Information Commissioner's Office

Investigation into the use of data analytics in political campaigns

Investigation update

ico.
Information Commissioner's Office

Contents

Executive summary

The Information Commissioner announced in May 2017 that she was launching a formal investigation into the use of data analytics for political purposes after allegations were made about the 'invisible processing' of people's personal data and the micro targeting of political adverts during the EU Referendum.

The inquiry eventually broadened and has become the largest investigation of its type by any Data Protection Authority involving social media online platforms, data brokers, analytics firms, academic institutions, political parties and campaign groups.

A key strand of our investigation surrounds the link between Cambridge Analytica, its parent company SCL Elections Limited and Aggregate IQ and involves allegations that data, obtained from Facebook, may have been misused by both sides in the UK referendum on membership of the EU and used to target voters during the 2016 American Presidential election process.

The investigation is live and remains ongoing but the Information Commissioner needed to meet her commitment to provide Parliament's Digital Culture Media and Sport Select Committee with a progress update on the investigation for the purposes of informing their work on "Fake News" before the summer recess.

A separate report, "Democracy Disrupted? Personal Information and Political Influence" has also been published covering the policy recommendations from the investigation.

This is a summary of the regulatory action taken so far:

Cambridge Analytica and SCL Elections Limited

- The ICO issued an Enforcement Notice to SCL Elections Limited requiring them to deal properly with Professor Carroll's Subject Access Request.
- The ICO is now taking steps with a view to bringing a criminal prosecution against SCL Elections Limited for failing to properly deal with the Enforcement Notice.

Facebook

- The ICO has issued Facebook with a Notice of Intent to issue a monetary penalty in the sum £500,000 for lack of transparency and security issues relating to the harvesting of data constituting

breaches of the first and seventh data protection principles under the Data Protection Act 1998.

We have served Facebook with a Notice of Intent setting out our areas of concern in detail and inviting their representations on these. Their representations are due later this month and we have taken no final view on the merits of the case at this time. We will consider carefully any representations Facebook may wish to make before finalising our views. Our findings and final decision on any regulatory action that may be necessary will then be made public. Our policy on Communicating Regulatory Actions makes clear that while we would not normally publish a Notice of Intent, we may do so where there is an overriding public interest. In this case we consider that the overriding public interest and the commitment to update the DCMS committee so it can progress its work mean that we decided in favour of publishing the Notice.

Cambridge University

- The ICO will conduct an audit of Cambridge University Psychometric Centre.
- The ICO also recommends that Universities UK work with all universities to consider the risks arising from use of personal data by academics in a university research capacity and where they work with their own private companies or other third parties. Universities UK has committed to this work.

As part of our investigation we are considering whether Cambridge University has sufficient systems and processes in place to ensure that data collected by academics for research is appropriately safeguarded in its use and not re-used for commercial work. Examination of equipment from the University is ongoing, and will help in this regard.

Political parties

- The ICO has sent 11 warning letters requiring action by the main political parties backed by Assessment Notices for audits later this year.

We have concluded that there are risks in relation to the processing of personal data by many political parties. Particular concerns include: the purchasing of marketing lists and lifestyle information from data brokers without sufficient due diligence, a lack of fair processing, and use of third party data analytics companies with insufficient checks around consent.

Data brokers

- The ICO has issued a Notice of Intent for regulatory action against data broker Emma's Diary (Lifecycle Marketing (Mother and Baby) Limited)
- The ICO will be conducting audits of the main credit reference companies

We have looked closely at the role of those who buy and sell personal data-sets in the UK. Our existing investigation of the privacy issues raised by their work has been expanded to include their activities in political processes.

Leave.EU and Eldon Insurance

We are investigating allegations that Eldon Insurance Services Limited shared customer data obtained for insurance purposes with Leave.EU and that the data was then used for political campaign purposes during the EU Referendum, contrary to the first and second data protection principles under the Data Protection Act 1998 (DPA98). We are also investigating whether Eldon Insurance Limited's call centre staff used customer databases to make calls on behalf of Leave.EU in contravention of the Privacy and Electronic Communication Regulations 2003.

In addition, we are investigating allegations that insurance customer data was sent to the USA and in particular to the University of Mississippi, and whether that was a contravention of the eighth data protection principle under the DPA98. We are in contact with the University and this line of enquiry is ongoing.

Relationship between AggregateIQ (AIQ), Vote Leave and other leave campaigns

- The ICO has issued an Enforcement Notice to AIQ to stop processing retained UK citizen data.

We have established that AIQ had access to personal data of UK voters provided by the Vote Leave campaign. We are currently working to establish from where they accessed that personal data, and whether they still hold personal data made available to them by Vote Leave. We have however established, following a separate report, that they hold UK data which they should not continue hold. We are engaging with our regulatory colleagues in Canada, including the federal Office of the Privacy Commissioner and the Office of the Information and Privacy Commissioner, British Columbia to assist in this work.

Vote Leave

We are investigating whether and to what extent Vote Leave transferred the personal data of UK citizens outside the UK and whether this was in

breach of DPA98, as well as whether that personal data has also been unfairly and unlawfully processed. We expect to take decisions on potential formal enforcement action within the next three months.

Remain campaign

We are investigating the collection and sharing of personal data by the official Remain campaign, the In Campaign Limited, trading as Britain Stronger in Europe (BSiE), and a linked data broker. We are specifically looking at inadequate third party consents and the fair processing statements used to collect personal data. These are similar issues to those we have explored in the rest of our investigation. Again, we expect to be in a position to take decisions on potential formal enforcement action within the next three months.

The report is an interim progress update, summarising the areas we are investigating and our actions to date. The full detail of our findings will be set out in any final regulatory notices we issue to the parties being investigated.

We anticipate that we will have concluded the current phase of our investigative work by the end of October 2018.

1. Introduction

In early 2017, there was a number of media reports in *The Observer* newspaper that claimed that Cambridge Analytica (CA) worked for the Leave.EU campaign during the EU referendum, providing data services that supported micro-targeting of voters. In March 2017, the Information Commissioner announced that her office (ICO) would begin a review of evidence as to the potential risks arising from the use of data analytics in the political process.

Following that review of the available evidence, the Information Commissioner announced in May 2017 that she was launching a broader formal investigation into the use of data analytics in political campaigns, and in particular whether there had been any misuse of personal data and therefore breaches of data protection law by the campaigns, on both sides, during the referendum. At the same time, the Information Commissioner committed to producing a policy report; that has been published alongside this update.[1]

The subsequent investigation identified a number of additional strands of enquiry that required consideration. Three other ongoing ICO operations in sectors such the credit reference agencies and data brokers also revealed evidence of relevance to this inquiry. The inquiry eventually broadened and involved various social media online platforms, data brokers, analytics firms, academic institutions, political parties and campaign groups. The nature of modern campaigning techniques and data flows means that some of these organisations of interest to the investigation are located outside the UK.

[1] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/blog-the-information-commissioner-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/

The investigation is significant and wide ranging. It is exceptional in that many of the key players have been offering their evidence publicly in various parliamentary and press forums around the world, and at different times. Our investigation has had to react to, and address, that. It has also had to respond to further offers of information from former staff of the organisations under investigation, and this has caused us to re-review and rethink elements of the evidence previously presented by those organisations.

It the largest investigation of its type by a data protection authority, involving at times over 40 ICO investigators working full-time on it. A significant number of external experts have been contracted to provide legal and forensic IT recovery support to various aspects of the investigation at various times. The investigation has identified a total of 172 organisations of interest that required engagement, of which around 30 organisations have formed the main focus of our enquiries, including political parties, data analytics companies and major social media platforms. Details of the organisations involved are set out at Annexe i.

Similarly, we have identified a total of 285 individuals relating to our investigation. We have spoken with around 100 individuals including through formal interviews and continue to engage with people who hold information of relevance to the investigation. The Commissioner has used the full range of her powers, including formal notices to require information to be provided under the Data Protection Act 1998 and Regulation of Investigatory Powers Act 2000, her powers of entry under warrant, and her audit and inspection powers. We are looking at both regulatory and criminal breaches. We are working with other regulators, EU data protection authorities and law enforcement agencies in the UK and abroad.

A key strand of our investigation is the link between CA, its parent company SCL Elections Ltd, Aggregate IQ and allegations that data that may have been misused by both sides in the UK referendum on membership of the EU, and obtained from Facebook and used to target voters during the 2016 American Presidential election.

In February 2018, our focus on Facebook and CA were heightened by evidence provided to the ICO by Mr Christopher Wylie, a former employee at CA, who provided us with evidence that an app developed by Cambridge University academics, including Dr Aleksandr Kogan, had been used to harvest the data of 50 million (now estimated as 87 million by Facebook) global Facebook users, including 1 million Facebook users in the UK.

In addition to the potential links between CA and Leave.EU, which initiated our investigation, we found a number of lines of enquiry, including their relationship with a Canadian firm, Aggregate IQ and its work with Vote Leave, BeLeave, Veterans for Britain and the Democratic and Unionist Party's Vote to Leave campaign. We have identified information during our investigation that confirmed a relationship between Aggregate IQ (AIQ) and CA / SCL. To the extent this relationship involved the acquisition and use of personal data, we have also considered their interactions during our investigation.

Our investigation also considered the use of personal data by the Remain campaign group, Britain Stronger in Europe, in particular their use of services provided by the Messina Group, amongst others.

The ICO's work needs to meet the applicable standards of evidence gathering and recovery if it is to be useful. The investigation has recovered materials, including dozens of servers and other equipment

containing in total hundreds of terabytes of data. These investigations are by their nature very complex and take time to complete.

The investigation remains ongoing but the Information Commissioner wanted to meet her commitment to provide Parliament's Department of Digital Culture Media and Sport (DCMS) Select Committee with a progress update on the investigation for the purposes of informing their work on fake news before the summer recess. Additionally, a number of overseas regulators and agencies have requested updates in order to advance their own regulatory actions and a number of strands of the enquiry are now complete and moving into public stages. Given this, and the high public interest issues raised by this work, this report has been put together to consistently inform all parties as to our progress at this time.

2. The investigation

Following a risk review, the formal broader investigation launched in May 2017 began as one into the use of data analytics for political purposes. An initial fact finding phase carried out during the second half of 2017 was both complex and wide ranging. This involved meetings, interviews and correspondence with over 30 organisations – including political parties, political campaign groups, social media platforms and data broker organisations. Among these organisations were Facebook, Cambridge Analytica and AggregateIQ (AIQ).

The aim of this phase was to understand how political campaigns use personal data to micro-target voters with political adverts and messages, the techniques used, and the complex eco-system that exists between data brokerage organisations, social media platforms and political campaigns and parties. This phase of our investigation was also used to identify potential breaches of the Data Protection Act (DPA) 1998 in force

at the time and the Privacy and Electronic Communications (PECR) Regulations 2003 for further investigation.

Key areas explored and analysed through the investigation included:

- The nature of the relationship between social media platforms, political parties and campaigns and data brokers in respect of the use of personal data for political purposes;

- The legal basis that political parties and campaigns, social media platforms and data brokers are using to process personal data for political purposes;

- The extent to which profiling of individuals is used to target messages/political adverts at voters;

- The type and sources of the data sets being used in the profiling and analysis of voters for political purposes;

- The technology being used to support the profiling and analysis of voters for political purposes;

- How political parties and campaigns, social media platforms and data brokers are informing individuals about how their information is being used; and

- Voters' understanding of how their personal data is being used to target them with political messaging and adverts.

A number of organisations freely co-operated with our investigation, answered our questions and engaged with the investigation. However, others failed to provide comprehensive answers to our questions,

attempted to undermine the investigation, or refused to cooperate altogether. In these situations we used our statutory powers to make formal demands for information.

Of the 30 organisations originally of interest to our investigation, eight have now been advised that we have no further enquiries for them at this stage.

The Information Commissioner has a number of powers available to her to carry out her work:

- Information Notices to request provision of information from organisations in a structured way (with changes to legislation these can now be issued to individuals as well as data controllers);

- Enforcement Notices to require specific action to be taken by a data controller to comply with the Data Protection legislation;

- A Demand for Access to allow the Commissioner to attend at premises to carry out investigations and examine material relevant to her investigation (backed by a warrant to do the same if access is unreasonably refused); and

- Monetary Penalty Notices to fine data controllers for breaches of the data protection legislation

To date, 23 Information Notices have been issued to 17 different organisations and individuals. These include Facebook, CA, Vote Leave, Leave.EU, a group of insurance companies related to Leave.EU and directors of those companies, and UKIP.

UKIP appealed to the Information Tribunal against the Information Notice issued by the Commissioner. The tribunal has dismissed the appeal, accepting that UKIP's response to the IN (which was found to accord with legislation) was brief, inadequate and in some instances possibly inaccurate, and UKIP's apparent willingness to cooperate in the Commissioner's enquiries rendering an IN unnecessary was insufficient grounds for allowing the appeal. UKIP should now respond to our Information Notice. In addition, we have executed warrants against premises and issued Enforcement Notices: one against SCL Elections Ltd for failure to comply with a Subject Access Request and one to AiQ to delete any UK data held on its systems.

As the investigation has broadened in scope and scale, we have increased resources and adopted a major incident room type approach to our work to retain order in our investigation and the security of our evidence recovery.

Our investigation also has a considerable international and inter-agency dimension. Several disclosures to us have suggested offences beyond the scope of the ICO, and we have made appropriate referrals to law enforcement in the UK and overseas. Several of the key subjects of our investigation are also subject to investigation by other data protection authorities and we are in contact with our counterparts in Canada and the United States (US) to co-ordinate elements of our investigation. Through our links to the Global Privacy Enforcement Network (GPEN), we have legal gateways to share and receive information that assists with our investigation and that of other data protection authorities.

3. Regulatory enforcement action and criminal offences

The investigation is considering both regulatory as well as criminal issues.

The main issues being examined are summarised as:

3.1 Failure to properly comply with the Data Protection Principles; anyone who processes personal data must comply with eight principles of the Data Protection Act, which make sure that personal information is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in line with your rights;
- secure; and
- not transferred to other countries without adequate protection.

3.2 Failure to properly comply with the Privacy and Electronic Communications Regulations (PECR); these regulations sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications. There are specific rules on: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy as regards traffic and location data, itemised billing, line identification and directory listings.

3.3 Section 55 offences under the Data Protection Act 1998; this states that it is a criminal offence to knowingly or recklessly without the consent of the data controller obtain, disclose or procure the disclosure of information in personal data. It is also an offence for someone to sell data if it has been obtained in those circumstances.

We are also examining the evidence we have recovered to identify where other criminal offences may have been committed; this includes criminal offences related to the failure to comply with Information Notices or Enforcement Notices issued by ICO as well as other offences for perverting the course of justice. In most cases, these carry significant financial sanction up to and including unlimited fines and terms of imprisonment for individuals.

We are looking at both organisations and the actions of individuals controlling them (including directors) during the relevant periods.

4. Interim update

This is an interim progress update, summarising the areas we are investigating and our actions to date. The full detail of our findings will be set out in any final regulatory notices we issue to the parties subject to investigation.

4.1 Political parties

Our investigation team met with the main political parties in the UK and wrote to all the major parties involved in UK political processes. Parties were asked to provide information about how they use personal data, how they obtain personal data, and the steps they take to comply with data protection legislation, including the guidance issued by the ICO.

We have concluded that there are risks in relation to the processing of personal data by many political parties. We have issued letters to the parties with formal warnings about their practices. Of particular concern are:

- The purchasing of marketing lists and lifestyle information from data brokers without sufficient due diligence around those brokers and the degree to which the data has been properly gathered and consented to;

- A lack of fair processing information;

- Use of third-party data analytics companies with insufficient checks those companies have obtained correct consents for use of data for that purpose;

- Practice to assume ethnicity and/or age and combine this with electoral data sets held, raising concerns about data accuracy;

- Provision of contact lists of members to social media companies without appropriate fair processing information in place and collation of social media with membership lists without adequate privacy assessments.

In writing to highlight our concerns and recommend actions the parties should take, including Data Protection Impact Assessments, we have indicated that we will allow them a period to address our findings before we follow up later this year with them individually through our audit process to assess their compliance with the new DPA 2018 requirements.

4.2 Social media platforms

We made enquiries to all the main social media platforms operating in the UK and involved in UK political processes. We engaged with social media platforms, such as Google, Snapchat and Twitter. For example, Twitter explained its approach to advertising, how the platform used data,

including personal data, location services, and target or 'Lookalike' audiences to direct advertising.

Twitter stated that it had not, and does not, have access to any psychometric data hosted by Cambridge University.

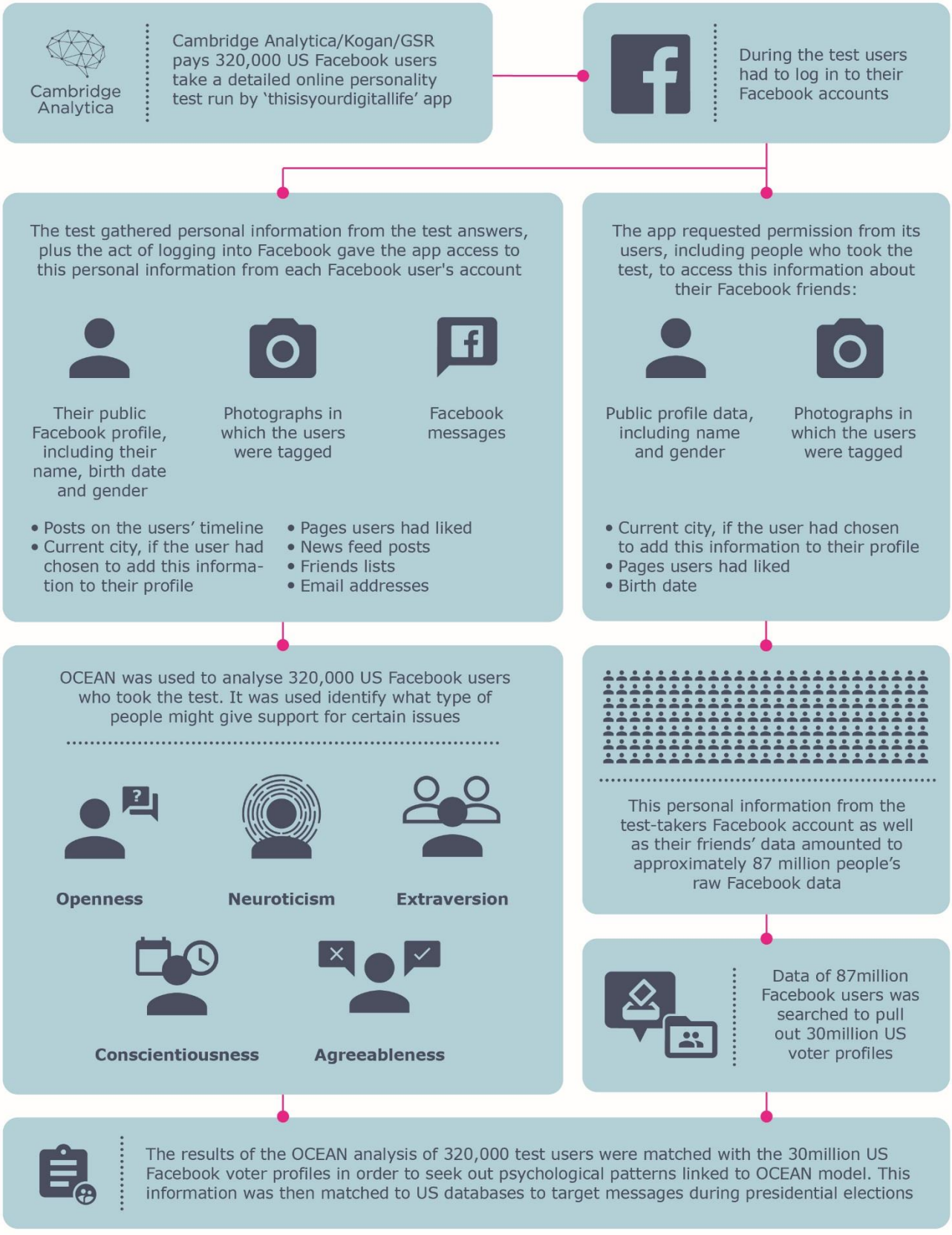
Twitter confirmed that CA/SCL Group placed advertisements for its own and its clients' services on the platform. Twitter did not provide access to CA/SCL for its data products, and had taken a policy decision to 'off-board' all advertising from accounts owned and operated by CA. Twitter explained that this was because Twitter determined that Cambridge Analytica operated a business model that inherently conflicted with acceptable Twitter Ads business practices.

We continue to review their responses to our information requests and are discussing with colleagues on the EDPB Social Media Working Group how best to take forward issues arising from the platforms' use in political processes.

4.3 Cambridge Analytica, Global Science Research (GSR) and the obtaining and use of Facebook data

4.3.1 Accessing data on the Facebook platform

Data harvesting of the Facebook data



One key strand of our investigation has been into allegations that an app, ultimately referred to as 'thisisyourdigitallife', was developed by Dr Aleksandr Kogan and his company GSR in order to harvest the data of at least 50 million (estimated by Facebook themselves to be up to 87 million) global Facebook users, including 1 million in the UK. Some of this data was then used by SCL Elections Ltd, operating under the name of Cambridge Analytica (CA), to target voters during the 2016 US Presidential campaign process.

Whilst the public focus has understandably been on the role of CA and whether it may have contravened the law, the development of the targeting techniques at the centre of this issue date back over a decade and has its origins in the work of academics at the Psychometric Centre of Cambridge University.

The Psychometrics Centre at Cambridge University[2] was set up in 2005 and is a Strategic Research Network dedicated to research, teaching and product development in both pure and applied psychological assessment. One of its key objectives is to provide both academia and R&D departments with cutting-edge tools tailored for the on-line environment. In the run up to 2013, the Psychometrics Centre was carrying out work on psychometric testing. Whilst working at the Centre, academics developed a number of applications (apps) including an app called 'My Personality' based on the OCEAN[3] model developed in the 1980s by two teams of psychologists. The University, and its academics, had an ongoing relationship with Facebook, and, as Dr Kogan has explained in his evidence to various select committees and hearings, was used to receiving and working on various aggregate data sets from Facebook.

[2] https://www.psychometrics.cam.ac.uk/about-us

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

In the age of big data, academics at the center were able to take the OCEAN model and pioneer the use of Facebook data for psychometric testing through the development of the 'My Personality' online quiz. Using the results from people who took the test, they were able to calculate their OCEAN scores and match those scores with other sorts of online data – for example, 'likes', 'shares' and 'posts' on Facebook – to develop personality profiles. They claim to have found that by referring to as few as 68 Facebook 'likes', they were able to predict with a high degree of accuracy a number of characteristics and traits, as well as other details such as ethnicity and political affiliation.

In 2013, Dr Kogan developed his own app (named the 'CPW Lab App' after his personal lab in Cambridge University, the Cambridge Prosociality and Well-Being lab), modelled on the work of the Centre , which he stated he had originally intended to use in the course of his academic research. However, in 2014, Dr Kogan was introduced, via a colleague who knew Mr Wylie, to SCL Elections Ltd, which it is believed was interested in the 'My Personality' app. Dr Kogan approached others at the Psychometric Centre about the possibility of a commercial venture with SCL Elections Ltd, but they decided not to participate on the terms involved.

Under a commercial venture, by means of his company, GSR, established with a partner, Dr Chancellor, Dr Kogan went on to repurpose the 'CPW Lab App', editing its name, its storage, terms and conditions into what is known as the 'GSR App'. The degree to which this was done alongside or separate to his academic work at Cambridge University forms part of our investigation. The app featured a personality test, and it was in relation to this that Dr Kogan entered into a contract with SCL Elections Ltd by which the latter would pay for US citizens to take the test.

In summary, the app accessed up to approximately 320,000 Facebook users to take a detailed personality test that required them to log into

their Facebook account. In addition to the data collected directly from the personality test itself, the app utilised the Facebook Login in order to request permission from the app user to access certain data from their Facebook accounts.

As a result, the app was able to collect the following categories of information from the user to varying degrees, depending on the privacy settings they had implemented on their Facebook profile:

- Public Facebook profile, including their name and gender;
- Birth date;
- Current city, if the user had chosen to add this information to their profile;
- Photographs in which the users were tagged;
- Pages that the users had liked;
- Posts on the users' timelines;
- News feed posts;
- Friends lists;
- Email addresses; and
- Facebook messages.

The app also requested permission from users of the app to access the following categories of data about their Facebook friends (again, subject to the settings they had selected):

- Public profile data, including name and gender;
- Birth date;
- Current city, if the friends had chosen to add this information to their profile;
- Photographs in which the friends were tagged; and
- Pages that the friends had liked.

The total number of users of the app, and their Facebook friends, whose data was accessed through the use of the app, was estimated by Facebook to be approximately 87 million.

A full list of the countries and locations of users affected has been published by Facebook. For some of this Facebook data, estimated to involve around 30 million users, the personality test results were paired with Facebook data to seek out psychological patterns and build models. GSR shared data with SCL Elections Ltd in at least four discrete disclosures. It is believed it then combined this with other sources of data, such as voter records held by SCL, to help inform targeting of individuals in key marginal states with personalised advertising during the presidential election process. Our forensic IT team is working through the many dozens of data sets it has recovered from CA and elsewhere to identify the exact pathway of data and its derivatives (including models developed using the data).

Our investigation has evidence that Dr Kogan shared data accessed from the Facebook platform with others, including but – we believe – not limited to, a US-based company called Euonia Technologies (owned by Mr Wylie) and the Universities of Cambridge (i.e. the CPW Lab) and Toronto.

Users of the app signed up to terms and conditions that allowed access to their Facebook data and that of their friends. However, in our view, this was not a sufficiently informed consent, in particular in relation to the data of friends, and it was not made sufficiently clear that, how and where the data could be sold on to a third-party organization, and how it would be processed or used in the ways described above, given the specific intent of the app and the purpose of GSR being a commercial one. This, and the range and scope of the data obtained, was also a breach of Facebook's platform policy at that time. The app remained in operation on the Facebook platform until at least December 2015, although (in line

with Facebook's announcement in April 2014) its abilities to access data of friends was reduced in May 2015.

Facebook permits third parties to operate apps in conjunction with the Facebook platform. At the relevant time, Facebook's policies permitted third-party apps to obtain personal data about users who installed the app. Whilst the GSR app was in operation, Facebook's default settings also allowed user's friends' data to be collected by the app unless the friends themselves had specifically changed their privacy settings to prevent this from occurring. There were, however, limitations in what this data could be used for; which did not extend to their use for commercial purposes but should instead have only been used to augment those users' experiences.

Following an audit reported in 2014 by the Irish Data Protection Commissioner, which identified a number of issues relating to the transparency with which users were aware that their data could be shared by friends, Facebook introduced changes to the Facebook platform. This reduced the ability of apps to access information about their users and about the Facebook friends of their users. This change included a one-year grace period for many pre-existing apps, which gave them until May 2015 to comply with the new policy. It was during this grace period that the GSR app accessed the majority of its information.

4.3.2 Regulatory issues for Dr Kogan and others

Based on evidence we have in our possession, we are concerned about the way in which data was accessed from the Facebook platform and used for purposes it was not intended for or that data subjects would not have reasonably expected. We are still investigating whether and to what extent Dr Kogan and others are culpable in this respect for Section 55 offences under the DPA 1998. We have written to a number of individuals,

including Dr Kogan, Alexander Nix and Dr Chancellor and invited them to attend interviews, to give us their side of the story. They have so far refused to do so. Our concerns also extend to who else may have received the harvested data and what they then did with it; our enquiries are continuing in that regard.

We have evidence that suggests that Dr Kogan was already in contact with SCL/CA when he applied to Facebook, using his Cambridge University credentials, to pre-emptively migrate his app to version 2 of Facebook's Application Programming Interface (API). It is understood that Facebook rejected this request on 7 May 2014 but allowed Dr Kogan to continue using version 1 of the API in a manner inconsistent with Facebook's Developer Policy until May 2015. We have further concerns arising from Dr Kogan's public statements that, given the nature and scope of his work, Dr Kogan had a poor understanding and awareness of Facebook's policy and applicable data protection laws.

4.3.3 Regulatory issues for SCL Elections Ltd and Cambridge Analytica

On 7h March 2018, under our powers in the DPA 1998, we issued a Demand for Access to premises occupied by SCL Elections Ltd/Cambridge Analytica. Cambridge Analytica did not respond by the deadline provided and offered an unacceptable alternative; therefore, an initial warrant application was heard on 21 March but was adjourned by the High Court until 23 March, when it was granted. We executed the warrant at 20.00 on 23 March and concluded the search at 03.00 on 24 March. We have subsequently secured a further warrant and searched other premises. We have seized significant volumes of evidence and several servers, including servers that had been disconnected from CA systems (which therefore would have been unavailable for onsite inspection in the manner originally suggested by the company). We continue to analyse that evidence.

Regulatory action against SCL/CA remains under consideration, and our investigation continues despite the current status of the organisation; the fact that an organisation happens to be in administration will not prevent the ICO from seeking to progress appropriate regulatory action as far as it is possible to do so. We also recognise it is important that we reach a conclusion about whether the law was broken, regardless of the company's status. In addition to material seized under the warrants, we are also in possession of large data sets provided by third parties that we believe are originally from SCL/CA.

We are in possession of data sets that we believe to be combined data sets, including Facebook harvested data or its derivatives. We have evidence that copies of the data/parts of it also seem to have been shared with other parties and on other systems beyond those of SCL/CA. This potentially brings into question the accuracy of the deletion certificates provided to FB by CA/SCL.

The process of analysing those data sets is ongoing. If evidence does come to light that suggests that individuals are culpable for offences arising from the use of those data sets, or for their onward transfer from CA/SCL systems without authority, we will pursue appropriate regulatory action against them accordingly. This includes any successor companies associated with ex-CA/SCL staff.

As a significant data controller in its own right – which, by virtue of its areas of activity, was holding large data sets of personal data from around the world and connected to its various activities as described in press and media reports – we have looked carefully at CA/SCL's data protection practices. Its responses to our information requests, our meeting with it and evidence secured during our searches has identified significant data protection concerns and poor practice by the company

and its staff. We have therefore indicated our intention to take formal regulatory action against the company for these breaches of the UK's data protection law.

4.3.4 Professor David Carroll complaint against Cambridge Analytica

A specific example of CA/SCL's poor practice with regard to data protection law was its failure to deal properly with a subject access request submitted in January 2017 by Professor David Carroll.

Following a protracted process during which the company had initially denied the ICO's jurisdiction and Professor Carroll's rights, failing to respond fully to our questions, the ICO served an Enforcement Notice on SCL Elections Ltd on 4 May 2018 ordering it to comply with the terms of the Subject Access Request submitted by Professor Carroll (as a US-based academic) under the DPA 1998 by providing copies of all the personal information the company held relating to him, along with an explanation as to the source of the data and its usage by the company.
The terms of the Enforcement Notice were not complied with by the deadline of 3 June 2018. Failure to comply with an Enforcement Notice invites further action, including the possibility of criminal action before the courts. Given the seriousness of these issues and the public interest concerns they raise, we are therefore pursuing the necessary legal avenues in order to bring criminal proceedings against SCL Elections Ltd for failing to properly respond to our Enforcement Notice regarding data held by the company in respect of Professor David Carroll.

4.3.5 Regulatory issues for Facebook group companies

As with other social media platforms, we had started our investigation examining the use of Facebook in the context of elections. We recognised

that many of the issues were common to a range of platforms, and, as with the others, we served Facebook with an Information Notice in this regard on 23 February 2018. However, with the further evidence of the use of Facebook data by GSR and SCL/CA and the specific complaints we have received about this, we have examined closely the operation of the Facebook platform at the time the GSR app was accessing its data. We have also looked at the actions Facebook took in the immediate aftermath of becoming aware of this problem in December 2015, when it suspended the app.

We recognise that Facebook has publicly acknowledged in a number of fora in Europe, Canada and the US issues with the operation of the platform and their follow-up to events in December 2015. Senior Facebook staff have apologised publicly for a variety of failings. They have told us they have made improvements to their systems and processes and have promised further changes. We are also aware that other regulators have looked at their operations at the relevant time and in the time period just prior – for example, our US counterparts and the Irish Data Protection Commissioner.

We have served Facebook with three Information Notices covering issues related to these events, including one covering issues relating to AIQ and the purchase of advertisements. In responding, Facebook has disputed our jurisdiction but has nevertheless answered the majority of our questions. It has promised to respond to the outstanding Notice. It has also reported to us four applications where it has concerns, and has at our request paused its own audit work with some of the subjects of our investigation pending conclusion of our evidence gathering. We have explored options for accessing any subsequent audit findings and for our sharing evidence with Facebook to enable it to follow up with other sources where our investigation evidence suggests that its data may still be found.

The evidence, public statements and comments we have reviewed have identified failings in the respect of the Data Protection Principles for us in relation to the openness and transparency for the processing of personal data by the app (in particular, the personal data of friends of the type accessed by Dr Kogan's app) and the basis for this. We are concerned that, in particular, friends were may not have been sufficiently informed that their data was accessible in this way.

In relation to security, we have questions about whether the technological and organisational measures put in place by Facebook to verify the Terms of Service being used by app developers might not have been sufficiently robust. Also, we are concerned that there might have been a missed opportunity as early as May 2014, when Dr Kogan applied to Facebook explaining he wished to use data for research purposes (a request Facebook declined) but was still allowed to operate his existing permissions; and, in addition, that when it became known in December 2015 that data had been harvested inappropriately that follow-up actions may not have been as robust as they should, particularly, in the context of a known breach of platform policies for commercial gain.

In line with our approach, we have served Facebook with a Notice setting out the detail of our areas of concern and invited their representations on these and any action we propose. Their representations are due later this month and we have taken no final view on the merits of the case at this time and are aware that there are issues which are disputed. We will consider carefully any representations it may wish to make before finalising our view. Our findings and decision on any regulatory action necessary will then be made public. Our policy on communicating regulatory actions makes clear that while we would not normally publish a Notice of Intent, we could do so where there is an over-riding public interest to do so. In this case we consider that the public interest and

profile in these matters, the public nature of much of it, and the commitment to update the DCMS committee so it can progress its work mean we have concluded the balance is in favour of setting out the Notice.

4.4 The relationship between AIQ and SCL Elections Ltd and Cambridge Analytica

Our investigation has been looking into the relationships between CA/SCL Elections and the Canada-based company AIQ.

In early 2014 SCL Elections Ltd/CA approached AIQ to help it build a new political Customer Relationship Management (CRM) tool for use during the American 2014 midterm elections. As part of this arrangement, SCL Elections Ltd required AIQ to transfer to it the intellectual property rights and ownership of the software that AIQ developed. SCL Elections Ltd called the tool RIPON. Work started on this in April 2014 and was designed to help political campaigns with typical campaign activity such as door to door, telephone and email canvassing. In October 2014 AIQ also placed online advertisements for SCL Elections Ltd on behalf of its clients. This work concluded in November 2014.

AIQ worked with SCL on a similar software development, online advertising and website development during the US presidential primaries between 2015 and 2016. AIQ have also confirmed it was directly approached by Mr Wylie when he was employed at SCL Elections Ltd.

AIQ has advised that all work was conducted with SCL Elections Ltd and not Cambridge Analytica and to date we have no evidence that personal data, including that of UK citizens, was shared with them by Cambridge Analytica directly.

AIQ has consistently denied having a closer relationship with SCL Elections Limited than merely software developer and client. Mr Silvester has stated that in 2014 SCL 'asked us to create SCL Canada but we declined'.

In the course of our investigation we have noted the following financial transactions and contacts; on 24 October 2014, SCL Elections Limited made payments to Facebook of around $270,000 for an AIQ ad account. On 4 November 2014, SCL made a payment of around $14,000 for the same AIQ ad account. A refund for unused AIQ ads was later made to SCL, with the explanation that SCL had made pre-payments for its campaigns under AIQ.

SCL Elections was listed as one of the main contacts for at least one of the AIQ Facebook accounts, and the email address for that contact belonged to an SCL employee who was also involved in the payments set out above. This pattern is suggestive of a close working relationship.

Further to this we believe an AIQ employee created and administered two 'apps' that ran on Facebook's platform associated with 'Ripon', the political CRM tool developed by AIQ for Cambridge Analytica. Finally, Mr Massingham's telephone number was listed on SCL Elections Limited's website for 'SCL Canada'. Mr Silvester has stated that he did not know why SCL had listed Mr Massingham's number in connection with SCL.
We continue to investigate the links between the companies insofar as they relate to the acquisition and sharing of UK personal data.

4.5 The university sector, Cambridge University and the Cambridge University Psychometric Centre.

As our investigation has broadened with examination of Dr Kogan's actions and his use of Cambridge University credentials to lend support to

his actions we have engaged with the University at senior level. Our engagement with the University (and others in the UK and abroad) has identified that there are some common issues to tackle.

Cambridge University has fully cooperated with our enquiries to establish to what extent the Psychometric Centre and individuals employed by them pursuing their own private enterprises may have breached data protection law. We have had access to University staff, academics and premises to carry out our work. Questions remain about the use of University equipment and the sufficiency of boundaries between academic studies and the commercial enterprises many academics legitimately establish. The portability of data sets, cross over in roles, sharing of premises and common use of students and postgraduates all serve to create a very complex picture for data protection. We consider there is scope to improve arrangements.

As part of our investigation we are considering whether the university more broadly has sufficient systems and processes in place to ensure that data collected by academics for research is appropriately safeguarded in its use and not re-used for commercial work (for example in the context of Dr Kogan through GSR or shared with third parties). Examination of equipment from the University and linked to Kogan and his work there is ongoing, and will help in this regard.

What is clear is that there is room for improvement in how Higher Education institutions overall handle data in the context of academic research and whilst well-established structures exist in relation to the ethical issues that arise from research, similar structures do not appear to exist in relation to data protection. Given the rapid developments in big data and digital technologies, research could increasingly involve personal data sourced from social media and other third party sources. It is therefore essential that Higher Education institutions have in place the

correct processes and due diligence arrangements to minimise the risk to data subjects and to the integrity of academic research practices.

We have therefore recommended that Universities UK work with the ICO to consider the risks arising from use of personal data by academics in a private research capacity and when they work with their own private companies or other third parties. Universities UK has committed to do so, and will convene a working group of Higher Education stakeholders to consider the wider privacy and ethical implications of using social media data in research, both within universities and in a private capacity.
In respect of the Psychometric centre, Facebook has indicated that it suspended three applications linked to academics there.

While these do not feature in our investigation we will monitor closely any issues or concerns about them. During the course of this investigation a breach in relation to the security of the Psychometric centre and one of its apps was also reported to us and we have launched a separate investigation of this.

The evidence we have gathered alongside the further breach report identifies a need to look carefully at the Psychometric Centre at the University and we will audit the Centre for this, so we can audit their compliance with the DPA 2018. Following this we will then make any specific recommendations required to address any data protection issues in the context of the new Data Protection legislation, based, as it is, on the GDPR.

4.6 Data brokers

We have looked closely at the role of those who buy and sell personal data sets in the UK. We had already started work in this area looking at

common sources of data we came across during our routine enforcement work. This identified links to this enquiry.

During the course of our investigation, we found that some political parties had purchased datasets of personal data from data brokers and used this for election and campaign purposes.

We also have evidence that some data brokers had failed to obtain lawful consent (for example by not explaining who the data would be sold to or how it would be used when it was gathered) for political parties to use those lists in this way.

We have made enquiries with some of the key data brokers operating in the UK supplying data to political parties, including Experian, Emma's Diary (Lifecycle Marketing (Mother and Baby) Ltd), CACI and Data8; raising concerns in relation to fair processing information provided to individuals and in particular whether the data had been obtained and shared in a way that was compliant with the fairness and transparency requirements under the first data protection principle of the DPA98
We have outstanding enquiries with a number of data brokers, and have indicated our intention to take formal action in relation to Emma's Diary (Lifecycle Marketing (Mother and Baby) Ltd) by serving a formal Notice of Intent. We will report the results of any action on our website. We will consider carefully any representations they may wish to make before finalising our view. Our findings and decision on any regulatory action necessary will then be made public. Our policy on communicating regulatory actions makes clear that while we would not normally publish a Notice of Intent we could do so where there is an over-riding public interest to do so. In this case we consider the public interest and profile in these matters, the public nature of much of it and the commitment to update the DCMS committee so they can progress their work mean we have concluded the balance is in favour of setting out the Notice.

We have also been looking at the services and operations of the credit reference agencies in respect of the services they promote to political parties and campaigns. Our existing investigation of the privacy issues raised by their work has been expanded to include their activities in political processes. Our teams will audit the agencies and report their findings by the end of this year.

4.7 The relationship between Cambridge Analytica and Leave.EU

We have investigated the allegation that Cambridge Analytica provided data analytics services to Leave.EU. Our focus has been on the use of personal data and whether Leave.EU breached the DPA98. We served Information Notices on Leave.EU and Cambridge Analytica to gather evidence as part of our investigation.

Information placed in the public domain by some of those subject to investigation suggested a relationship between Cambridge Analytica and Leave.EU, and both sides have acknowledged there was an initial exploration of how to work together during the Referendum campaign. Brittany Kaiser, Director of Program Development at Cambridge Analytica, appeared at a Leave.EU news conference in 2015. Statements by representatives of Leave.EU made in 2016 also indicated that Cambridge Analytica had worked for them. Senior Cambridge Analytica staff also claimed they worked with Leave.EU.

In response to Information Notices served on them, both parties have stated that only preliminary discussions took place, and the relationship did not move forward when Leave.EU failed to attain the designation as the official Leave campaign. In evidence provided to the ICO, Leave.EU stated that four meetings took place:

1. 23 October 2015 representatives of Leave EU met with CA staff, this was a basic introductory meeting to express interest in potentially working together.

2. 18 November 2015 CA appeared at a press conference with Leave.eu

3. 20 November 2015 CA went to Leave.EU's Bristol offices and pitched their product.

4. 8 January 2016 representatives of Leave.EU met CA in London, and CA presented a proposal for future work together.

During our investigation allegations were made that Cambridge Analytica were paid for work on UKIP data in 2015, and that Leave.EU paid for this work. The ICO served an information notice on UKIP as part of this investigation. They appealed the notice to the Information Tribunal and at the time of writing that appeal is ongoing.

4.8 Relationship between Leave.EU and Eldon Insurance, Big Data Dolphins and the University Of Mississippi case

We are investigating allegations that Eldon Insurance Services Ltd shared customer data obtained for insurance purposes with Leave.EU and that the data was then used for political campaign purposes during the EU referendum, contrary to the first and second data protection principles under the DPA 98. We are also investigating whether Eldon Insurance Ltd call centre staff used customer databases to make calls on behalf of Leave.EU in contravention of the Privacy and Electronic Communication Regulations 2003.

On 25th October 2017 we issued an Information Notice to Leave.EU. This was followed by a subsequent Information Notice to Leave.EU and a number of related companies and individuals.

The purpose of the Information Notices was to obtain information about whether personal data held by Eldon Insurance was provided to various organisations associated with the Leave campaign, and if so how it was used.

In addition, we are investigating allegations that insurance customer data was sent to the USA and in particular to the University of Mississippi, and whether that was a contravention of the eighth data protection principle under the DPA98.

The ICO has engaged with the University of Mississippi, seeking to understand whether the personal data of UK citizens has been transferred to the US by Eldon Insurance Services or related companies. This line of enquiry is ongoing.

A UK resident had also, filed a law suit in a Mississippi court to determine whether any UK data was transferred to Mississippi and whether the data was then used to illegally target voters during the EU referendum campaign.

On the 26th April the Court issued a temporary preservation order to prevent any UK personal data held at the University of Mississippi being removed. The ICO was then made aware of the order and provided a letter in support of the preservation request but not joining in the case, as it would of course be of interest to the ICO that any potentially relevant evidence was preserved.

On the 21st June 2018 the case for a permanent preservation order was rejected by the Court, as the Court found that the plaintiff had not exhausted all reasonable means of finding out whether his data was being held by the University. We continue to liaise with senior officials at the University in this regard.

4.9 The relationship between Aggregate IQ, Vote Leave and other Leave campaigns

In response to information requested by the ICO from Facebook they confirmed on 18th May 2018 that AIQ created and, in some cases, placed advertisements ('ads') on behalf of the DUP Vote to Leave campaign, Vote Leave, BeLeave and Veterans for Britain.

The majority of the ads – 2,529 out of a total of 2,823, were created on behalf of Vote Leave.

In the run-up to the referendum vote on 23rd June 2016, AIQ ran 218 ads solely on behalf of Vote Leave and directed at email addresses on Facebook. Facebook believe the email addresses originated from a different source than the data collected through the GSR app. Facebook confirmed that Vote Leave and BeLeave used the same data set to identify audiences and select targeting criteria for ads. However, BeLeave did not then go on to run any ads, albeit their electoral return indicates that they committed expenditure to this. Vote Leave ran 1,034 ads between 19th April 2016 and 20th June 2016.

Payment for all of these Facebook ads was made by AIQ, and amounted to around $2 million (approximately £1.5 million) between 15th April 2016 and 23rd June 2016. Our regulatory concern is therefore whether, and on

what basis, the two groups have shared data between themselves and others.

The Electoral Commission have separately investigated allegations of coordination between Vote Leave and BeLeave and whether there was a breach of the electoral rules. We have had contact with the Electoral Commission and shared relevant evidence where appropriate under our legal gateway.

We have established that AIQ had access to UK voter personal data provided from the Vote Leave campaign. We are currently working to establish where they accessed that personal data, and whether they still hold personal data made available to them by Vote Leave. We are engaging with our regulatory colleagues in Canada, including the federal Office of the Privacy Commissioner and the Office of the Information and Privacy Commissioner, British Columbia.

As a result of a report, we have identified 397 email addresses and names relating to the UK, out of a total of 1,439 email addresses, that AIQ made publically accessible via GitLab, and which were discovered by a cyber security specialist. This information was backed up to AIQ's server on 20th March 2017 and 27th April 2017.

The investigation into the activities of AIQ have presented a number of jurisdictional challenges. In their letter of the 5th March 2018, in response to a number of enquiries, AIQ stated that they were 'not subject to the jurisdiction of the ICO' and ended with a statement that they considered their involvement in the ICO's investigation as 'closed'.

It was during this period that the Information Commissioner advised the Canadian Parliament that AIQ had not been cooperating with our investigations, noting that they had previously not answered our

questions fully or at all. Since then AIQ have agreed to cooperate with our investigation in full and we have been in contact with them.
On 5th April 2018 the OPC and BC announced that they were jointly investigating Facebook and AIQ as to whether the organisations are in compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the BC's PIPA. The investigation is to look into allegations about unauthorised access and use of Facebook user profiles.

The ICO has shared information in relation to our own investigation with both authorities and both authorities have shared information with us. We have also served AIQ with an Enforcement Notice requiring that they cease processing of UK citizen data.

4.10 Vote Leave

We are investigating whether and how Vote Leave transferred the personal data of UK citizens outside the UK and whether this was breach of the Data Protection Act 1998, and whether that personal data has also been unfairly and unlawfully processed.

We served Information Notices on Vote Leave on 13th September 2017 and 20th December 2017, in order to obtain evidence about how they obtained and used personal data, and the organisations with whom they shared information. We continue to engage with individuals, including Mr Dominic Cummings, in relation to information we believe they hold, and which we believe is of relevance to the investigation.

On 14th June 2018, we served a further Information Notice to Vote Leave. We expect to be in a position to take decisions on potential formal enforcement action within the next three months.

4.11 The Remain campaign

We are investigating the collection and sharing of personal data by the official Remain campaign – the In Campaign Limited, trading as Britain Stronger in Europe (BSiE), and a linked data broker. We are specifically looking at inadequate third party consent and the fair processing statements used to collect personal data. These are similar issues as we have explored on the Leave and wider political parties side of our investigation.

On 19th June 2018, an Information Notice has been served on Open Britain, the successor organisation to BSiE, under the Data Protection Act 1998. Again, we expect to be in a position to take decisions on potential formal enforcement action within the next three months.

5. Summary of potential regulatory action

In the course of this initial phase of our investigation we have identified the following regulatory action:

- 11 warning letters requiring action by the main political parties backed by Assessment Notices for audits later this year.

- An Enforcement Notice for SCL Elections Ltd to deal properly with Professor Carroll's subject access request.

- A criminal prosecution for SCL Elections Ltd for failing to properly deal with the ICO's Enforcement Notice.

- An Enforcement Notice for AiQ to stop processing retained UK Citizen data.

- Notices of Intent to take regulatory action for a data broker Emma's Diary (Lifecycle Marketing (Mother and Baby) Ltd), and Facebook Group of companies.

- Audits of the main credit reference companies and Cambridge University Psychometric centre.

6. Next steps

Our teams continue to pursue active lines of enquiry to finalise the issues we have set out above. There is a considerable amount of relevant material to review from retrieved servers and equipment and we continue to pursue interviews with key individuals, including those who have so far refused to speak with us, to provide them an opportunity to provide their account and evidence.

We have also committed to undertake audits of several organisations linked to the investigation, and, where they relate to the Facebook material, we will seek to examine their systems for traces of the data accessed from the Facebook platform.

We are aware of a number of locations and systems to which we believe the data has been sent and are liaising with a number of organisations and other regulators to ensure the deletion of the data and any derivatives; this will include companies established by ex-CA/SCL staff where we have concerns they may have retained materials from SCL Group following their administration.

We anticipate that we will have concluded this next phase of our investigative work by the end of October 2018.

Annex i: Organisations of interest

Advanced skills initiative

Aggregate IQ

BeLeave

CACI

Cambridge Analytica / SCL Elections

Cambridge University

Clarity Campaigns

Data8

Democratic Unionist Party

Eldon Insurance

Emma's diary

Experian

Facebook

Google

Grass Roots Out

Green Party

Plaid Cymru

Scottish National Party

Sinn Fein

Snapchat

Social Democratic and Labour Party

The Conservative party

The In Campaign/Open Britain

The Labour Party

The Liberal Democrats

The Messina Group

Twitter

UKIP

Ulster Unionist Party

Veterans for Britain

Vote Leave

Annex ii: Regulatory action documents

Enforcement notice – Aggregate IQ

Notice of intent – Facebook

Notice of intent - Emma's Diary (Lifestyle Marketing (Mother and Baby) Ltd)