Information Commissioner's Office

Investigation into the use of data analytics in political campaigns

A report to Parliament

6 November 2018

ico.

Information Commissioner's Office

Table of contents

Commissioner's message

When we opened our investigation into the use of data analytics for political purposes in May 2017, we had little idea of what was to come.

Eighteen months later, multiple jurisdictions are struggling to retain fundamental democratic principles in the face of opaque digital technologies.

The DCMS Select Committee is conducting a comprehensive inquiry into Disinformation. The EU says electoral law needs to be updated to reflect the new digital reality, initiating new measures against electoral interference. A Canadian Parliamentary Committee has recommended extending privacy law to political parties and the US is considering introducing its first comprehensive data protection law.

Parliamentarians, journalists, civil society and citizens have woken up to the fact that transparency is the cornerstone of democracy. Citizens can only make truly informed choices about who to vote for if they are sure that those decisions have not been unduly influenced.

The invisible, 'behind the scenes' use of personal data to target political messages to individuals must be transparent and lawful if we are to preserve the integrity of our election process.

We may never know whether individuals were unknowingly influenced to vote a certain way in either the UK EU referendum or the in US election campaigns. But we do know that personal privacy rights have been compromised by a number of players and that the digital electoral eco-system needs reform.

My office's report to Parliament beings the various strands of our investigation up to date. We intended our investigation to be comprehensive and forensic. We have identified 71 witnesses of interest,

reviewed the practices of 30 organisations and are working through 700 terabytes – the equivalent of 52 billion pages – of data.

We have uncovered a disturbing disregard for voters' personal privacy. Social media platforms, political parties, data brokers and credit reference agencies have started to question their own processes – sending ripples through the big data eco-system.

We have used the full range of our investigative powers and where there have been breaches of the law, we have acted. We have issued monetary penalties and enforcement notices ordering companies to comply with the law. We have instigated criminal proceedings and referred issues to other regulators and law enforcement agencies as appropriate. And, where we have found no evidence of illegality, we have shared those findings openly.

Our investigation uncovered significant issues, negligence and contraventions of the law. Now we must find the solutions. What can we do to ensure that we preserve the integrity of elections and campaigns in future, in order to make sure that voters are truly in control of the outcome?

Updated data protection law sets out legal requirements and it should be government and regulators upholding the law. Whilst voluntary initiatives by the social media platforms are welcome - a self-regulatory approach will not guarantee consistency, rigour or public confidence.

A Code of Practice for use of personal data in campaigns and elections, enshrined in law - will give our powers a sharper edge, providing clarity and focus to all sectors, and send a signal from parliament to the public that it wants to get this right.

I have also called for the UK Government to consider whether there are any regulatory gaps in the current data protection and electoral law

landscape to ensure we have a regime fit for purpose in the digital age. We are working with the Electoral Commission, law enforcement and other regulators in the UK to increase transparency in election campaign techniques.

The General Data Protection Regulation (GDPR) was designed to regulate the use of personal data in the internet age. It gives data protection authorities the tools to take action where breaches of this kind occur.

Data protection agencies around the world must work with other relevant regulators and with counterparts in other jurisdictions to take full advantage of the law to monitor big data politics and make citizens aware of their rights.

This is a global issue, which requires global solutions. I hope our investigation provides a blueprint for other jurisdictions to take action and sets the standard for future investigations.

Elizabeth Denham

UK Information Commissioner

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

This is the summary report of our investigation. It covers the areas we investigated, our findings and our actions to date. Where we have taken regulatory action, the full details of our findings are – or will be – set out in any final regulatory notices we issued to the parties being investigated.

A separate report, Democracy Disrupted? Personal Information and Political Influence was published in July 2018, covering the policy recommendations from the investigation.

One of the recommendations arising from this report was that the Government should introduce a statutory code of practice for the use of personal data in political campaigns and we have launched a call for views on this code.

We will continue to pursue any actions still outstanding at the time of writing. Regulatory action taken to date:

Political parties

- We sent 11 warning letters requiring action by the main political parties, backed by our intention to issue 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 the use of third party data analytics companies, with insufficient checks around consent.

Cambridge Analytica and SCLE Elections Limited

- Cambridge Analytica (CA) is a trading name of SCLE Elections Ltd (SCLE) and so the responsibilities of the companies often overlapped. Both are subsidiaries of SCLE Group (SCL). For ease of reading we will be referring to all the company entities using Cambridge Analytica.
- We issued an enforcement notice requiring the company to deal properly with Professor David Carroll's Subject Access Request.
- Despite the company having entered into administration, we are now pursuing a criminal prosecution for failing to properly deal with the enforcement notice.
- While we are still conducting our investigations and analysis of the evidence we have recovered so far, we've already identified serious breaches of data protection principles and would have issued a substantial fine if the company was not in administration.
- We are in the process of referring CA to the Insolvency Service.

Facebook

- We issued Facebook with the maximum monetary penalty of £500,000 available under the previous data protection law for lack of transparency and security issues relating to the harvesting of data. We found that Facebook contravened the first and seventh data protection principles under the Data Protection Act 1998 (DPA1998).
- We are in the process of referring other outstanding issues about Facebook's targeting functions and techniques used to monitor individuals' browsing habits, interactions and behaviour across the internet and different devices to the Irish Data Protection Commission, as the lead supervisory authority for Facebook under the General Data Protection Regulation (GDPR).

Leave.EU and Eldon Insurance

- We issued a notice of intent to fine both Leave.EU and Eldon Insurance (trading as GoSkippy) £60,000 each for serious breaches of the Privacy and Electronic Communications Regulations 2003 (PECR), the law which governs electronic marketing. More than one million emails were sent to Leave.EU subscribers over two separate periods which also included marketing for GoSkippy services, without their consent. This was a breach of PECR regulation 22.
- We also issued a notice of intent to fine Leave.EU £15,000 for a separate, serious breach of PECR regulation 22 after almost 300,000 emails were sent to Eldon Insurance (trading as GoSkippy) customers containing a Leave.EU newsletter.
- We have issued a preliminary enforcement notice to Eldon Insurance under s40 of the DPA1998, requiring the company to

take specified steps to comply with PECR regulation 22. We will follow this up with an audit of the company.

- We are investigating allegations that Eldon Insurance Services Limited shared customer data obtained for insurance purposes with Leave.EU. We are still considering the evidence in relation to a breach of principle seven of the DPA1998 for the company's overall handling of personal data. A final decision on this will be informed by the findings of our audit of the company.

We have also begun a wider piece of audit work to consider the use of personal data and data sharing in the insurance and financial sectors.

Relationship between AggregateIQ, Vote Leave and other leave campaigns

- We issued an Enforcement Notice to AggregateIQ to stop processing retained UK citizen data.
- We established the contractual relationship between AggregateIQ and the other related parties. We also investigated their access to UK personal data and its legality. And we engaged 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.

Remain campaign

- We are still looking at how the Remain side of the referendum campaign handled personal data, including the electoral roll, and will be considering whether there are any breaches of data protection or electoral law requiring further action. We investigated the collection and sharing of personal data by Britain Stronger in Europe and a linked data broker. We specifically looked at

inadequate third party consents and the fair processing statements used to collect personal data.

Cambridge University

- We conducted an audit of the Cambridge University Psychometric Centre and made recommendations to ensure that the university makes improvements to its data protection and information security practices, particularly in the context of safeguarding data collected by academics for research.
- We also recommended that Universities UK work with all universities to consider the risks arising from use of personal data by academics. They have convened 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.

Data brokers

- We issued a monetary penalty in the sum of £140,000 to data broker Emma's Diary (Lifecycle Marketing (Mother and Baby) Limited), for a serious breach of the first principle of the Data Protection Act 1998.
- We issued assessment notices to the three main credit reference agencies - Experian, Equifax and Call Credit - and are in the process of conducting audits.
- We have issued assessment notices to data brokers Acxiom Ltd, Data Locator Group Ltd and GB Group PLC.
- We have looked closely at the role of those who buy and sell personal datasets in the UK. Our existing investigation into privacy

issues raised by their services has been expanded to include their activities in political campaigns.

172 organisations identified.

30 organisations formed the main focus of the investigation.

71 witnesses of interest.

40 ICO investigators

31 information notices issued

2
- warrants executed
- monetary penalties
- enforcement notices

1 criminal prosecution

22 documents seized.

85 pieces of equipment seized including servers.

700 terabytes of data seized, equivalent to 52.5 billion pages.

1. Introduction

1.1 Background

In early 2017, a number of media reports in *The Observer* newspaper alleged that a company, 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 Commissioner stated that the office 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, we announced in May 2017 that we were launching a formal investigation into the use of data analytics in political campaigns - in particular, whether there had been any misuse of personal data and, therefore, breaches of data protection law during the referendum. At the same time, we committed to producing a policy report, which was published in July 2018.[1]

The subsequent investigation identified a number of additional strands of enquiry that required consideration. Three other ongoing ICO operations, investigating sectors such as credit reference agencies and data brokers, also revealed evidence of relevance to this investigation. The investigation ultimately involved various online platforms, data brokers, analytics firms, academic institutions, political parties and campaign groups. The nature of modern campaigning techniques and data flows meant that some of

[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/

these organisations of interest to the investigation are located outside the UK.

1.2 The scale of the investigation

This is the most complex data protection investigation we have ever conducted. Not only has it required us to draw on the full range of regulatory tools available to the ICO, but it has been a catalyst for our request for additional powers. These additional powers were granted by Parliament in the Data Protection Act 2018 (DPA2018).

It is exceptional in that many of the key players have offered their evidence publicly in various parliamentary and media forums around the world, and at different times. Our investigation has had to react to and address an abundance of claims and allegations played out in public. We have also had to respond to further offers of information from whistleblowers and former employees at some of the organisations under investigation, and this has on occasion caused us to review, reconsider and rethink elements of the evidence previously presented by those organisations.

At times it has required the full-time focus of more than 40 ICO investigators. A significant number of external experts have been contracted to provide legal and forensic IT recovery support for various aspects of the investigation.

The investigation has identified a total of 172 organisations that required initial engagement, of which 30 have formed the main focus of our investigation. These include political parties, data analytics companies and major online platforms.

Similarly, we spoke to nearly 100 individuals of interest, including through formal interviews, and we continue to engage with people who hold information of relevance to the investigation.

The aim 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.

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.

We have used the full range of our powers under both the current and previous data protection legislation, including:

- serving information notices to request provision of information from organisations in a structured way (with changes to legislation, these can now be issued to 'persons' as well as data controllers);
- serving enforcement notices requiring specific action to be taken by a data controller in order to comply with data protection legislation;
- attending premises to carry out investigations and examine and seize material relevant to our investigation (backed by a warrant to do the same if access is unreasonably refused); and
- issuing monetary penalty notices to sanction data controllers for breaches of the law.

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.

Our investigation also had a considerable inter-agency and international dimension. In the UK we have worked with the Electoral Commission and the National Crime Agency and have taken advice from the Insolvency Service and the Financial Conduct Authority.

Several disclosures to us suggested offences beyond the scope of the ICO's legal remit, and we 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 law enforcement and so we worked with our counterparts in Canada and

the United States (US) to co-ordinate elements of our investigation. We have legal gateways to share and receive information through the DPA 2018 and that has assisted with our investigation and also those of other data protection authorities. We also have links to data protection authorities worldwide through our links to the Global Privacy Enforcement Network (GPEN).

We are interrogating 700 terabytes of data - the equivalent of 52.2 billion pages - taken from machines both voluntarily surrendered and seized, as well as information stored on cloud servers.

1.3 The importance of the investigation

Rapid developments in technology and social media over the last 15 years have, inevitably, led to data-driven campaigns, as political parties seek to follow commercial organisations by taking advantage of increasingly sophisticated marketing techniques to engage with voters.

The fact that political parties and campaigns all over the world have invested heavily in digital messaging in recent years shows the potential to reach more people in an efficient, targeted and accessible manner, for a fraction of the cost of more traditional methods.

This brings a number of advantages. Social media provides unprecedented opportunities to engage hard-to-reach groups in the democratic process on issues of particular importance to them. However, these developments have been so rapid that many voters are unaware of the scale and context in which they are being targeted. The public have the right to expect that political messaging is conducted in accordance with the law.

Our investigation focused particularly on the data protection principle of transparency. If voters are unaware of how their data is being used to target them with political messages, then they won't be empowered to exercise their legal rights in relation to that data and the techniques being deployed, or to challenge the messages they are receiving.

Without a high level of transparency and trust amongst citizens that their data is being used appropriately, we are at risk of developing a system of voter surveillance by default.

It is impossible for us to say whether the data techniques used by either side in the UK EU referendum campaign impacted on the result. However, what is clear is that we are living in an era of closely fought elections, where the outcome is likely to be decided on the votes of a small number of people. There are significant gains to be made by parties and campaigns which are able to engage individual voters in the democratic debate and on areas of public policy that are likely to influence the outcome.

There is no turning back the clock – digital elections are here to stay. We need to work on solutions to protect the integrity of our democratic processes. We believe our call for a statutory code to clearly set out the law, along with our enforcement action, our engagement with political parties, campaigns, social media platforms and Universities UK for reform of the political eco-system are all positive steps.

2. Regulatory enforcement action

The investigation is considering potential criminal offences as well as wider regulatory issues.

We focused on the following main issues:

2.1 Failure to properly comply with the Data Protection Principles

Under the previous law, anyone who processes personal data must comply with eight principles of the DPA1998, which state that personal information must be:

- 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 individuals' rights;
- secure; and
- not transferred to other countries without adequate protection.

2.2 The relationship between the GDPR and the Data Protection Act 1998

The DPA1998 was replaced by the GDPR and the Data Protection Act 2018 (DPA2018) on 25 May 2018. Throughout this investigation, consideration has been given to all relevant legislation, including transitional provisions.

2.3 Failure to properly comply with the Privacy and Electronic Communications Regulations

These regulations sit alongside data protection legislation. 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.

2.4 Section 55 offences of the Data Protection Act 1998

It is a criminal offence to knowingly or recklessly, without the consent of the data controller, obtain or disclose personal data or the information contained within it. Additionally, it is an offence to procure the disclosure to another person of the information contained in personal data. It is also an offence for someone to sell data if it has been obtained in those circumstances.

We have also examined the evidence we recovered to identify where other criminal offences may have been committed; this included criminal offences related to the failure to comply with information notices or enforcement notices issued by the ICO, as well as other offences.

We looked at organisations and also the actions of individuals controlling them during the relevant periods.

2.5 This report

This report summarises the areas we investigated, actions taken and any areas where our work needs to continue. The full details of our findings

are – or will be – set out in any final regulatory notices we issue to the parties subject to investigation.

Some of these investigations have resulted in the publication of a notice of intent, where the Commissioner expresses her intention to impose a monetary penalty. See our Communicating Regulatory Activity policy. The affected parties then have a chance to respond to the notice of intent, after which a final decision will be made.

3. Summary of investigations and regulatory action taken

3.1 Political parties

Our investigators interviewed representatives and reviewed the practices of the main political parties in the UK. Parties were asked to provide information about how they obtain and use personal data, and the steps they take to comply with data protection legislation.

We concluded that there are risks in relation to the processing of personal data by all the major 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;
- the use of third-party data analytics companies with insufficient checks that those companies have obtained correct consents for use of data for that purpose;
- assuming ethnicity and/or age and combining this with electoral data sets they hold, raising concerns about data accuracy;
- the provision of contact lists of members to social media companies without appropriate fair processing information and collation of social media with membership lists without adequate privacy assessments.

The formal warnings included a demand for each party to provide Data Protection Impact Assessments (DPIAs) for all projects involving the use of personal data.

Under the GDPR, data controllers are required to complete a DPIA wherever their intended processing is 'likely to result in high risk' to the rights and freedoms of data subjects.

Because parties are using special category data (relating political opinions and ethnicity), as well as automated decision making and profiling, they would therefore be required undertake a DPIA under the GDPR.

A DPIA gives a systematic and objective description of the intended processing and considers the risk to people's personal data – not only the compliance risk of the organisation involved. The ICO provides written advice to organisations about their DPIAs and can issue warnings where we consider projects would potentially breach the GDPR.

The formal warnings were issued to 11 political parties (Conservatives, Labour, Lib Dems, Greens, SNP, Plaid Cymru, DUP, Ulster Unionists, Social Democrat, Sinn Féin and UKIP) detailing the outcome of our investigation and the steps that needed to be taken. We required them to report on the actions taken within three months.

Processing personal data in the context of political campaigning can be complex and we require additional confirmation on the parties' data activities, particularly in light of changes to the law. We will be issuing assessment notices and carrying out audits of the parties from January 2019.

One of the main recommendations from our Democracy Disrupted? report is that the Government should legislate at the earliest opportunity to introduce a statutory code of practice under the DPA2018 for the use of personal information in political campaigns.

We have met with the Cabinet Office, DCMS and the Electoral Commission to discuss how this can be achieved before the next General Election. We have launched a call for views on the code.

In particular, we are interested in views from political parties, campaign groups, potential electoral candidates, data brokers, companies providing online marketing platforms, relevant regulators, think-tanks, interested academics, the general public and those representing the interests of the public.

We anticipate that the code will apply to all data controllers which process personal data for the purpose of political campaigning. By 'political campaigning' we mean activity which relates to elections or referenda, in support of or against a political party, a referendum campaign or a candidate standing for election. This includes but is not limited to processing by registered political parties, electoral candidates, referendum permitted participants and third party campaigners, as defined in the Political Parties and Referendums Act 2000.

3.1.1 – The United Kingdom Independence Party (UKIP)

We issued an information notice to UKIP in the early stages of our investigation, specifying information we required it to provide for our investigation. UKIP appealed against our notice to the First Tier Information Tribunal in November 2017.

The Tribunal dismissed this appeal on 10 July 2018, stating that UKIP's response to the information notice was brief, inadequate and, in some instances, possibly inaccurate - and that UKIP's apparent willingness to co-operate with the Commissioner's enquiries, rendering an information notice unnecessary, was insufficient grounds for allowing the appeal.

UKIP has since appealed this dismissal decision to the Upper Tribunal (Administrative Appeals Chamber), and we are awaiting a date for the hearing to be set.

Therefore, at the time of writing we are unable to progress the part of the investigation involving this information notice for UKIP. We will pursue this once the legal process has concluded, in order to ensure that we have a complete understanding of UKIP's practices and involvement with the other organisations under investigation.

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

3.2.1 Accessing data on the Facebook platform

One key strand of our investigation involved allegations that an app, ultimately referred to as 'thisisyourdigitallife', was developed by Dr Aleksandr Kogan and his company Global Science Research (GSR) in order to harvest the data of up to 87 million global Facebook users, including one million in the UK. Some of this data was then used by Cambridge Analytica, to target voters during the 2016 US Presidential campaign process.

It should be noted that a number of companies including Cambridge Analytica (UK) Limited and SCLE Elections Limited (SCLE) operated as part of the SCLE Group of Companies (SCLE) under the more publicly

familiar trading name Cambridge Analytica (CA). For ease of reading we will be referring to all the company entities using 'Cambridge Analytica/CA', unless there is a specific point which requires further clarification.

In 2008, Facebook launched V1 of their Graph Application Platform Interface (API). This platform allowed third party application developers access to a wealth of data concerning Facebook users and their Facebook friends. In order to obtain this information, app developers had to request permission directly from app users prior to their use of the developer's app; this authorisation allowed the app developers access to users' Facebook friends information as well as the information of the app user.

Facebook produced a range of policies for developers who deployed apps on their platform. However, as a result of our investigation, we have concluded that despite these policies, Facebook did not take sufficient steps to prevent apps from collecting data in contravention of data protection law.

Over the course of 2011 and 2012, the office of the Irish Data Protection Commissioner (IDPC) audited Facebook's European headquarters in Ireland and identified concerns surrounding the prominence of Facebook privacy policies and giving users more granular privacy controls regarding the use and accessibility of Facebook friends' data.

Our investigators uncovered evidence from a range of sources to show that there was a close working relationship between Facebook and individual members of the research community. Witnesses described a process whereby there were frequent meetings and travel at Facebook's expense for those undertaking work and research associated with the platform, and much collaboration between the company and the academic

community. This included many individuals involved in research eventually going on to work at the company. We understand that this engagement with academics continued up until 2016.

Any new apps on the platform were automatically added to API V2 and did not have access to Facebook friend data.

In the run up to 2013, the Psychometric Centre at Cambridge University was carrying out work on psychometric testing. Whilst working at the Centre, academics, including Dr David Stillwell and Dr Aleksandr Kogan continued to develop a number of applications (apps) including an app called 'My Personality' based on the OCEAN[1] model developed in the 1980s.

Academics at the Psychometric Centre pioneered the use of Facebook data (in connection with the OCEAN model) 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. The academics 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.

By 2014, Facebook had begun to migrate third party apps from API V1 to V2, which limited developers' access to Facebook friend data. In order to

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

ensure continuity of service for Facebook users and app developers, Facebook gave developers a one-year 'grace period' in order to allow time to adjust their apps' code and also to adapt their business models to account for the withdrawal of access to Facebook friend data.

During the course of our investigation, the ICO has reviewed evidence which suggests around the same time in 2014, CA wanted to take advantage of the pre-existing access to Facebook friend data enjoyed by app developers with access to V1 of Facebook's API. They planned to use this data in order to create data models which would inform on their work on electoral campaigns in the USA. However, CA themselves could not access V1 at this time because they did not have a pre-existing app on the platform.

Witnesses have told us that in order to gain access to Facebook friend data on API V1, CA initially discussed a collaboration with Dr David Stillwell. Dr Stillwell's app, 'MyPersonality' had already collected a large Facebook dataset – this data was legitimately collected for academic purposes. Dr Stillwell refused CA's offer, citing data protection concerns as his reason for not allowing the company access to the MyPersonality dataset.

In May 2014, Dr Aleksandr Kogan, another academic with links to Cambridge University, who had been involved in discussions with CA along with Dr Stillwell, offered to undertake the work himself as he had developed his own app called the 'CPW Lab App' - later renamed as Thisisyourdigitallife - which was operating on API V1.

We have seen evidence that CA staff, including whistleblower Chris Wylie, were involved in setting up these contacts through their networks of

friends and colleagues; many of whom had been involved in earlier campaigns in North America.

The ICO has evidence that CA staff assisted Dr Kogan to set up GSR. Once the company was set up and a contract signed with CA, Dr Kogan, with some help from Chris Wylie, overhauled the 'CPW Lab App' changing the name, terms and conditions of the app into the 'GSR App' which ultimately became thisisyourdigitallife (the app). Information reviewed by the ICO suggests that in order for a Facebook user's data to be harvested and processed by CA, the user, or one of their Facebook friends, would have had to log into and authorise the app. The data of these users and their Facebook friends was then available to GSR and, ultimately, to CA.

In summary, the new app accessed up to approximately 320,000 Facebook users to take a detailed personality test while logged 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;
- Facebook 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.

During his appearance before the DCMS Select Committee, Dr Kogan explained that GSR then took a Facebook user's answers to the app survey and used them to make predictions about the Facebook user. This information was then combined with other information taken from the user's Facebook profile, such as the pages the Facebook user had liked and used to build a data model about that individual which could predict how the user was likely to vote. However, because of the configuration of API V1, GSR also received the public profile information about the app users' Facebook friends, including their Facebook likes. As such GSR was able to provide modelled data about the 'app' user and their Facebook friends whose privacy settings allowed access by third party apps.

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 approximately 30 million US users, the personality test results were paired with Facebook data to seek out psychological patterns and build models.

Obtaining Facebook data

In order to understand how the Facebook data was extracted, transferred and used, it is first necessary to define precisely whose data was involved.

- The GSR app (the app) was able to obtain the data of Facebook users who used the app.
- Additionally, the app was also able to obtain the data of the app user's Facebook friends (app user's friend).

The precise nature and quantity of data which was available for the app to access was defined by the particular 'privacy settings' which the app user and the app user's friend selected on their own Facebook profiles.

Unless it was specifically prevented by the app user, and the app user's Friend, the app was able to access the data of both persons by default.

CA commissioned a third party survey company called Qualtrics who then sought out and paid members of the public, less than a dollar to access the App. This was done in order to maximise the number of Facebook Users' data which was accessible to GSR and, ultimately, CA.

Once the data had been obtained by GSR, it was then modelled and transferred to a secure 'drop-zone'. From this drop-zone, CA was then

able to extract the modelled data relating to data subjects that they were interested in and for whom they had pre-existing data.

CA's internal data scientists then performed further data modelling and created 'proprietary data models' that they then used during their political targeting work in the US.

When Facebook was initially alerted to the breach by media coverage in 2015, Facebook contacted CA informing them that CA had breached Facebook's terms and conditions and then asked CA to delete all data and any derivative data it was holding.

Using our powers under the DPA1998, the ICO obtained a warrant for access to the premises of CA. We executed the warrant at 20.00 on 23 March and concluded the search at 03.00 the following morning. We subsequently secured a further warrant and searched other premises linked to the companies.

In the course of these actions we seized significant volumes of evidence, including mobile telephones, storage devices, tablets, laptops, numerous servers, financial records and paperwork of relevance to our enquiries. At one location we discovered a number of disconnected and physically damaged servers; these servers have been subject to intense digital analysis to recover relevant material at component level.

The ICO is continuing to review evidence seized during the execution of the warrants. However, CA employees have confirmed that although some effort was made to delete the Facebook data at various points ranging from when Facebook initially contacted the company to just after we announced our investigation, some 'proprietary data models', data models derived from the data harvested from Facebook, may not have

been deleted. We will be making sure any organisations, which may still have copies of the Facebook data and its derivatives demonstrate its deletion.

During the time period stated, Facebook's policies permitted third-party apps to obtain personal data about users who installed the app, and in some circumstances, the data of the user's friends. However, Facebook's platform policy sought to impose limitations on what this data could be used for – it was focused on providing for enhanced user experiences, and did not extend to its use for commercial purposes. Any terms of service changes used by app developers were supposed to comply with Facebook's terms of service and policies, and developers should have been aware of this.

3.2.2 Regulatory issues for Dr Kogan and others

Based on evidence we have received or recovered, we are concerned about the manner in which data from the Facebook platform was accessed by Dr Kogan and his company GSR, and how it was then used for purposes for which it was not originally collected and for purposes that data subjects would not have reasonably expected. We are still investigating whether and to what extent Dr Kogan and others are individually culpable in this respect for potential Section 55 offences under the DPA1998.

However, we have seen evidence that CA sought out Dr Kogan's expertise and access to Facebook data (provided on a research basis) they were aware was not easily available to them on a commercial basis. They had insight (and seeming disregard) that they were commercialising data that had not been consented for that purpose and were active in directly

controlling the manner and frequency with which that data was harvested from the platform.

We have written to a number of individuals, including Dr Kogan and Alexander Nix, and invited them to attend voluntary interviews under caution, to provide us with their account of events. They have 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 active and continuing in that regard.

3.2.3 Regulatory issues for SCLE Elections Ltd (SCLE) and Cambridge Analytica (CA)

On 3 May 2018, Cambridge Analytica and SCLE as part of the SCLE Group were placed into administration. Since then the companies have ceased trading.

Had SCLE still existed in its original form, our intention would have been to issue the company with a substantial fine for very serious breaches of principle one of the DPA1998 for unfairly processing people's personal data for political purposes, including purposes connected with the 2016 US Presidential campaigns. For ease of reading we'll again refer to Cambridge Analytica throughout this section.

Even though most or all of the personal data in question related to US citizens and residents, the processing of this data took place within the UK and was performed by a UK entity.

Facebook users who accessed the app, together with friends of those Facebook users, were not made aware:

- that their personal data would be provided to CA;

- that their personal data would be used for the purposes of political campaigning;
- that their personal data would be processed in a manner that involved drawing inferences about their political opinions, preferences and their voting behaviour.

CA processed the personal data in circumstances where none of the conditions for lawful processing in Schedule 2 of the DPA1998 were satisfied. As far as consent is concerned, people had not given valid and effective consent for their personal data to be processed by CA, or for that data to be processed for the purposes of political campaigning. Additionally, the processing in question did not serve the legitimate interests of CA or any other person.

Since CA used the information collected to make predictions about data subjects' political affiliations and opinions, it is clear that the data should be considered sensitive personal data. CA processed it in circumstances where none of the conditions for lawful processing in Schedule 3 of the DPA1998 was satisfied.

The breach was serious because it affected a very large number of individuals and personal data was used for a purpose that those individuals were not aware of and would not have anticipated.

People were likely to be distressed by the fact that CA processed their personal data in the context of political profiling without their direct consent. The ongoing public reaction to the incident and the number of individuals affected provides sufficient evidence to conclude that substantial distress is likely to have been caused in this instance.

The underlying objective of issuing a monetary penalty is to achieve ongoing compliance and best practice, with the organisation being held to account for previous failings, and to act as a deterrent against other similar behaviour.

Since the companies are in administration, insolvency law imposes a moratorium on legal proceedings which would include steps toward issuing a monetary penalty. We do not however consider it to be in the public interest to pursue this course of action, since if any financial penalty against the organisation would be to the detriment of any legitimate creditors of SCLE rather than the company itself.

Our investigation also revealed other organisational shortcomings in how CA stored, secured and processed personal data.

A specific example of CA'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 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 DPA1998 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.

Given the seriousness of these issues and the public interest concerns they raise, we have pursued criminal proceedings against the company as the corporate entity responsible.

Proceedings began on 3 October 2018, when the company entered a not guilty plea, and a trial has been set for 9 January 2019 at Hendon Magistrates Court.

Additionally, we identified other shortcomings. The servers seized under warrant revealed a chaotic IT infrastructure. CA failed to ensure that the information provided to it by Dr Kogan was transferred securely between themselves and external contractors. The use of personal email accounts added to security concerns. Security breaches were identified when, as part of the execution of the warrant, Post-it notes were found on the walls of CA offices containing passwords. CA also failed to delete all the Facebook data in a timely manner, despite assurances given that it had done so.

We are also in the process of referring CA directors to the Insolvency Service. The organisation administers compulsory company liquidations and personal bankruptcies, and deals with misconduct through investigation of companies and enforcement. The service can take action to wind companies up and disqualify company directors.

3.2.4 Regulatory issues for Facebook group companies

On 25 October 2018, the Information Commissioner issued a monetary penalty notice to Facebook, imposing a fine of £500,000. The scale of the penalty reflects the seriousness of the breaches and Facebook's repeated failures to protect their user's personal information, even after the misuse of data was discovered in December 2015. The Commissioner has also

made it clear that the fine - the highest permitted by the DPA1998 - would have been significantly higher had these failings occurred after the GDPR and the DPA2018 replaced the DPA1998 in May of this year.

Our investigation found that between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information, without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' of people who had.

Facebook also failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform.

These failings meant Dr Kogan and his company GSR were able to harvest the data of up to 87 million people worldwide, without their knowledge, as described in section 3.3.1. A subset of this data was later shared with other organisations, including CA.

We found that the personal information of at least one million UK users was among the harvested data and consequently put at risk of further misuse.

We are also aware that other regulators have looked at Facebook's operations at the relevant time and in the time period just prior – for example, our US counterparts and the Irish Data Protection Commission.

We have referred our ongoing concerns about Facebook's targeting functions and techniques that are used to monitor individuals' browsing habits, interactions and behaviour across the internet and different devices to the to the IDPC. Under the GDPR, the IDPC is the lead authority for Facebook in the EU. We will work with both the Irish

regulator and other national data protection authorities to develop a long-term strategy on how we address these issues.

3.3 The relationship between Aggregate IQ (AIQ), SCLE and CA

We investigated the relationships between CA, SCLE and the Canadian-based company AIQ.

Concerns have been raised about the closeness of the two organisations including suggestions that AIQ, SCLE and CA were, in effect, one and the same entity. AIQ did some work directly for some campaigns during the EU referendum (see section 3.6) so when CA indicated that it did not work on the EU referendum, the claim seemed to be misleading.

Documents produced by CA - for example what appeared to be an internal CA telephone list and some marketing material, and the cross over in some staff at the companies - suggested that there was a permeability between the companies above and beyond what would normally be expected to be seen.

Our concern however, given our remit, was focused on whether there was any truth to allegations that UK data had been processed in Canada by AIQ outside the protections of the DPA1998.

Our investigators confirmed that in early 2014 SCLE 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, SCLE required AIQ to transfer to it the intellectual property rights and ownership of the software that AIQ developed. SCLE 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 SCLE on behalf of its clients. This work concluded in November 2014.

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

AIQ has explained in its responses to us that all work was conducted with SCLE and not the trading name company CA, and we have uncovered no evidence in the material so far recovered that personal data, including that of UK citizens, was shared with them by CA.

While there was clearly a close working relationship between the entities and several staff members were known to each other, we have no evidence that AIQ has been anything other than a separate legal entity.

We can, however, understand the broader concerns about the close collaboration between the companies which stemmed from shared contact details on company websites and details of payments. In the course of our investigation we noted the following financial transactions and contacts:

- On 24 October 2014, SCLE Elections Limited made payments to Facebook of approximately $270,000 for an AIQ ad account.
- On 4 November 2014, SCLE made a payment of $14,000 for the same AIQ ad account.
- A refund for unused AIQ ads was later made to SCLE, with the explanation that SCLE had made pre-payments for its campaigns under AIQ.

SCLE 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 SCLE employee who was also involved in a number of payments. This pattern is suggestive of a close relationship between the companies but ultimately we have concluded that this was a contractual relationship - AIQ provided adverts for SCLE. To ease the administration of this contract the payments and access arrangements above appear to have been put in place.

While this is not a common arrangement we see in our work, when it is set alongside the poor organisational practices we have seen elsewhere in the running of SCLE and without a trail of personal data being misused as a result of these practices we have concluded there is no further action for us to take on this strand, unless more evidence comes to light.

In summary, we found that the relationship between AIQ and SCLE was a contractual one; AIQ supplied services as outlined above for work on US campaigns. We found no evidence of unlawful activity in relation to the personal data of UK citizens and AIQ's work with SCLE. To date, we have no evidence that SCLE and CA were involved in any data analytics work with the EU Referendum campaigns. Our findings to date regarding UK citizens have been informed by the federal Office of the Privacy Commissioner of Canada. The Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia have an ongoing investigation into AIQ and have not yet made findings.

On 5 April 2018 the OPC and OIPCBC announced that they were jointly investigating Facebook and AIQ as to whether the organisations were in compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the BC's Personal Information Protection Act

(PIPA). That investigation is ongoing, but they have advised us that they have not located any UK personal data, other than that identified within the scope of our enforcement notice.

3.4 The relationship between Cambridge Analytica (CA) and Leave.EU

Leave.EU is an organisation that campaigned for Brexit in the June 2016 EU referendum.

We investigated the allegation that CA provided data analytics services to Leave.EU. Our focus was on the use of personal data and whether Leave.EU breached the DPA1998. We served information notices on Leave.EU and CA 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 CA 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 CA, appeared at a Leave.EU news conference in 2015. Statements by representatives of Leave.EU made in 2016 also indicated that CA had worked for them. Senior CA staff also claimed they had worked with Leave.EU.

In response to information notices served on them, both parties 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:

- On 23 October 2015, representatives of Leave.EU met with CA staff; this was a basic introductory meeting to express interest in potentially working together.
- On 18 November 2015, CA appeared at a press conference with Leave.EU.
- On 20 November 2015, CA went to Leave.EU's Bristol offices to pitch their product.
- On 8 January 2016, representatives of Leave.EU met CA in London, and CA presented a proposal for future work together.

Based on our enquiries, testimony and interviews, we conclude that this is indeed the case - there is no evidence of a working relationship between CA and Leave.EU proceeding beyond this initial phase.

During our investigation, allegations were made that CA was paid for work on UKIP membership data in 2015, and that Leave.EU paid for this work. On 11 October 2017 the ICO served an information notice on UKIP as part of this investigation. UKIP appealed this information notice - we set out the legal situation in relation to UKIP in section 3.1.1.

3.5 Relationship between Leave.EU and Eldon Insurance Ltd (Eldon), Big Data Dolphins and the University Of Mississippi (UoM) case

Eldon is an insurance management and claims management provider, specialising in private motor and commercial insurance. Its policies are provided through a number of brands, including GoSkippy Insurance.

Leave.EU and Eldon are closely linked. Both organisations share at least three directors, and there is further crossover of both employees and projects.

We investigated allegations that Eldon 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 DPA1998.

On 25 October 2017 we issued an information notice to Leave.EU. This was followed by a subsequent 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 was provided to various organisations associated with the Leave campaign, and if so how it was used.

The answers provided to the information notices then led us to further correspondence and interviews with representatives of the organisations, and other individuals.

In addition, we investigated allegations that the personal data of UK citizens was sent to the UoM by Eldon or related companies. We engaged with the company and the UoM at senior level and examined documents detailing their relationship. We found no evidence the personal data of UK citizens was transferred to the UoM.

During the course of the investigation we made a number of findings.

3.5.1 Eldon Insurance sharing personal data with Leave.EU

We have concerns about the overall management of personal data within the company particularly about the arrangements for sharing personal data handled by the company and its associated entities.

We have evidence to show that some customers' personal data, in the form of email addresses, held by Eldon was accessed by staff working for Leave.EU and was used to unlawfully send political marketing messages.

We are considering the apparent weakness of controls in Eldon allowing its customer information to be accessed by Leave.EU staff in this way on different occasions, and we are still considering the evidence in relation to a breach of principle seven of the DPA1998.

We have decided to issue a preliminary enforcement notice on the company requiring immediate action to ensure that it is compliant with data protection law. We intend to audit the company to ensure that changes have been made and that there are now effective controls to ensure customer data is secure.

3.5.2 Leave.EU sending unsolicited marketing information to Eldon Insurance (trading as GoSkippy) email subscribers

As part of its campaign work, Leave.EU built up a database of subscribers who had consented to receive email information from Leave.EU. However, during two separate campaigns, Leave.EU sent emails to their subscribers which contained other marketing information, promoting GoSkippy and its insurance products, for which they did not have consent. They were:

- 1,069,852 emails sent between 25 February and 31 July 2017, which included the GoSkippy banner and a discount offer for Leave.EU supporters.
- A single email to over 49,000 email address on 23 August 2016, announcing a 'sponsorship' deal with GoSkippy.

On 5 November 2018, the Commissioner issued two notices of intent (NOI) outlining her decision to fine Leave.EU and Eldon Insurance Services (trading as Go Skippy Insurance) for breaching Regulation 22 of PECR 2003 by sending marketing emails without specific consent.

The full factual and legal considerations are set out in the notices. Taking all of these factors into account, the Commissioner has notified her intent to impose penalties of £60,000 on each company.

The NOIs set out our areas of concern and invite their representations. Their representations are due by 5 December 2018 and we have taken no final view on the case at this time. We will consider carefully any representations both organisations may wish to make before finalising our views.

3.5.3 Leave.EU newsletter sent to Eldon customers

As part of its response to an information notice, Eldon admitted to one incident where a Leave.EU newsletter was incorrectly emailed to Eldon customers, due to an error in managing an email distribution system.

Eldon claimed that the ICO had been made aware of the error. However, we have no record of any such incident being reported to us and have asked the company for details to confirm this. We established that this incident occurred on 16 September 2015, when Leave.EU marketing staff sent an email newsletter, intended for Leave.EU subscribers, to more than 319,000 email addresses on Eldon's customer database.

On 5 November 2018, the Commissioner issued a notice of intent to fine Leave.EU for breaching Regulation 22 of PECR 2003 by sending this email newsletter.

The full factual and legal considerations are set out in the NOI (Annex ii), but a key factor is that Leave.EU did not have the consent of the subscribers for the 296,522 unsolicited direct marketing emails it sent.

The Commissioner has notified her intent to impose a penalty of £15,000. She has also issued a preliminary enforcement notice (Annex IV), requiring Leave.EU to be fully compliant with the PECR 2003 before sending emails to subscribers.

The NOI sets out our areas of concern and invites their representations. Their representations are due by 5 December 2018 and we have taken no final view on the case at this time. We will consider carefully any representations Leave.EU may wish to make before finalising our views.

3.5.4 Personal data and the University of Mississippi (UoM)

As referenced in section 3.4, Leave.EU and CA did not pursue a working relationship once Leave.EU failed to obtain designation as the official leave campaign for the 2016 referendum.

But Leave.EU did explore creating a new organisation, called Big Data Dolphins, with a view to collecting and analysing large quantities of data for political purposes. They explored this project with other organisations, including the UoM.

We investigated Big Data Dolphins, and the possibility that the personal data of UK citizens was ever transferred to the UoM. We engaged with Leave.EU, Eldon and the University itself.

We found no evidence that Big Data Dolphins ever actually functioned, and no evidence that Leave.EU, Eldon or any associated companies had transferred any personal data relating to UK citizens to the UoM.

3.6 The relationship between AggregateIQ (AIQ), Vote Leave and other Leave campaigns

In response to an information notice, Facebook confirmed 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 in June 2016, AIQ ran 218 ads solely on behalf of Vote Leave and directed at email addresses on

Facebook. In response to our information notice, Facebook stated that the email addresses did not originate from data collected through Dr Kogan's app but came from a different source (as an analysis of the accounts affected by the GSR app did not return a greater than random chance match to the target audience).

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 proceed to run ads using that data set. The Electoral Commission report dated 17 July 2018 confirms that BeLeave did not submit an electoral return.

Vote Leave ran 1,034 ads between 19 April 2016 and 20 June 2016.

Payment for all of these Facebook ads was made by AIQ, and amounted to approximately $2 million (£1.5 million) between 15 April 2016 and 23 June 2016. Our regulatory concern was whether, and on what basis, the two groups shared the personal data of UK voters between themselves and others in order to target these ads.

The Electoral Commission has separately investigated allegations of coordination between Vote Leave and BeLeave and whether there was a breach of the electoral rules. We have shared relevant evidence with the Electoral Commission where appropriate under our legal gateway. The Electoral Commission has referred individuals to the police for investigation; those individuals have therefore declined to speak to our enquiry at this time. We will revisit this strand of the investigation for any data protection issues at the conclusion of the police enquiries.

3.6.1 The use of UK personal data

We established that AIQ had access to the personal data of UK voters provided by the Vote Leave campaign. We investigated where it accessed that personal data, and whether AIQ continued to hold personal data made available to it by Vote Leave.

During our investigation, AIQ confirmed it had identified a total of 1,439 email addresses, from which a total of 397 email addresses and names related to the UK. These email addresses had been made publicly accessible via GitLab by AIQ. This information was also found to have been backed up to AIQ's server on 20 March 2017 and 27 April 2017.

In response to our investigation, AIQ stated that it used the Git repository as a form of version control for its work, allowing it to create back-ups of code during development. Its response when asked about the 1,439 email addresses was that the emails were stored as part of a back-up process and were then not deleted, contrary to its usual procedure.

On 6 July 2018, we issued an enforcement notice to AIQ, ordering the company to cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes.

AIQ appealed our enforcement notice to the First Tier Tribunal, asking for more specific details. After receiving its points of appeal, we decided to vary the original enforcement notice to clarify the steps AIQ should take. We have the legal power to vary the enforcement notice under section 153 of the DPA2018.

The enforcement notice was reissued on 24 October 2018 with specific instructions for AIQ. The company has accepted the revised notice and the Tribunal has allowed it to withdraw its appeal.

Our further investigations into AIQ revealed no evidence of the unlawful processing of UK personal data.

3.6.2 Jurisdictional challenges

The investigation into the activities of AIQ presented a number of jurisdictional challenges. In its letter dated 5 March 2018, in response to a number of our enquiries, AIQ stated that it was 'not subject to the jurisdiction of the ICO' and ended with a statement that it considered its 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 it had previously not answered our questions fully - or at all. Since April 2018, AIQ agreed to co-operate with our investigation in full.

AIQ had in its possession and control, personal data of individuals in the UK as a result of work it did on behalf of a UK client.

The GDPR and DPA2018 both have extra-territorial scope by virtue of article 3 of the GDPR and section 207 of the DPA2018.

3.7 Vote Leave

We investigated whether and how Vote Leave transferred the personal data of UK citizens outside the UK and whether this was breach of the

DPA1998, and whether that personal data was also unfairly and unlawfully processed.

We served information notices on Vote Leave on 13 September 2017 and 20 December 2017, in order to obtain evidence about how it obtained and used personal data, and the organisations with whom they shared information. We served further information notices to Vote Leave in 2018, in response to additional information we uncovered during our investigation.

We know that Vote Leave had a commercial relationship with AIQ. In respect of that work, we have not obtained any evidence that Vote Leave transferred or processed personal data outside the UK unlawfully - or that it processed personal data without the consent of data subjects.

However, we are investigating how Vote Leave delivered electronic marketing communications and whether its actions contravened PECR. We do have cause for concern and we will be reporting on this imminently.

3.8 BeLeave and Veterans for Britain

We investigated both of these organisations and how they obtained and processed personal data. AIQ undertook some work for both organisations.

In relation to the work AIQ created for BeLeave — this occurred towards the end of the EU referendum campaign. We know that AIQ was asked to provide some online advertising on BeLeave's behalf. This included placing ads on platforms and landing pages. AIQ provided input in terms of the content, and whether the advertisement would 'work'. In respect of this work, AIQ reported to BeLeave on the number of times an ad was

shown, how many people clicked on it and so on. Any data provided on the website forms was sent directly to BeLeave; AIQ confirmed it had no access to this information. We found no evidence that BeLeave unlawfully processed this personal data.

In respect of Veterans for Britain, AIQ created and placed ads at the campaign's direction and reported on them. We have found no evidence that personal data was misused by either organisation in respect of this work.

3.9 The Remain campaign

We investigated 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 specifically looked at possibly inadequate third party consent and the fair processing statements used to collect personal data, which were similar to the issues we explored on the Leave campaigns and the wider political parties area of our investigation.

During the course of our investigation, we obtained information that the Liberal Democrats had sold the personal data of its party members to BSiE for approximately £100,000.

In June and July 2018, we served information notices on Open Britain, the successor organisation to BSiE, and the Liberal Democrats, under the DPA1998, to investigate these issues.

In response to our information notices, the Liberal Democrats stated that they had worked with a third party group which took subsets of the electoral register – which the party was entitled to access – and carried

out a simple enhancement service, for example, adding phone numbers where available.

The party had further worked with BSiE to model electoral roll data, with a view to highlighting potential voting intentions.

Both the Liberal Democrats and Open Britain denied that party members' personal data had been sold. Instead, both confirmed that the In Campaign bought Electoral Register information from the Liberal Democrats.

We are still looking at how the Remain side of the referendum campaign handled personal data, including the electoral roll, and will be considering whether there are any breaches of data protection or electoral law requiring further action.

3.10 The university sector, Cambridge University and the Cambridge University Psychometric Centre

Whilst the media and public focus on our investigation 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 have their origins in the work of academics at the 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

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

academia and research and development (R&D) departments with cutting-edge tools tailored for the online environment.

As our investigation developed, with examination of Dr Kogan's actions and his use of Cambridge University credentials to lend support to his actions, we engaged with the university at senior level.

This engagement and other work in the UK and abroad, has identified some common and potentially serious data protection concerns that we suspect are widespread across the university sector.

The University has fully co-operated with our enquiries to establish to what extent the Psychometrics Centre, and individuals employed by them pursuing their own private enterprises, may better comply with data protection law. We had access to university staff, academics and premises to carry out our work. Questions remain about the sufficiency of boundaries between academic studies and the commercial enterprises many academics legitimately establish, as well as the use of university equipment. 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.

3.10.1 Audit of the Psychometric Centre

As a starting point we have conducted an audit of Cambridge University's Psychometric Centre, including the university's information governance arrangements, assessing their compliance with the GDPR and the DPA2018. No enforcement action has been considered for Cambridge University because we determined that it is not a relevant data controller within the context of the investigation.

However, we have made 42 recommendations following our audit and have raised the following significant concerns:

- The university's current data security policy is in need of updating; the new Chief Information Security Officer is in the process of developing a new information security policy framework to replace and expand upon it. Further work is needed to ensure that the new framework is fit for purpose. Once it is finalised, work will be needed to ensure that it is suitably embedded and put into practice across the university. An outdated data security policy can be a risk to the secure handling of personal data.
- The university has recently appointed an external third party to operate as its Data Protection Officer. As this is a new arrangement, work will be needed to ensure that reporting lines and oversight arrangements are in place to allow the new structure to work effectively in practice and ensure that it is fit for purpose.
- The university has recently developed an Information Asset Register. However, this is focused on operational data and a conscious decision was initially made not to include research data on this register. The register should be updated to include research, particularly if the register is intended to act as the university's record of processing activities under Article 30 of the GDPR.
- There is no over-arching Access Control Policy in place. There was evidence of a variety of approaches to access permissions across the university. It would be beneficial for an Access Control Policy to be implemented to set out expected standards and for monitoring of compliance with the policy to take place. There are problems understanding who has had access to any personal data used as part of its projects. The centre needs to create an over-arching Access Control Policy, to replace the current variance in approaches across the University;

- There is currently a lack of oversight in relation to the management of IT equipment and hardware assets and, particularly, the use of non-university equipment by students and researchers. A new process should be developed to provide this oversight and assurance for the university.

The audit covered governance and accountability, information security, records management, information risk management and training and awareness.

We considered whether the university more broadly had sufficient systems and processes in place to ensure that data collected by academics for research was appropriately safeguarded in its use and not re-used for commercial work.

In respect of the Psychometric Centre, Facebook indicated that it suspended numerous applications linked to academics there.

During the course of our investigation a breach in relation Dr Stillwell's 'MyPersonality' app, one of those suspended by Facebook, was also reported to us.

The ICO's investigation into access to personal data via the MyPersonality application is ongoing. The data contained within the MyPersonality app database was reported to have been anonymised. However, we are currently finalising our understanding of the anonymisation techniques used on the dataset in order to ensure that appropriate measures were taken to prevent de-anonymisation. It is vital that we evaluate the likelihood of a full de-anonymisation of the dataset in order to come to a conclusion about the potential detriment to those potentially affected.

3.10.2 Improvements to Higher Education practices

What is clear is a serious overhaul of data protection practices is needed in how higher education institutions handle data in the context of academic research and, while 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 the correct processes and due diligence arrangements to minimise the risk to data subjects and to the integrity of academic research practices.

We have recommended that Universities UK works with the ICO to consider the risks arising from the 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. Through this group we will provide guidance on how the sector can best comply with the requirements of data protection law.

3.11 Data brokers

We looked closely at the role of those who buy and sell personal data sets in the UK and who were linked to the political campaigns. 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 investigation.

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, but had failed to obtain lawful consent for political parties to use those lists in this way. For example, the brokers had not explained who the data would be sold to or how it would be used when it was gathered.

We 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, GB Group and Data8.

We raised 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 DPA 1998.

3.10.3 Emma's Diary (Lifecycle Marketing (Mother and Baby Ltd)

Our investigation revealed that this company had illegally collected and sold personal information belonging to more than one million people.

The company, which provides advice on pregnancy and childcare, sold the information to Experian Marketing Services, a branch of the credit reference agency, specifically for use by the Labour Party. Experian then created a database which the party used to profile new mothers in the run-up to the 2017 General Election.

We found that the company failed to disclose that the personal information provided would be used for political marketing or by political parties, which contravened the first principle of the DPA1998.

The Information Commissioner fined the company £140,000 for this breach. The full facts of the breach are set out in our Monetary Penalty Notice dated 9 August 2018.

3.10.4 CACI, GB Group and Data8

Our investigations revealed no evidence that these companies had breached DPA1998 or PECR 2003 when processing personal data in the political campaigning work they were directly or indirectly involved in. However, we have sought to obtain additional information about the practices of several other data brokers. We've issued assessment notices to GB Group PLC, Acxiom Ltd and Data Locator Group Ltd in order for us to be able to carry out audits.

3.10.5 Credit reference agencies (CRAs)

We have also been looking at the services and operations of the three main credit reference agencies - Experian, Equifax and Callcredit - in respect of the services they promote to political parties and campaigns.

We have an existing project, separate to our data analytics investigation, in which we are examining the privacy issues raised by their work. This project has been expanded to include their activities in political processes. Our teams have issued assessment notices to the three main CRAs and are currently in the process of auditing the agencies. We expect to report on our findings by the end of this year.

4. Summary of regulatory action

In the course of our investigation we carried out the following regulatory action:

4.1 Notices of Intent and Monetary Penalties

- Monetary penalty of £500,000 imposed on Facebook for serious breaches of the first and seventh Principles of the DPA1998.
- Monetary penalty of £140,000 imposed on Emma's Diary for serious contravention of the first principle of the DPA 1998.
- Notice of intent to fine Eldon Insurance (trading as Go Skippy) £60,000 for serious contraventions of regulation 22 of PECR 2003 (annex iii)
- Notice of intent to fine Leave.EU £60,000 for serious contraventions of regulation 22 of PECR 2003 (annex i)
- Notice of intent to fine Leave.EU £15,000 for serious contraventions of regulation 22 of PECR 2003 (annex ii)

4.2 Enforcement Notices

- Enforcement notice requiring SCLE Elections to comply with the terms of the Subject Access Request submitted by Professor Carroll (as a US-based academic) under the DPA 1998.
- Enforcement notice requiring AiQ to stop processing retained UK citizen data.
- Preliminary enforcement notice requiring Eldon Insurance Ltd to only instigate email marketing that is fully compliant with PECR 2003, ensuring that due diligence is applied and they have full evidence of consent (annex IV).

4.3 Criminal prosecutions

Criminal proceedings against SCLE Elections Ltd for failing to properly deal with the enforcement notice dated 4 May 2018.

4.4 Regulatory actions

- 11 warning letters requiring action by the main political parties backed by Assessment Notices for audits in 2019.
- Audits of Cambridge University and its Psychometric centre.
- Assessment notices for Experian, Equifax and Call Credit leading to audits.
- Assessment notices for data brokers Acxiom Ltd, Data Locator Group Ltd and GB Group PLC leading to audits.
- Referral of CA to the Insolvency Service
- Referral of individuals to law enforcement for other offences evidenced but not linked to these matters.

5. Next steps

A number of the issues set out in this report are still ongoing, or require further investigation or action, but this will be our final update on the investigation as a whole. Any enforcement action required in the future will be announced and absorbed as part of our general regulatory action.

Some strands of the investigation will continue as stand-alone enforcement action, such as finalising our notices of intent and pursuing criminal actions.

In relation to CA, we continue to work through the exact detail as to when the harvested Facebook data and its derivatives were deleted and we are reviewing other information seized as part of the warrants.

Other issues raised have been merged into other existing operations, such as the ongoing audits of the credit reference agencies, and any enforcement that arises from these operations will highlight where our data analytics investigation has contributed.

And some actions will themselves form the basis for new operations and activities, such as pursuing the recommendations made in “Democracy Disrupted? Personal information and political influence” - including formulating our statutory code and working with the Higher Education sector to make improvements to its handling of personal information obtained during research.

Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

NOTICE OF INTENT

To: Leave.EU Group Limited

Of: Lysander House, Catbrain Lane, Cribbs Causeway, Bristol BS10 7TQ

1. The Information Commissioner ("Commissioner") is minded to issue Leave.EU Group Limited ("Leave.EU") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is in relation to a serious contravention of Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

2. This notice explains the Commissioner's decision.

Legal framework

3. Leave.EU, whose registered office is given above (Company House Reference: 09763501), is the organisation stated in this notice to have transmitted unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing contrary to regulation 22 of PECR.

4. Regulation 22 of PECR states:

"(1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

(4) A subscriber shall not permit his line to be used in contravention of paragraph (2)."

5. Section 11(3) of the DPA defines "direct marketing" as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". This definition also applies for the purposes of PECR (see regulation 2(2)).

6. "Individual" is defined in regulation 2(1) of PECR as "a living individual and includes an unincorporated body of such individuals".

7. "Electronic mail' is defined in regulation 2(1) of PECR as "any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

8. The term "soft opt-in" is used to describe the rule set out in Regulation 22(3) of PECR. In essence, an organisation may be able to e-mail its existing customers even if they haven't specifically consented to electronic mail. The soft opt-in rule can only be relied upon by the organisation that collected the contact details.

9. A "subscriber" is defined in regulation 2(1) of PECR as "a person who is a party to a contract with a provider of public electronic communications services for the supply of such services".

10. Section 55A of the DPA (as amended by the Privacy and Electronic Communications (EC Directive)(Amendment) Regulations 2011 and the Privacy and Electronic Communications (Amendment) Regulations 2015) states:

"(1) The Commissioner may serve a person with a monetary penalty if the Commissioner is satisfied that –

(a) there has been a serious contravention of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 by the person,

(b) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the person –

(a) knew or ought to have known that there was a risk that the contravention would occur, but

(b) failed to take reasonable steps to prevent the contravention."

11. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

12. PECR implements European legislation (Directive 2002/58/EC) aimed at the protection of the individual's fundamental right to privacy in the electronic communications sector. PECR was amended for the purpose of giving effect to Directive 2009/136/EC which amended and strengthened the 2002 provisions. The Commissioner approaches PECR so as to give effect to the Directives.

13. The provisions of the DPA remain in force for the purposes of PECR notwithstanding the introduction of the Data Protection Act 2018 (see paragraph 58(1) of Part 9, Schedule 20 of that Act).

Background to the case

14. Leave.EU came to the attention of the Commissioner during investigations in relation to the wider use of personal data and analytics by political campaigns, social media and insurance companies. In particular Leave.EU has been investigated about its relationship with Eldon Insurance/GoSkippy Insurance and their use of personal data. It is noted that there is a significant cross-over of employees and senior figures between the organisations named above.

15. The Commissioner's investigations led to an Information Notice being served on Leave.EU on 27 July 2018, primarily requesting details in relation to a promotional banner advertising the services of GoSkippy Insurance ("GoSkippy") which the Commissioner had discovered had been included within newsletters sent via email by Leave.EU to Leave.EU subscribers.

16. Leave.EU responded to the Information Notice on 23 August 2018 providing the following information:

- Between 25 February 2017 and 31 July 2017, 1,020,661 such emails were received by Leave.EU subscribers.

- The majority of these emails were weekly round-up newsletters and all of them contained a banner showing the GoSkippy logo and offered '10% off' for Leave.EU supporters. If the banner is clicked the GoSkippy website is accessed.

- In addition, on 23 August 2016, 49,191 emails were sent to subscribers titled "Skippy Saves the Day". Again, the content of these messages offered a 10% discount on all GoSkippy insurance products.

17. This response confirmed therefore that a total of 1,069,852 messages were sent by Leave.EU and received by subscribers over two separate periods, each containing marketing material promoting the services of GoSkippy.

18. When queried as to the consent held by Leave.EU for the sending of these messages, Leave.EU responded to say that they believed the emails were not unsolicited since subscribers, as part of their registration process, provided consent to receive Leave.EU newsletters, and the privacy policy that Leave.EU provided made reference to subscribers receiving 'information about other organisations' products and services'.

19. A review of the cited Privacy Policy was conducted by the Commissioner. The Policy advises that the subscribers' data may be used by Leave.EU or 'third parties' to provide information about goods or services which may be of interest, it does not however appear to specifically name GoSkippy, or indeed any of the third parties at all. Furthermore, it does not make clear the types of marketing which subscribers could expect to receive.

20. It was confirmed that there is no formal contract in place between Leave.EU and GoSkippy to provide direct marketing.

21. The Commissioner has made the above findings of fact on the balance of probabilities.

22. The Commissioner has considered whether those facts constitute a contravention of regulation 22 of PECR by Leave.EU and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

23. The Commissioner finds that Leave.EU has contravened regulation 22 of PECR.

24. The Commissioner finds that the contravention was as follows:

25. On 23 August 2016, and between the dates of 25 February 2017 and 31 July 2017, Leave.EU transmitted 1,069,852 direct marketing emails to subscribers containing a banner advertising the services of GoSkippy.

26. Section 11(3) DPA definition of direct marketing covers any advertising or marketing material, and applies to messages which contain even some marketing elements, even if that is not their main purpose.

27. There is no evidence to suggest that Leave.EU held the requisite consent of subscribers to send direct marketing relating to GoSkippy.

28. The Commissioner is of the view that these messages therefore constitute unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing contrary to regulation 22 of PECR.

29. "Consent" within the meaning of regulation 22(2) requires that the recipient of the electronic mail has notified the sender that he consents to messages being sent by, or at the instigation of, that sender. Indirect, or third party, consent can be valid but only if it is clear and specific enough.

30. As the sender of the direct marketing emails, it was the responsibility of Leave.EU to ensure that it held appropriate consent to send those

messages, and that this consent applied to marketing material advertising GoSkippy.

31. Regulation 22(3) provides for a 'soft opt-in' exception to enable organisations to send marketing emails to existing customers however the Commissioner's Direct Marketing Guidance at paragraph 131 states that to rely on this exception the organisation must have obtained the contact details in the course of a sale of a product or service to that person; must only be marketing their own similar products and services; and must have given the person a simple opportunity to refuse/opt-out of the marketing.

32. As Leave.EU were advertising the services of GoSkippy, and not 'their own similar products or services', they cannot rely on the "soft opt-in" exception.

33. The Privacy Policy relied on by Leave.EU does not specifically name GoSkippy, rather it referred only to third parties.

34. Consent will not be "informed" if individuals do not understand what they are consenting to. Organisations should therefore always ensure that the language used is clear, easy to understand, and not hidden away in a privacy policy or small print. Consent will not be valid if individuals are asked to agree to receive marketing from "similar organisations", "partners", "selected third parties" or other similar generic description.

35. The Commissioner's direct marketing guidance says "organisations need to be aware that indirect consent will not be enough for texts, emails or automated calls. This is because the rules on electronic marketing are stricter, to reflect the more intrusive nature of electronic messages."

36. It goes on to say that indirect consent can be valid but only if it is clear and specific enough. Moreover, "the customer must have anticipated that their details would be passed to the organisation in question, and that they were consenting to messages from that organisation. This will depend on what exactly they were told when consent was obtained".

37. It was apparent to the Commissioner that the wording of the Privacy Policy relied upon by Leave.EU was not sufficiently clear and precise so as to give the subscriber a reasonable expectation that they would receive direct marketing advertising the services of GoSkippy.

38. The Commissioner is therefore satisfied that Leave.EU did not have the necessary valid consent for the 1,069,852 direct marketing emails which were sent to subscribers.

39. The Commissioner is satisfied that Leave.EU was responsible for this contravention and has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

40. The Commissioner is satisfied that the contravention identified above was serious. This is because on 23 August 2016 and between the dates of 25 February 2017 and 31 July 2017, a total of 1,069,852 direct marketing emails were sent by Leave.EU and received by subscribers advertising marketing material for which they had not provided consent.

41. The Commissioner is therefore satisfied that condition (a) from section 55A(1) DPA is met.

Deliberate or negligent contraventions

42. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that Leave.EU's actions which constituted that contravention were deliberate actions (even if Leave.EU did not actually intend thereby to contravene PECR).

43. The Commissioner considers that in this case Leave.EU did not deliberately contravene regulation 22 of PECR.

44. The Commissioner has therefore gone on to consider whether the contraventions identified above were negligent. First, she has considered whether Leave.EU knew or ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is met, given that the issue of unsolicited emails have been widely publicised by the media as being a problem. Furthermore, it would be reasonable to expect an organisation who is registered with the ICO to be aware of their obligations under PECR and to carry out steps to ensure compliance when engaging in direct marketing advertising a third party.

45. Second, the Commissioner considered whether Leave.EU failed to take reasonable steps to prevent the contraventions. The Commissioner has published detailed guidance for those carrying out direct marketing explaining their legal obligations under PECR. This guidance gives clear advice regarding the requirements of consent for direct marketing and explains the circumstances under which organisations are able to carry out marketing over the phone, by text, by email, by post, or by fax. In particular it states that organisations can generally only send marketing emails to individuals if that person has specifically consented

to receiving them from the sender. It also makes it clear that particular care must be taken when promoting the aims, ideals, or services of third party organisations to ensure that the consent being relied upon is appropriate.

46. Reasonable steps could have included listing third parties by name within the Privacy Policy, and providing subscribers with clear opt-in/out boxes to allow them to make an informed choice as to whether they would wish to receive marketing material relating to those organisations, and the methods by which that marketing would be received. It is not sufficient that Leave.EU and GoSkippy share directors since this would not be immediately apparent to the subscriber, nor could it be reasonably expected by the subscriber that they would receive marketing relating to insurance products as part of a political party newsletter.

47. In the circumstances, the Commissioner is satisfied that Leave.EU failed to take reasonable steps to prevent the contraventions.

48. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

The amount of the penalty the Commissioner proposes to impose

49. The Commissioner has taken the following **mitigating factor** into account:

- The Commissioner has received no complaints about the contravention.

50. The Commissioner has attempted to consider the likely impact of a monetary penalty on Leave.EU, however, in order that the Commissioner can form a complete financial picture she requires that Leave.EU provides details of its current accounts.

51. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with PECR. The sending of unsolicited marketing emails is a matter of significant public concern. A monetary penalty in this case should act as a general encouragement towards compliance with the law, or at least as a deterrent against non-compliance, on the part of all persons running businesses currently engaging in these practices. The issuing of a monetary penalty will reinforce the need for businesses to ensure that they are only messaging those who specifically consent to receive marketing.

52. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£60,000 (sixty thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Conclusion

53. The Commissioner intends to make her final decision as to whether to serve a monetary penalty notice for such amount on or after **5 December 2018**. If you wish to make any representations as to why the Commissioner should not serve a monetary penalty notice you must do so before that date. A sheet explaining the procedure for making representations is attached to this Notice of Intent as Annex 1.

Dated the 5th day of November 2018

Signed [redacted]

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

DATA PROTECTION ACT 1998

REPRESENTATIONS IN RESPONSE TO A NOTICE OF INTENT

The Commissioner has power under sections 55A and 55B of the Data Protection Act 1998 to serve a monetary penalty notice on a Data Controller. Before she exercises this power the Commissioner wishes to take account of all the relevant facts and arguments.

This Notice of Intent is to enable the Data Controller affected to put forward their side of the case. The Commissioner's intentions are set out in the accompanying Notice of Intent. If you wish to make representations on those matters you have an opportunity to do so. The closing date for this is in the accompanying Notice of Intent.

Representations should be made in writing. You may wish to comment on the facts and views set out by the Commissioner or to make general remarks on the case and enclose documents or other material. You should also inform the Commissioner if any confidential or commercially sensitive information should be redacted from a monetary penalty notice.

All representations will be carefully considered by the Commissioner before a final decision is made.

Representations should be sent by post to Mr Zachary Whiting, Chartered Legal Executive, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by email to zachary.whiting@ico.org.uk.

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

NOTICE OF INTENT

To: Leave.EU Group Limited

Of: Lysander House, Catbrain Lane, Cribbs Causeway, Bristol BS10 7TQ

1. The Information Commissioner ("Commissioner") is minded to issue Leave.EU Group Limited ("Leave.EU") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is in relation to a serious contravention of Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

2. This notice explains the Commissioner's decision.

Legal framework

3. Leave.EU, whose registered office is given above (Company House Reference: 09763501), is the organisation stated in this notice to have transmitted unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing contrary to regulation 22 of PECR.

4. Regulation 22 of PECR states:

"(1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

(4) A subscriber shall not permit his line to be used in contravention of paragraph (2)."

5. Section 11(3) of the DPA defines "direct marketing" as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". This definition also applies for the purposes of PECR (see regulation 2(2)).

6. "Individual" is defined in regulation 2(1) of PECR as "a living individual and includes an unincorporated body of such individuals".

7. "Electronic mail' is defined in regulation 2(1) of PECR as "any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

8. The term "soft opt-in" is used to describe the rule set out in Regulation 22(3) of PECR. In essence, an organisation may be able to e-mail its existing customers even if they haven't specifically consented to electronic mail. The soft opt-in rule can only be relied upon by the organisation that collected the contact details.

9. A "subscriber" is defined in regulation 2(1) of PECR as "a person who is a party to a contract with a provider of public electronic communications services for the supply of such services".

10. Section 55A of the DPA (as amended by the Privacy and Electronic Communications (EC Directive)(Amendment) Regulations 2011 and the Privacy and Electronic Communications (Amendment) Regulations 2015) states:

"(1) The Commissioner may serve a person with a monetary penalty if the Commissioner is satisfied that –

(a) there has been a serious contravention of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 by the person,

(b) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the person –

(a) knew or ought to have known that there was a risk that the contravention would occur, but

(b) failed to take reasonable steps to prevent the contravention."

11. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

12. PECR implements European legislation (Directive 2002/58/EC) aimed at the protection of the individual's fundamental right to privacy in the electronic communications sector. PECR was amended for the purpose of giving effect to Directive 2009/136/EC which amended and strengthened the 2002 provisions. The Commissioner approaches PECR so as to give effect to the Directives.

13. The provisions of the DPA remain in force for the purposes of PECR notwithstanding the introduction of the Data Protection Act 2018 (see paragraph 58(1) of Part 9, Schedule 20 of that Act).

Background to the case

14. Leave.EU came to the attention of the Commissioner during investigations in relation to the wider use of personal data and analytics by political campaigns, social media and insurance companies. In particular Leave.EU has been investigated about its relationship with Eldon Insurance/GoSkippy Insurance and their use of personal data. It is noted that there is a significant cross-over of employees and senior figures between the organisations named above.

15. During the course of her wider investigations, on 20 April 2018, the Commissioner was informed by Eldon Insurance ("Eldon") [which shares directors with Leave.EU], that an incident had taken place whereby a Leave.EU newsletter was incorrectly emailed to some Eldon customers, apparently due to an error in the way the email distribution system was used. It was advised that Eldon data was not combined or shared with Leave.EU.

16. It was indicated that this incident had been referred to the Commissioner at the time, however the Commissioner has been unable to locate any such log.

17. Further investigations revealed the following:

- The Leave.EU newsletter was sent to Eldon customers on 16 September 2015 as a result of administrative error by Leave.EU staff.

- That this was an isolated incident which resulted in one complaint and was resolved quickly.

- Leave.EU sent the Newsletter and Leave.EU instigated the sending of it.

- 319,645 emails were sent in total to an Eldon dataset. 296,522 of those emails were successfully delivered and 61,396 of those emails were opened.

- There were no similar incidents (i.e. where referendum information was sent to insurance customers in error).

- Mailchimp (an account/application which appears to house distribution lists) was used to distribute marketing communications by email to GoSkippy customers. The same account was used by marketing staff acting on behalf of Leave.EU/BFTC. The member of marketing staff selected the incorrect data file (i.e. the Eldon data file) to be used to distribute a Leave.EU newsletter.

- Eldon's insurance database is held on an IT system called OpenGI and generally is kept completely separate from the database held by Leave.EU.

- At the time of the incident one Mailchimp account was being used but another account was introduced in November 2016.

18. The Commissioner has made the above findings of fact on the balance of probabilities.

19. The Commissioner has considered whether those facts constitute a contravention of regulation 22 of PECR by Leave.EU and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

20. The Commissioner finds that Leave.EU has contravened regulation 22 of PECR.

21. The Commissioner finds that the contravention was as follows:

22. On 16 September 2015, Leave.EU used a public electronic telecommunications service for the purposes of instigating the transmission of 296,522 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing contrary to regulation 22 of PECR.

23. "Consent" within the meaning of regulation 22(2) requires that the recipient of the electronic mail has notified the sender that he consents to messages being sent by, or at the instigation of, that sender. Indirect, or third party, consent can be valid but only if it is clear and specific enough.

24. In this case the Commissioner is satisfied that Leave.EU did not have the consent, within the meaning of regulation 22(2), of the subscribers for the 296,522 unsolicited direct marketing emails it sent. The Commissioner is satisfied that the 'soft opt-in' exception afforded under regulation 22(3) would not apply in this instance since Leave.EU has no apparent prior relationship with the subscribers.

25. The Commissioner is satisfied that Leave.EU was responsible for this contravention.

26. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

27. The Commissioner is satisfied that the contravention identified above was serious. This is because on one day, 16 September 2015, a total of 296,522 direct marketing emails were successfully delivered by Leave.EU and received by subscribers for whom they did not hold valid consent.

28. The Commissioner is therefore satisfied that condition (a) from section 55A(1) DPA is met.

Deliberate or negligent contraventions

29. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that Leave.EU's actions which constituted that contravention were deliberate actions (even if Leave.EU did not actually intend thereby to contravene PECR).

30. The Commissioner considers that in this case Leave.EU did not deliberately contravene regulation 22 of PECR.

31. The Commissioner has therefore gone on to consider whether the contraventions identified above were negligent. First, she has considered whether Leave.EU knew or ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is met, given that the issue of unsolicited emails have been widely publicised by the media as being a problem. Furthermore, it would be reasonable to expect an organisation engaging in the sending of material constituting direct marketing to be aware that sharing a single Mailchimp account, housing multiple

distribution lists, might at the very least result in a risk that a contravention could occur.

32. In the circumstances the Commissioner is satisfied that Leave.EU ought reasonably to have known that there was a risk a contravention would occur.

33. Second, the Commissioner considered whether Leave.EU failed to take reasonable steps to prevent the contravention. The Commissioner has published detailed guidance for those carrying out direct marketing explaining their legal obligations under PECR. This guidance gives clear advice regarding the requirements of consent for direct marketing and explains the circumstances under which organisations are able to carry out marketing over the phone, by text, by email, by post, or by fax. In particular it states that organisations can generally only send marketing emails to individuals if that person has specifically consented to receiving them from the sender. The Commissioner accepts that this contravention appears to have arisen as a result of a single administrative error, but is of the view that reasonable steps taken could have prevented the cross contamination of distribution lists.

34. Reasonable steps could have included using separate Mailchimp accounts to house separate data sets – a step which it is understood has since been taken.

35. In the circumstances, the Commissioner is satisfied that Leave.EU failed to take reasonable steps to prevent the contraventions.

36. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

The amount of the penalty the Commissioner proposes to impose

37. The Commissioner has attempted to consider the likely impact of a monetary penalty on Leave.EU, however, in order that the Commissioner can form a complete financial picture she requires that Leave.EU provides details of its current accounts.

38. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with PECR. The sending of unsolicited marketing emails is a matter of significant public concern. A monetary penalty in this case should act as a general encouragement towards compliance with the law, or at least as a deterrent against non-compliance, on the part of all persons running businesses currently engaging in these practices. The issuing of a monetary penalty will reinforce the need for businesses to ensure that they are only messaging those who specifically consent to receive marketing.

39. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£15,000 (fifteen thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Conclusion

40. The Commissioner intends to make her final decision as to whether to serve a monetary penalty notice for such amount on or after **5 December 2018**. If you wish to make any representations as to why the Commissioner should not serve a monetary penalty notice you must do so before that date. A sheet explaining the procedure for making representations is attached to this Notice of Intent as Annex 1.

Dated the 5th day of November 2018

Signed [redacted]

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

DATA PROTECTION ACT 1998

REPRESENTATIONS IN RESPONSE TO A NOTICE OF INTENT

The Commissioner has power under sections 55A and 55B of the Data Protection Act 1998 to serve a monetary penalty notice on a Data Controller. Before she exercises this power the Commissioner wishes to take account of all the relevant facts and arguments.

This Notice of Intent is to enable the Data Controller affected to put forward their side of the case. The Commissioner's intentions are set out in the accompanying Notice of Intent. If you wish to make representations on those matters you have an opportunity to do so. The closing date for this is in the accompanying Notice of Intent.

Representations should be made in writing. You may wish to comment on the facts and views set out by the Commissioner or to make general remarks on the case and enclose documents or other material. You should also inform the Commissioner if any confidential or commercially sensitive information should be redacted from a monetary penalty notice.

All representations will be carefully considered by the Commissioner before a final decision is made.

Representations should be sent by post to Mr Zachary Whiting, Chartered Legal Executive, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by email to zachary.whiting@ico.org.uk.

Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

NOTICE OF INTENT

To: Eldon Insurance Services Limited (trading as GoSkippy Insurance)

Of: Lysander House (2nd floor), Catbrain Lane, Cribbs Causeway, Bristol BS10 7TQ

1. The Information Commissioner ("Commissioner") is minded to issue Eldon Insurance Services Limited [T/A GoSkippy Insurance] (referred to hereafter as "GoSkippy" for the purposes of this notice) with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is in relation to a serious contravention of Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

2. This notice explains the Commissioner's decision.

Legal framework

3. GoSkippy, whose registered office is given above (Company House Reference: 06334001), is the organisation stated in this notice to have instigated the transmission of unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing contrary to regulation 22 of PECR.

4. Regulation 22 of PECR states:

"(1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

(4) A subscriber shall not permit his line to be used in contravention of paragraph (2)."

5. Section 11(3) of the DPA defines "direct marketing" as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". This definition also applies for the purposes of PECR (see regulation 2(2)).

6. "Individual" is defined in regulation 2(1) of PECR as "a living individual and includes an unincorporated body of such individuals".

7. "Electronic mail' is defined in regulation 2(1) of PECR as "any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

8. A "subscriber" is defined in regulation 2(1) of PECR as "a person who is a party to a contract with a provider of public electronic communications services for the supply of such services".

9. Section 55A of the DPA (as amended by the Privacy and Electronic Communications (EC Directive)(Amendment) Regulations 2011 and the Privacy and Electronic Communications (Amendment) Regulations 2015) states:

"(1) The Commissioner may serve a person with a monetary penalty if the Commissioner is satisfied that –

(a) there has been a serious contravention of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 by the person,

(b) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the person –

(a) knew or ought to have known that there was a risk that the contravention would occur, but

(b) failed to take reasonable steps to prevent the contravention."

10. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

11. PECR implements European legislation (Directive 2002/58/EC) aimed at the protection of the individual's fundamental right to privacy in the electronic communications sector. PECR was amended for the purpose of giving effect to Directive 2009/136/EC which amended and strengthened the 2002 provisions. The Commissioner approaches PECR so as to give effect to the Directives.

12. The provisions of the DPA remain in force for the purposes of PECR notwithstanding the introduction of the Data Protection Act 2018 (see paragraph 58(1) of Part 9, Schedule 20 of that Act).

Background to the case

13. GoSkippy came to the attention of the Commissioner during investigations in relation to the wider use of personal data and analytics by political campaigns, social media and insurance

companies. In particular GoSkippy has been investigated about its relationship with Leave.EU and their use of personal data. It is noted that there is a significant cross-over of employees and senior figures between the organisations named above.

14. The Commissioner, on 3 July 2018, having learned that Leave.EU were including advertisements for GoSkippy on their electronic newsletters, requested details from GoSkippy in relation to the consent being relied upon for that marketing.

15. On 18 July 2018 GoSkippy responded to the Commissioner to advise that although no data was shared, Leave.EU were indeed including a promotional discount for GoSkippy within their emails.

16. The Commissioner served Go Skippy with an Information Notice on 27 July 2018, receiving a response on 23 August 2018 which advised that although GoSkippy prepared marketing material for general use, it was Leave.EU which had incorporated it into a banner to be included within their newsletters.

17. Further it was advised that there existed no formal contract between GoSkippy and Leave.EU for the processing of data or the promotion of each other's services, but that in any event it was Leave.EU which had both instigated and sent the emails.

18. The further information provided to the Commissioner during her investigations disclosed the following:

- Between 25 February 2017 and 31 July 2017, 1,020,661 such emails were received by Leave.EU subscribers.

- The majority of these emails were weekly round-up newsletters and all of them contained a banner showing the GoSkippy logo and offered '10% off' for Leave.EU supporters. If the banner is clicked the GoSkippy website is accessed.

- In addition, on 23 August 2016, 49,191 emails were sent to subscribers titled "Skippy Saves the Day". Again, the content of these messages offered a 10% discount on all GoSkippy insurance products.

19. This response confirmed therefore that a total of 1,069,852 messages were sent by Leave.EU and received by subscribers over two separate periods, each containing marketing material promoting the services of GoSkippy.

20. The Commissioner has made the above findings of fact on the balance of probabilities.

21. The Commissioner has considered whether those facts constitute a contravention of regulation 22 of PECR by GoSkippy and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

22. The Commissioner finds that GoSkippy has contravened regulation 22 of PECR.

23. The Commissioner finds that on 23 August 2016, and between the dates of 25 February 2017 and 31 July 2017, GoSkippy instigated the transmission of 1,069,852 direct marketing emails to Leave.EU subscribers contrary to regulation 22 of PECR.

24. Section 11(3) DPA definition of direct marketing covers any advertising or marketing material, and applies to messages which contain even some marketing elements, even if that is not their main purpose.

25. In this instance, although Leave.EU would appear to be the sender, and whilst the primary reason for the messages seems to be its function as a Leave.EU political newsletter, it appears to the Commissioner to be reasonable to find that, for the purposes of the promotional banner at least, GoSkippy are the instigator of those messages.

26. Therefore, it is incumbent on GoSkippy, as the instigator of direct marketing, to ensure that it is compliant with the requirements of regulation 22 of PECR, and to ensure that valid consent to send those messages had been acquired.

27. "Consent" within the meaning of regulation 22(2) requires that the recipient of the electronic mail has notified the sender that he consents to messages being sent by, or at the instigation of, that sender. Indirect, or third party, consent can be valid but only if it is clear and specific enough.

28. The Commissioner's direct marketing guidance says "organisations need to be aware that indirect consent will not be enough for texts, emails or automated calls. This is because the rules on electronic marketing are stricter, to reflect the more intrusive nature of electronic messages."

29. It goes on to say that indirect consent can be valid but only if it is clear and specific enough. Moreover, "the customer must have anticipated that their details would be passed to the organisation in question, and that they were consenting to messages from that organisation. This will depend on what exactly they were told when consent was obtained".

30. Consent will not be "informed" if individuals do not understand what they are consenting to. Organisations should therefore always ensure that the language used is clear, easy to understand, and not hidden away in a privacy policy or small print. Consent will not be valid if individuals are asked to agree to receive marketing from "similar organisations", "partners", "selected third parties" or other similar generic description.

31. The Commissioner understands that there exists no formal contract between GoSkippy and Leave.EU, with GoSkippy indicating only that they had received an assurance from Leave.EU that marketing would be sent only to those who had consented to receive its communications.

32. Since it does not appear that GoSkippy have had a prior relationship with the subscribers who received marketing for their products, they would not be able to rely on the 'soft opt-in' exception provided under regulation 22(3) of PECR.

33. Furthermore, having reviewed the Privacy Policy relied upon by Leave.EU, it is clear to the Commissioner that GoSkippy are not specifically named, or identified in such a way that would suggest they could lawfully instigate direct marketing to subscribers.

34. The Commissioner is therefore satisfied that GoSkippy did not have the necessary valid consent for the 1,069,852 direct marketing emails for which it instigated transmission to subscribers.

35. The Commissioner is satisfied that GoSkippy was responsible for this contravention and has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

36. The Commissioner is satisfied that the contravention identified above was serious. This is because on 23 August 2016 and between the dates of 25 February 2017 and 31 July 2017, a total of 1,069,852 direct marketing emails were instigated by GoSkippy and received by subscribers advertising marketing material for which they had not provided consent.

37. The Commissioner is therefore satisfied that condition (a) from section 55A(1) DPA is met.

Deliberate or negligent contraventions

38. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that GoSkippy's actions which constituted that contravention were deliberate actions (even if GoSkippy did not actually intend thereby to contravene PECR).

39. The Commissioner considers that in this case GoSkippy did not deliberately contravene regulation 22 of PECR.

40. The Commissioner has therefore gone on to consider whether the contraventions identified above were negligent. First, she has considered whether GoSkippy knew or ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is met, given that the issue of unsolicited emails have been widely publicised by the media as being a problem. Furthermore, it would be reasonable to expect an organisation who is registered with the ICO to be aware of their obligations under PECR

and to carry out steps to ensure compliance when engaging in the instigation of direct marketing.

41. Second, the Commissioner considered whether GoSkippy failed to take reasonable steps to prevent the contraventions. The Commissioner has published detailed guidance for those carrying out direct marketing explaining their legal obligations under PECR. This guidance gives clear advice regarding the requirements of consent for direct marketing and explains the circumstances under which organisations are able to carry out marketing over the phone, by text, by email, by post, or by fax. In particular it states that organisations can generally only send, or instigate, marketing emails to individuals if that person has specifically consented to receiving them from the sender.

42. Reasonable steps could have included for instance carrying out the necessary due diligence checks to ensure that GoSkippy were specifically named within the Privacy Policy of Leave.EU as the holder of the marketing list, or ensuring sufficiently contractual relations existed between the organisations to provide suitable assurance to GoSkippy that marketing of their products by Leave.EU was lawful. It is not sufficient that Leave.EU and GoSkippy share directors since this would not be immediately apparent to the subscriber, nor could it be reasonably expected by the subscriber that they would receive marketing relating to insurance products as part of a political party newsletter.

43. In the circumstances, the Commissioner is satisfied that GoSkippy failed to take reasonable steps to prevent the contraventions.

44. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

The amount of the penalty the Commissioner proposes to impose

45. The Commissioner has taken the following mitigating factor into account:

- The Commissioner has received no complaints about the contravention.

46. The Commissioner has considered the likely impact of a monetary penalty on GoSkippy. She has decided on the information that is available to her, that GoSkippy has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

47. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with PECR. The sending of unsolicited marketing emails is a matter of significant public concern. A monetary penalty in this case should act as a general encouragement towards compliance with the law, or at least as a deterrent against non-compliance, on the part of all persons running businesses currently engaging in these practices. The issuing of a monetary penalty will reinforce the need for businesses to ensure that they are only messaging those who specifically consent to receive marketing.

48. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£60,000 (sixty thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Conclusion

49. The Commissioner intends to make her final decision as to whether to serve a monetary penalty notice for such amount on or after **5 December 2018**. If you wish to make any representations as to why the Commissioner should not serve a monetary penalty notice you must do so before that date. A sheet explaining the procedure for making representations is attached to this Notice of Intent as Annex 1.

Dated the 5th day of November 2018

Signed [redacted]

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Information Commissioner's Office

ANNEX 1

DATA PROTECTION ACT 1998

REPRESENTATIONS IN RESPONSE TO A NOTICE OF INTENT

The Commissioner has power under sections 55A and 55B of the Data Protection Act 1998 to serve a monetary penalty notice on a Data Controller. Before she exercises this power the Commissioner wishes to take account of all the relevant facts and arguments.

This Notice of Intent is to enable the Data Controller affected to put forward their side of the case. The Commissioner's intentions are set out in the accompanying Notice of Intent. If you wish to make representations on those matters you have an opportunity to do so. The closing date for this is in the accompanying Notice of Intent.

Representations should be made in writing. You may wish to comment on the facts and views set out by the Commissioner or to make general remarks on the case and enclose documents or other material. You should also inform the Commissioner if any confidential or commercially sensitive information should be redacted from a monetary penalty notice.

All representations will be carefully considered by the Commissioner before a final decision is made.

Representations should be sent by post to Mr Zachary Whiting, Chartered Legal Executive, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by email to zachary.whiting@ico.org.uk.

Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

PRELIMINARY ENFORCEMENT NOTICE

To: Eldon Insurance Services Limited (trading as GoSkippy Insurance)

Of: Lysander House (2nd floor), Catbrain Lane, Cribbs Causeway, Bristol BS10 7TQ

1. The Information Commissioner ("Commissioner") is minded to issue Eldon Insurance Services Limited [T/A GoSkippy Insurance] (referred to hereafter as "GoSkippy" for the purposes of this notice) with an enforcement notice under section 40 of the Data Protection Act 1998 ("DPA"). The notice is in relation to a contravention of Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").

2. This notice explains the Commissioner's decision.

Legal framework

3. GoSkippy, whose registered office is given above (Company House Reference: 06334001), is the organisation stated in this notice to have instigated the transmission of unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing contrary to regulation 22 of PECR.

4. Regulation 22 of PECR states:

"(1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

(4) A subscriber shall not permit his line to be used in contravention of paragraph (2)."

5. Section 11(3) of the DPA defines "direct marketing" as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". This definition also applies for the purposes of PECR (see regulation 2(2)).

6. "Individual" is defined in regulation 2(1) of PECR as "a living individual and includes an unincorporated body of such individuals".

7. "Electronic mail' is defined in regulation 2(1) of PECR as "any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

8. A "subscriber" is defined in regulation 2(1) of PECR as "a person who is a party to a contract with a provider of public electronic communications services for the supply of such services".

9. PECR implements European legislation (Directive 2002/58/EC) aimed at the protection of the individual's fundamental right to privacy in the electronic communications sector. PECR was amended for the purpose of giving effect to Directive 2009/136/EC which amended and strengthened the 2002 provisions. The Commissioner approaches PECR so as to give effect to the Directives.

10. The DPA contains enforcement provisions at Part V which are exercisable by the Commissioner. Those provisions are modified and extended for the purposes of PECR by Schedule 1 PECR.

11. Section 40(1)(a) of the DPA (as extended and modified by PECR) provides that if the Commissioner is satisfied that a person has

contravened or is contravening any of the requirements of the Regulations, he may serve him with an Enforcement Notice requiring him to take within such time as may be specified in the Notice, or to refrain from taking after such time as may be so specified, such steps as are so specified.

12. The provisions of the DPA remain in force for the purposes of PECR notwithstanding the introduction of the Data Protection Act 2018 (see paragraph 58(1) of Part 9, Schedule 20 of that Act).

The contravention

13. The Commissioner finds that on 23 August 2016, and between the dates of 25 February 2017 and 31 July 2017, GoSkippy instigated the transmission of 1,069,852 direct marketing emails to Leave.EU subscribers contrary to regulation 22 of PECR.

14. "Consent" within the meaning of regulation 22(2) requires that the recipient of the electronic mail has notified the sender that he consents to messages being sent by, or at the instigation of, that sender. Indirect, or third party, consent can be valid but only if it is clear and specific enough.

15. The Commissioner understands that there exists no formal contract between GoSkippy and Leave.EU, with GoSkippy indicating only that they had received an assurance from Leave.EU that marketing would be sent only to those who had consented to receive its communications.

16. Since it does not appear that GoSkippy have had a prior relationship with the subscribers who received marketing for their products, they

would not be able to rely on the 'soft opt-in' exception provided under regulation 22(3) of PECR.

17. Furthermore, having reviewed the Privacy Policy relied upon by Leave.EU, it is clear to the Commissioner that GoSkippy are not specifically named, or identified in such a way that would suggest they could lawfully instigate direct marketing to subscribers.

18. The Commissioner is therefore satisfied that GoSkippy did not have the necessary valid consent for the 1,069,852 direct marketing emails for which it instigated transmission to subscribers.

19. The Commissioner is satisfied that GoSkippy was responsible for this contravention.

20. The Commissioner has considered, as she is required to do under section 40(2) of the DPA (as extended and modified by the Regulations) when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage. The Commissioner has decided that it is unlikely that actual damage has been caused in this instance.

21. The Commissioner is minded to exercise her powers under section 40 of the Act to serve an Enforcement Notice requiring GoSkippy to take specified steps to comply with regulation 22 of PECR. The terms of such Notice are set out in Annex 1 of this Preliminary Notice.

22. The Commissioner intends to make her final decision as to whether an Enforcement Notice should be served on or after **5 December 2018**. If you wish to make any representations as to why the Commissioner should not serve an Enforcement Notice in those terms you must do so

before that date. A sheet explaining a procedure for making representations is attached to this Preliminary Notice as Annex 2.

Dated the 5th day of November 2018

Signed [redacted]

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

TERMS OF THE PROPOSED ENFORCEMENT NOTICE

GoSkippy shall within 30 days of the date of this notice:

Except in the circumstances referred to in paragraph (3) of regulation 22 of PECR, neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified GoSkippy that he clearly and specially consents for the time being to such communications being sent by, or at the instigation of GoSkippy.

ANNEX 2

DATA PROTECTION ACT 1998

REPRESENTATIONS IN RESPONSE TO A PRELIMINARY NOTICE

If you wish to make representations as to why the Commissioner should not issue an Enforcement Notice in the terms proposed, you now have an opportunity to do so. The closing date for this is shown in the accompanying Preliminary Notice. Representations should be made in writing. You may wish to comment on the facts and views set out by the Commissioner or to make general remarks on the case and enclose documents or other material. All representations will be carefully considered by the Commissioner before a final decision is made.

In exceptional circumstances the Commissioner may agree to hold a hearing in which you or your representative can put your points to her in person rather than in writing. If you think your circumstances warrant an oral hearing of this nature please write to the Commissioner within 14 days of the Preliminary Notice explaining why you think this is the case. She will then decide whether or not to invite you to an oral hearing.

Representations should be sent by post to Mr Zachary Whiting, Chartered Legal Executive, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by email to zachary.whiting@ico.org.uk.

If the Commissioner decides to serve an Enforcement Notice you will then have a right of appeal to the First-tier Tribunal (Information Rights). This is an independent Tribunal. If a notice is served you will be notified of your rights of appeal in full.

Annex v: List of 30 organisations that formed the main focus of our investigation

- Advanced skills initiative
- Aggregate IQ
- BeLeave
- 41
- CACI
- Cambridge Analytica / SCLE 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