone numbers, as was carried out by AIQ for that client. The statement does, however, indicate that information individuals submitted about themselves on the BeLeave website would be used to "keep you [the individual] up to date with our campaign, in particular to offer opportunities to engage with our activities."

Given that users provided their phone numbers for purposes of the campaign engaging with them, we are of the view that they would have reasonably expected to be contacted by SMS message for this purpose.

79. Under PIPA, AIQ would have been authorized to use the personal information provided to it by BeLeave, so long as the purpose for which the information was used was the same as a purpose identified by BeLeave to the individuals in question.
80. Under PIPEDA, AIQ was required to have consent to use the personal information provided to it by BeLeave. If AIQ wished to rely on consent obtained by BeLeave for its practices on behalf of that client, it would be required to take reasonable measures to ensure such consent was meaningful and valid under PIPEDA.
81. AIQ represented to us that it was aware of the consent obtained by BeLeave via its privacy statement and was assured such consent was sufficient. We have not uncovered evidence that AIQ used personal information for purposes other than those identified in BeLeave's privacy statement.

4. Canadian political campaigns

82. AIQ provided services to several political organizations and campaigns in BC. These entities included a provincial party, certain candidates in the 2017 provincial election, a candidate for the leadership of a provincial party, and a municipal slate in the 2018 local elections.
83. AIQ submitted that its work was authorized by privacy laws and provided several reasons to support this argument. AIQ advised that they used personal information in a manner consistent with the purposes for which individuals originally provided the personal information to their clients. AIQ added that they encourage their clients to provide notice to individuals about the collection of personal information.
84. AIQ also provided our investigators with examples of campaign webpages they created for their clients that included a "consent checkbox" or button for individuals to register their support for a particular campaign. The websites also included privacy policies.
85. The webpages included fields where individuals could input their contact information, and submit that information to the campaign using the aforementioned checkboxes or buttons. The wording that accompanied the consent checkboxes or buttons included messages such as "count me in," "sign up," "join the campaign," or "stay updated." It is the case that where an individual voluntarily provides their email address or contact information to a campaign for the purpose of campaign updates or communications, AIQ could rely on their consent for the campaign to contact them via those means. However, additional explanations would be required for other uses of that same information.

86. The privacy policies addressed to some extent how personal information collected via campaign websites or other avenues would be used, but they did not address the social media advertising work performed by AIQ, and AIQ provided no evidence that individuals consented to the disclosure of their personal information for online advertising or data analytics (via “lookalike audiences”).
87. The OIPC BC’s report about political parties, which was issued in February 2019,⁶ concluded that contacting a person on a social media platform by using their email address, for example, requires that the person specifically permitted the political party to use their email for that purpose. In other words, if an individual provides their email address to a campaign, they expect to receive emails from that campaign. This same action does not qualify as consent for campaigns to use that email address to look up individuals on social media and serve them advertisements.
88. When it comes to “look-alike audiences,” the OIPC BC also indicated in its report that PIPA does not allow parties to disclose email addresses or other identifying information of supporters to a social media platform for data analysis or profiling without the express consent of the individual.
89. AIQ did not provide other evidence that the political campaigns for which it worked had garnered the necessary consent through other methods. It was AIQ’s legal responsibility to take reasonable steps to ensure the adequacy of the third-party consent on which it was relying for its use and disclosure of the personal information in question.
90. AIQ noted that they encourage their clients to have clear privacy statements on their websites and to review their privacy obligations. While this may be true, AIQ still had a legal responsibility to check that the third-party consent on which they were relying applied to the activities they subsequently performed with that data.
91. With respect to AIQ’s work for the mayoral campaign in St. John’s, NL, the OPC notes that consent would not have been required for collection, use, or disclosure of phone numbers collected from the phonebook, as such information would be considered publicly available⁷ under PIPEDA.
92. In any event, with respect to contact information obtained by the campaign via its website, we note that AIQ was aware of the language that the campaign had used to

⁶ The report, [Full Disclosure: Political parties, campaign data, and voter consent](#), is available on the OIPC BC website.

⁷ Paragraph 1 (a) of the [Regulations Specifying Publicly Available Information](#) provides that “personal information consisting of the name, address and telephone number of the subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory,” is considered publicly available for the purposes of paragraphs 7(1)(d), (2)(c.1) and (3)(h.1) of PIPEDA, such that consent is not required for the collection, use or disclosure of that information.

obtain consent from individuals who provided their information, as AIQ had built the website.

93. This language included a statement that “[b]y submitting this form you agree to receive communications from [candidate’s name] regarding this and future campaigns, including by email, sms, and phone unless you have indicated otherwise and to the use of your contact details in any of our current and future campaigns. You can opt out at any time”. This clearly addressed the types of activities AIQ performed on behalf of the campaign.

4.4 Findings and recommendations

94. **Finding:** In certain cases, such as with AIQ’s work for the mayoral campaign and the BeLeave Campaign, AIQ was aware of consent language that may have been sufficient to cover its handling of personal information on behalf of its clients. In other cases, such as with respect to AIQ’s work for SCL, the Vote Leave Campaign, and the BC campaigns, AIQ either: (i) took no measures to verify that there was appropriate consent it could rely on or (ii) relied on consent that was not sufficient to cover all of AIQ’s activities. Accordingly, we find that AIQ failed to ensure adequate consent for its collection, use, or disclosure of personal information in accordance with applicable PIPA and PIPEDA requirements.

RECOMMENDATION

AIQ should take reasonable measures to ensure that the consent on which it relies – as the basis for its collection, use, or disclosure of personal information on behalf of its clients – is compliant with PIPA and PIPEDA, as appropriate.

Those reasonable measures should include contractual measures, as well as further measures, such as reviewing consent language used by the client, to verify that the third-party consent upon which AIQ is relying would in fact meaningfully explain its intended uses and disclosures.

Where the personal information in question is sensitive and/or the collection, use, or disclosure of personal information is beyond the reasonable expectations of the individual, AIQ should ensure that the consent, for its purposes, is express. Personal information will often be sensitive when used or disclosed for political purposes, as we noted in relation to AIQ’s use of personal information in providing its services to SCL and its disclosure of information to Facebook for SCL and Vote Leave.

Issue 3: Did AIQ take reasonable security measures to protect the personal information in its custody or control?

95. AIQ used GitLab as part of its software development process. GitLab is an open-source application that allows multiple software developers to work concurrently on developing the same code. It is often used by programming teams who are developing large or complex software applications.
96. On March 20, 2018, a cybersecurity researcher in the US discovered, on GitLab, a large data repository that was owned by AIQ (the “repository”). In the repository, he discovered over 20,000 folders and 113,000 files, which he downloaded. He submitted to us that the repository he downloaded was unprotected and contained encryption keys and login credentials for client databases (the “databases”) to which AIQ had access.
97. The information in the databases included the personal information of over 35 million people, relating to a number of political campaigns around the world, such as in the UK⁸, British Columbia, and a U.S. presidential primary campaign.
98. The researcher submitted, however, that the repository itself did not contain these databases. In other words, the data downloaded from the repository could have provided the means to access the databases, stored elsewhere, as the data included some usernames, passwords, and encryption keys. The cybersecurity researcher told us that he did not take the next step to download the information held in the databases. AIQ asserted that other safeguards would have prevented such access.
99. The researcher did note, however, that some residual personal information was contained in the repository that he downloaded. These files included back-ups stored on the site, with information about eligible US voters, such as name, address, phone number, email, date of birth and, sometimes, whether or not the individual had children.
100. The compromised GitLab repository also included code for an application that could be used to target and influence people during election campaigns and for another application to scrape information from at least one social network.
101. The cybersecurity researcher explained that he was able to find the AIQ repository because an SCL employee had left open, on his own private GitHub account, a software script that pointed to the AIQ GitLab repository. The researcher then registered for a free GitLab account, which only required an email address, and was able to view and download some of AIQ’s GitLab files. AIQ alleges that the researcher also used software

⁸ With respect to approximately 1,400 UK email addresses, AIQ was unable to determine which client the personal information came from, but was able to determine that the information was related to a client for whom AIQ worked after the Brexit campaigns were complete.

tools to illegally bypass security controls that limited access to some AIQ projects, but they were unable to provide logs to substantiate this.

102. AIQ stated that a journalist advised it of the data breach. On March 26, 2018, the cybersecurity researcher published a news story about the discovery of the AIQ GitLab repository.
103. According to AIQ's sworn testimony, when AIQ was notified of this breach, it removed the ability for the general public to access this personal information. AIQ also notified the OIPC BC about this potential breach on March 25, 2018. AIQ launched an internal investigation into the breach and advised the OIPC BC that the only other unauthorized person, in addition to the cybersecurity researcher, to view this information was the aforementioned journalist.
104. During the course of our investigation, AIQ advised us that it had implemented the following security arrangements to prevent a similar incident from happening in the future:
 - Improved employee training to help employees better understand data protection and in particular personal information best practices;
 - Technical safeguards and administrative procedures to ensure that no unnecessary personal information is inadvertently backed up to the GitHub repository;
 - Regular audits to review active GitHub projects to ensure no unnecessary personal information is stored there;
 - A new policy to ensure all completed projects are audited and removed from the GitHub repository within a month of the completion of a project. If a backup is required, it is only kept in secure, non-internet accessible storage which would contain very limited personal information, such as the names and addresses of administrative users; and
 - New security measures for all of its servers, and for the Git repository (which it detailed to our Offices).
105. Section 34 of PIPA requires that organizations make reasonable security arrangements to protect personal information in their custody or control. PIPEDA sets out similar requirements to safeguard personal information. In this case, safeguard failures resulted in: (i) a breach of personal information, as outlined in paragraph 99 of this report; and (ii) increased vulnerability for the personal information, some of it sensitive, of approximately 35 million people contained in AIQ-client databases.
106. This lack of security arrangements represents a clear contravention of PIPA and PIPEDA.

4.5 Findings and recommendations

107. **Finding:** AIQ failed to take reasonable security measures to ensure that personal information under its control was secure from unauthorized access or disclosure, in contravention of s. 34 of PIPA and similar requirements in Principle 4.7 and 4.7.1 of Schedule 1 of PIPEDA to safeguard personal information. This issue is, however, resolved as, in our view, the security arrangements implemented by AIQ since the breach will satisfy the requirements of s. 34 of PIPA and Principle 4.7 of Schedule 1 of PIPEDA, and significantly reduce the likelihood of a privacy breach in future. AIQ also provided our Offices with a sworn affidavit attesting that it had deleted the personal information within its control as described in the recommendation below.

RECOMMENDATION

AIQ must put in place, and maintain, reasonable security measures to ensure that personal information in its custody or under its control is secure from unauthorized access or disclosure, as required by s. 34 of PIPA and in accordance with similar requirements under Principle 4.7 of Schedule 1 of PIPEDA.

More specifically, AIQ should attest that it has, at a minimum, fully implemented the remedial measures that it planned to implement, as outlined in Section 4 of this Report.

AIQ should delete all personal information in its custody or under its control that is no longer necessary for legal or business purposes as required by s. 35 of PIPA and in accordance with similar requirements under Principle 4.5 of Schedule 1 of PIPEDA.

5 CONCLUSION

AIQ has worked on political campaigns around the world. When taking into account all of the campaigns it has been involved in over the last several years, AIQ's work spanned four continents and involved the personal information of tens of millions of individuals. This illustrates how modern information technology can enable a small company (essentially an

SME, or “small-to-medium enterprise”) to engage in activities that have global and cascading privacy implications.

When a British Columbia-based organization, or other Canadian business, does work for clients located in other jurisdictions, it continues to be subject to Canadian privacy laws. AIQ demonstrated some awareness of privacy laws when it made contractual commitments with its clients to observe all applicable data protection laws. The company was also emphatic when it told the UK’s *Digital, Culture, Media and Sport Committee* that it had, at all times, acted legally with respect to personal privacy. However, our investigation found that AIQ often fell short of this mark, ultimately contravening both PIPA and PIPEDA.

When the company used and disclosed the personal information of Vote Leave supporters to Facebook for the purpose of analysing the characteristics of those supporters (via “lookalike audiences”) and targeting advertisements on social media (via custom audiences), it went beyond the purposes for which Vote Leave had consent to use that information.

Similarly, when AIQ collected personal information from SCL in order to inform the microtargeting of voters in the United States, it used personal information from an array of sources without any assurances that consent had been obtained. In fact, AIQ delivered targeted ads to lists of recipients that were in some circumstances determined using potentially sensitive personal information, such as ethnicity, or psychographic profiles derived from information Facebook had disclosed without the consent of its users.

In its work for Canadian campaigns, AIQ was often aware of the consent obtained by those clients, on which it relied for its purposes, but that consent did not always extend to the work it performed for those campaigns. For instance, individuals often entered their personal information into websites to show their support for candidates or campaigns. These actions would have indicated consent to receive news and information about the campaign. But they did not go so far as to allow that information to be disclosed to Facebook or other social media platforms for the purpose of targeted advertising or to conduct analytics on those individuals in order to find and target other like-minded individuals.

When AIQ failed to ensure it had meaningful consent from the individuals whose personal information it collected, used, or disclosed, it contravened BC and Canadian privacy laws.

In addition, AIQ’s inadequate safeguards resulted in unauthorized access to US voter information and left the personal information of some 35 million people, some of it sensitive, in a state of increased vulnerability on GitLab until discovered by a cybersecurity researcher. This failure to adequately protect personal information is also a contravention of Canadian privacy laws.

Our Offices made certain recommendations to AIQ, as detailed in this report, with a view to bringing AIQ into compliance with PIPA and PIPEDA. AIQ has committed to implementing those recommendations. Our Offices will, in approximately 6 months, engage with AIQ to obtain

evidence confirming that the company has in fact implemented those recommendations. We therefore conclude this matter to be **well founded and conditionally resolved**.

In general, the circumstances described in this report are not unique to AIQ. The use of microtargeting and analytics to target voters, with the assistance of third parties, has been reported elsewhere, both in BC⁹ and abroad.¹⁰ This kind of advertising is often based on repurposed and sensitive information and can involve algorithms that are opaque to individuals.

As tempting and effective as these tools might be, they must not be employed at the expense of individuals' privacy rights, which in most cases require organizations to seek meaningful consent for such activities, by adequately explaining to people how their personal information will be collected, used, or disclosed.

November 26, 2019

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

ORIGINAL SIGNED BY

Daniel Therrien
Privacy Commissioner of Canada

⁹ [OIPC BC Investigation Report P19-01](#): *Full Disclosure: Political parties, campaign data, and voter consent*.

¹⁰ Information Commissioner's Office: *Democracy Disrupted: Personal information and political influence*.