May 2nd, 2018
Parliament of Canada
House of Commons
Standing Committee on Access to Information, Privacy and Ethics
MP Bob Zimmer, Chair
MP Charlie Angus, Vice Chair
MP Nathaniel Erskine-Smith, Vice Chair

Dear Messrs. Zimmer, Angus, and Erskine-Smith,

We at UpGuard are reaching out to you, honorable chair and vice chairs of the Standing Committee on Access to Information, Privacy, and Ethics, regarding an important matter of privacy and data integrity affecting not just Canadian citizens, but individuals around the world. The issue of preserving any and all relevant data stored by companies AggregateIQ, Cambridge Analytica, and SCL on the systems of external services, including but not limited to Github, and Amazon Web Services, is a matter of great urgency and public significance.

Chris Vickery, UpGuard's Director of Cyber Risk Research, previously testified before the Committee on April 17th, 2018, regarding our Cyber Risk Team's discovery of a data exposure from within the systems of AggregateIQ. AggregateIQ (AIQ) is a data analytics firm based in British Columbia which has been investigated by regulators and public officials around the world for its ties to Cambridge Analytica and its parent company SCL. These companies have been probed in North America and Europe regarding their work in a number of prominent political campaigns, including the UK "Brexit" referendum vote and the 2016 US presidential election, as well as regarding Cambridge Analytica's improper acquisition of the personal data associated with as many as 87 million Facebook user accounts.

Earlier this year, UpGuard researchers discovered and analyzed a public-facing source code repository hosted on an AggregateIQ server, containing code designed for clients around the world, including a number known to have patronized Cambridge Analytica. The UpGuard Cyber Risk Team has since published four reports detailing the contents, relating their significance and shedding further light on issues of international importance. The news today that Cambridge Analytica and SCL are being dissolved raises a serious concern: is there more data out there, hosted using services such as AWS, that is relevant to inquiries in the US, UK, and Canada into all three companies?

We write to you in the hopes that public servants might immediately put forward data preservation requests to GitHub, Amazon Web Services, Facebook, and other relevant data services, to freeze and preserve the data in any accounts used by AggregateIQ, Cambridge Analytica, and SCL. As stated by UK MP Damian Collins, "Cambridge Analytica and SCL group cannot be allowed to delete their data history by closing. The investigations into their work are vital."

We hope these data preservation requests would be made public, as ultimately the directors for all of these companies should be held accountable. We fear that if the proverbial paper trail is wiped, important information could be lost of interest to the relevant international inquiries.

In this spirit, we offer a few questions of relevance to the ongoing investigations in both Canada and the United Kingdom:

1. Have regulators and/or Members of Parliament issued data preservation requests to Cambridge Analytica, SCL, and/or AggregateIQ?
2. Have regulators and/or Members of Parliament issued data preservation requests to any third-party vendors used by Cambridge Analytica, SCL, and/or AggregateIQ?
3. Have officials discovered any further use by Cambridge Analytica, SCL, and/or AggregateIQ of third-party service providers, such as Amazon Web Services, where as-yet unexamined information related to these inquiries may reside?
4. Are regulators able and willing to issue data preservation requests to any and all external vendors that may possess or service Cambridge Analytica, AggregateIQ, and/or SCL?

As we have seen with the AggregateIQ exposure discovered by our team, which contained information of critical importance to the public, as well as unobscured access credentials for other systems, any such data that may be stored using other services may be of great significance to your ongoing inquiries. The risk is that one cluster of companies have the keys to all of this data, yet turns a blind eye to all of the egregious uses of their platform without governance nor controls in place for transparency or oversight into their operations. It would compound the potential issues under investigation were this data to now disappear with the dissolution of Cambridge Analytica and SCL.

A wide range of services used by Cambridge Analytica, AIQ, and associated entities rely on Amazon's services and storage in some shape or fashion. We believe this is perhaps the most important service to discuss these issues with; the exposure discovered by UpGuard reveals AIQ used Amazon Web Services. Whatever data of this sort which Amazon could preserve would be beneficial to your inquiries.

We would be eager to discuss this matter further with you and any other Canadian or international officials, and hope we can assist in ensuring this data is preserved.

Sincerely,
Mike Baukes, Co-CEO
Greg Pollock, Vice President of Product, BreachSight
Jon Hendren, Director of Strategy
UpGuard, Inc
909 San Rafael Avenue
Mountain View, California 94043