Written evidence submitted by Jeff Silvester, Chief Operating Officer, AggregatelQ

Introduction

I appreciate the opportunity to provide a thorough and detailed description of the work AggregatelQ does - as well as what we don't do - in order to provide transparency and to correct some of the inaccurate and misleading information and speculation about AggregatelQ that has been published or shared online over the last several months.

The founding of AggregatelQ

AggregatelQ was created in 2011 when one of our co-founders, Zack Massingham, was working on a local political campaign. Zack saw there were a number of improvements that campaigns could make by applying the technology and digital tools that were commonplace in other areas. He created AggregatelQ to provide IT and web services to help campaigns use technology to better organize operations. He purchased the Aggregate!Q.com domain name in April of 2011 and used AggregatelQ as a trade name for his consulting work.

Quite separately, I had been working and volunteering in politics since 2005. I had been involved with a variety of campaigns, but had recently stepped out of working in politics by the time I met Zack in 2012. By 2013, Zack and I decided to work together. We created a new website with a new logo and formally incorporated AggregatelQ Data Services Ltd. in November of 2013.

I want to emphasize that AggregatelQ was created by Zack Massingham and myself. Our company has always been and continues to be 100% Canadian-owned and operated. There have only ever been two directors of our company, Zack and myself. The company was built by us and our employees, many of whom have been with us since the beginning. Chris Wylie has never been an employee of AggregatelQ, has never done contract work for us, and has never had any role in any operations of the company.

Our early work for SCL Elections

Chris Wylie did reach out to us in his role with SCL Elections to ask for some advice on a project he was putting together. He did introduce AIQ to SCL. And AIQ did agree to build a political customer relationship management (CRM) tool for a political party in Trinidad and Tobago on contract for SCL. This contract work started in late 2013, and was completed in early 2014.

In early 2014, after the work in Trinidad and Tobago, SCL asked us to help them build an entirely new political CRM tool for use in state races during the American 2014 midterm elections. As part of the contract, SCL required that we transfer the intellectual property rights and ownership of the software that AIQ wrote for them. SCL called the tool Ripon. The work started in April of 2014 and the tool was designed to help political campaigns with typical campaign activity such as door-knocking, phone-calling and emailing. In October of the mid-term cycle we also placed online ads for SCL on behalf of their respective clients. This work concluded in November of 2014 when the midterm elections ended. We subsequently worked with SCL on similar software development, online advertising and website development during the US presidential primary from March 2015 to May 2016.

As has been reported, AIQ did help SCL with some online advertising for a campaign in Nigeria in 2015. It was during this campaign that a very graphic and disturbing video surfaced. We saw the video, and we were asked to promote the video with online advertising, but we refused. We do not know who produced the video. After this frankly disturbing incident, we began adding language to our standard contracts to address ethics in advertising.

As with all of our work, at the conclusion of each of our contracts with SCL, we destroyed any information in our possession from those campaigns.

Until 2015, SCL was certainly our largest client, but not our only client and we were always completely independent and had no cross ownership, nor any cross board membership. In fact, the last contact we had with SCL was shortly after the conclusion of our work on the US presidential primaries in May of 2016. It consisted only of a request from SCL to us to transfer the code for the political CRM that they had paid for, and from us to them to get our final invoice paid. We have not done any work for them or any of their group of companies, nor have we communicated with them since.

False allegations of connections to Cambridge Analytica

As described above, we did software development and online advertising work for SCL on contract. Aside from having done that work for them, we have no corporate ties, legal or otherwise, to SCL or any individuals associated with them. We have never worked for, contracted with, nor have any corporate ties, legal or otherwise to Cambridge Analytica or any individuals associated with them. We understand there has been some confusion around this point in SCL internal email messages shared with the UK Parliament. The reality is we have always been a completely separate legal entity and suggestion of any other relationship, whether misconstrued internally or externally, is untrue.

In 2017, we were alerted by a journalist that SCL had published Zack Massingham's phone number on its website under the heading "SCL Canada." We had no knowledge of this listing prior to the call from the journalist. We have never been contacted by anyone thinking we were SCL Canada and we never referred any work or clients to SCL. SCL did ask us in early 2014 to establish "SCL Canada" on its behalf. We declined. It appears that SCL likely adopted that term internally without our knowledge or consent. When contacted by that same journalist for comment, SCL removed the number and acknowledged it did not accurately describe our relationship.

We did become aware in 2014 of a company called Cambridge Analytica (CA) and that it had some kind of business relationship with SCL. We understood that CA was an American firm based in New York, and that SCL was a UK firm based in London. We were not aware of the details of their particular business relationship. We knew CA worked on the US primary campaign concurrently with SCL. However, we only worked as a contractor to SCL, our instructions came from SCL, and we were paid by SCL.

I would like to take this opportunity to address a document provided to the UK Parliament as "evidence" that we had a contractual relationship with CA. The document resembles a contract we signed with SCL. However, we had never seen the document prior to news reports about it. We have no knowledge of, and can say nothing about, whether that document with the joint SCL/CA letterhead is genuine or otherwise. It has nothing to do with AIQ, we never had any such relationship as might be implied by that document, and we note that it is unsigned. As mentioned above, we have never signed any contract with CA.

Voter Information and the "Kogan data"

While supporting SCL's Ripon political CRM in 2014, we became aware that SCL had and was developing models for predicting voter personality with the help of a Dr. Kogan from Cambridge University. However, we were never involved in nor exposed to any data modeling or data analytics. We have never met nor had any interaction with Dr. Kogan. Nor have we ever seen or had access to the Facebook data Dr. Kogan is said to have used. We have never managed, had access to, nor used any Facebook data allegedly improperly obtained by CA or by anyone else. In fact, recently, while speaking to your committee on Fake News, the Chief Technology Officer of Facebook confirmed that AggregatelQ did not use any improperly obtained Facebook data during the UK Referendum.

The only personal information we use in our work is that which is provided to us by our clients for specific purposes. In doing so, we believe we comply with all applicable privacy laws in each jurisdiction where we work.

The UK Referendum

In April of 2016, after an acquaintance who was consulting with Vote Leave at the time let us know that Vote Leave was looking for a contractor to provide digital advertising services, we submitted a poposal to the Vote Leave campaign. On April 12th, we were informed that we were the preferred choice of the campaign. On April 13th, the Vote Leave campaign was given the designation as the official "Leave" campaign in the referendum.

During the campaign, in addition to the online advertising, we provided limited website, software development, and IT support. Our work with Vote Leave continued through to the vote on June 23, 2016. The only information we used in our work for Vote Leave was the information that was provided to us by Vote Leave.

Near the end of the referendum, we also provided online advertising services to BeLeave, Veterans for Britain, and the DUP. In each case the work we did was directed by each of our clients independently.

In the course of our work for BeLeave we submitted a variety of invoices and digital advertising insertion orders (similar to a purchase order but for advertising services). We were informed by Darren Grimes of BeLeave that Vote Leave would be providing a donation to BeLeave, and that BeLeave asked that the donation be sent directly to us to pay for our services and advertising costs.

As part of our due diligence we conducted research into the appropriateness of the payment method. The people responsible for compliance at Vote Leave assured us that such a donation was allowed. They also told us the Electoral Commission had written to them to confirm the legality of a similar situation Vote Leave had already been in. Indeed, after the vote, in March of 2017, the Electoral Commission reviewed the donation and found that no further investigation was required and the UK High Court has recently confirmed, again (hearing of March 15, 2018), that a donation, whether of cash or kind, was entirely allowed under Electoral Law in the UK.

We have never thought that the work we did for any of our clients during the referendum was anything but above board - legally and ethically. We have no reason to believe that there was any content shared between the campaigns we worked for, nor did we see any evidence of coordination. As a small organization it was necessary for our CEO to know some details of more than one campaign. In terms

of the generic expertise we were hired to provide, creating and placing online ads through platforms like Facebook and Google, we gave that expertise equally and fully to all our clients. Nonetheless, campaigns were kept entirely separate from each other and we did not share plans or information of any client with any other client.

Ongoing privacy investigations

AggregatelQ works in full compliance within all legal and regulatory requirements in all jurisdictions where it operates. We have been cooperating fully with the joint investigation by the Canadian and BC Privacy Commissioners and are looking forward to any recommendations they might have on how we can improve our practices.

We also strongly believe that we have been cooperating with the UK Information Commissioner's Office and its investigation into the use of data analytics in political campaigns. So it came as a surprise to us when a member of the Canadian Parliament's Standing Committee on Information, Privacy and Ethics received an SMS text from the Chair of this committee while we were testifying in real-time to the Canadian committee suggesting that we weren't being cooperative.

We are on the record - and will state again here - that the UK ICO sent us a letter on May 17, 2017, to which we replied promptly. We heard nothing from the UK ICO until we received a letter from them some eight months later on January 30, 2018, to which we also replied promptly. Our impression was that by responding to the UK ICO's letters promptly and as thoroughly as we could, we were cooperating with its investigation. We did not receive any indication in the two letters from the UK ICO that they believed we were not cooperating and the Commissioner's recent statement that we refused to answer any further questions is simply not true.

Nevertheless, we did follow up with the UK ICO after our hearing in front of the Canadian Parliamentary committee. Having now received a letter in response from the UK ICO, a subsequent letter with additional questions from the UK ICO, and a variety of positive email communication back and forth with high ranking officials in the UK ICO, we believe we have resolved this apparent miscommunication and we look forward to continuing to cooperate with the UK ICO's investigation.

How we protect personal information

The only personal information we use in our work is that which is provided to us by our clients for specific purposes. This might include lists of emails or voter contact information for use in political CRM software used by campaigns. We also might receive a list of names and email addresses to include in advertising campaigns to assist in showing ads to groups of Facebook users who are supporters of a campaign.

In all of the cases where we receive or have access to information for a campaign, we only use this information for the purposes it was provided. We always encourage our clients to inform potential visitors to their websites in clear and understandable language how any of the information they provide might be used and how that information can be removed later if desired.

Any personal information that is provided to AggregatelQ is kept on secure servers with security protocols that meet or exceed industry standards. Where possible, personal information is tokenized or anonymized and the original information deleted. This information is never shared between any of our

clients.

At the end of our engagement with a client or at any time before that when any information is no longer required, we return the information to our client and destroy it from our systems.

The unauthorized access to our code repository

We acknowledge that, while we always endeavour to observe and exceed industry privacy standards, we don't always get everything right.

On Sunday, March 25th, we were alerted by a journalist to unauthorized access to an Aggregate IQ code repository. We took immediate steps to secure that server as well as all of our servers and services to ensure no further access was possible.

During the process of securing the server and investigating how the unauthorized access had occurred, we discovered that some personal information from voters was inadvertently left in one of the code backups. Within a few hours of the initial report by the media, in addition to notifying our clients, we contacted the Acting Deputy Commissioner from the Office of the Information and Privacy Commissioner of British Columbia and we launched a full and thorough investigation. That investigation is still ongoing.

What I can say at this time is that the information accessed by the security researcher is primarily software code, but also included contact information for supporters and voters from a few of our past clients. None of these files contained any individual financial, password or other sensitive information, and none of the personal information came from the Brexit campaign. That there was any personal information in our code repository at all was a mistake on our part. For that we apologize. We have already put in place measures to prevent that from happening again, and as we complete our investigation we anticipate there may be additional recommendations and improvements that can be made. The Federal and Provincial Privacy Commissioners may also have recommendations. We welcome and will act upon them. We are committed to ensuring that this investigation is done thoroughly and done right.

Working with Facebook

We have always operated within the Facebook terms of service and we have never managed, had access to, nor even seen the Facebook data allegedly improperly obtained by Cambridge Analytica or Mr. Kogen.

We understand that Facebook reported to this committee that they found some apparent administrative links between AIQ and CA on the Facebook platform. We don't know what they are referring to, and they have not provided this information to us. We have reached out to Facebook and have been told that they were instructed by the UK ICO not to communicate substantively with us while their investigation is ongoing. We have written to the UK ICO to demand that they rescind this order. Nevertheless, we are looking forward to discussing this matter fully and resolving this issue with Facebook so we can continue to be a good customer of theirs.

When we create an advertising campaign for a client we use the services available on advertising platforms like Facebook and Google. Facebook provides a platform that allows an advertiser to show ads

to its users based on criteria such as demographic information like age range or sex, geographic information like cities or states, and interests that people may have identified on Facebook. All of this allows a campaign to run a very complex and comprehensive advertising campaign without the need for any external information. Typically a campaign will provide us with a general description of the sort of voters they believe will support them. An example might be conservative voters outside of cities, older than 39 years of age. We would place this information into the Facebook platform along with the ads that we create at the direction of the client. Each ad consists of a picture, often with a few words on it, along with some descriptive text and a link to a webpage should someone click on the ad. We also sometimes assist in creating that web or "landing" page. We then work with the client to decide how many times people should see these ads and over what time period. The Facebook platform takes care of the rest, showing these ads to its users and providing reports on how many times the ads have been shown and how many times the ads have been clicked. None of that information includes any personal information. Facebook also gives advertisers the ability to count the number of people who might land on a certain webpage on the client site using a piece of code called a pixel. We often help our clients place this Facebook pixel code on their site so that the client can measure if a particular ad is reaching its goal to show people a video, versus signing up to be on a mailing list for example.

None of this requires any external data. Facebook's advertising platform has everything you need to create a national campaign without needing to see any personal information. Facebook already has information on the vast majority of Canadian, American, and UK Citizens that it keeps securely within its system. It does not share any of this information with advertisers. When you place ads on the Facebook platform, Facebook uses its own algorithms and techniques to show the ads to individuals. You don't need your own data to do this - and even if you had your own data, it is likely not going to be as effective as just using Facebook. Allegations that AIQ or anyone would benefit from using information allegedly improperly obtained from Facebook in 2013 predominantly or wholly from US citizens to target UK citizens in a UK referendum in 2016 makes no sense. Again, the Facebook advertising platform provides all the necessary information and tools based on current and relevant Facebook information, and the speed of execution means advertising decisions can be put into effect within minutes.

Conclusion

As I stated at the outset, much of what has been said about AggregatelQ by those who neither know nor represent us, has been largely inaccurate. With all due respect to this committee, "fake news" cuts both ways, and can sometimes come from unexpected, and normally reliable sources. In fact, the media outlet leading the charge against us - The Guardian - has had to publish corrections about our involvement in this issue:

"[W]e did not intend to suggest that Aggregate IQ is a direct part and/or the Canadian branch of Cambridge Analytica, or that it has been involved in the exploitation of Facebook data, or otherwise been involved in any of the alleged wrongdoing made against Cambridge Analytica. Further, we did not intend to suggest that AIQ secretly and unethically co-ordinated with Cambridge Analytica on the EU referendum."

Unfortunately, corrections on page 50 of a newspaper do not get as much attention as a headline on the front page.

In closing, we have at all times acted ethically, legally and with full respect to personal privacy. We have attempted to provide clear and accurate information to regulators, to the media, to elected officials, our

clients and the public. We will continue to do so. We thank you for taking the time to hear us, and we look forward to addressing any further questions you may have.

May 2018