Data Protection and Democracy

Peter Ryan
06 September 2018
COMMON WEAL is a non-profit “think-and-do tank” based in Glasgow which campaigns for greater social and economic equality, environmental sustainability, democratic participation and a higher quality of life based on an “All of Us First” approach. It was founded in 2014 and has since produced high quality, research-based policy proposals across a broad range of topics such as housing, energy, finance, social security and local democracy.

For more information on Common Weal Policy visit allofusfirst.org/policy or email craig@common.scot
Peter Ryan has worked in IT for financial services companies since 1990, over half that time as an independent contractor. He started as a programmer in 1990 on stock broking systems in London. Peter is currently working as a Product Manager and has a particular focus on taking legislation and understanding what changes need to be made to computer systems to ensure they comply with legislation. At the moment his focus is on the revised European Payment Services Directive, the roll out of the ISO 20022 message standard and the UK Payments Strategy. He is the author of a previous Common Weal reports, ‘How to make a currency’, and 'Backing Scotland’s currency' which can be found at allofusfirst.org/library
Introduction

Following the revelations that Facebook data was used by Cambridge Analytica to identify the politics of individuals based on their Facebook profiles, a light has been shone into the use of data by technology companies and the impact this has on our lives and our democracy. This Facebook data was used to target adverts to Facebook profiles in the 2015 US presidential election. In addition evidence has been provided by Chris Wylie to the ICO (Information Commissioner’s Office – the Data Protection Regulator in the UK) that Facebook data from 1 million UK users was harvested and used to influence the outcome of the European Union Referendum in the U.K. These revelations of the use of data has shocked many people and led to calls for the reform of the use of data by social media companies. It has also led some politicians to call for reform of the status of social media companies to regulate them as broadcasters instead of telecommunications companies.

The business model of many technology companies appears to be new and created by technology. They offer a free service; a search engine, a social media site, a messaging service, in return for data about us. This data is then used to target adverts to influence our behaviour; to get a better deal on insurance, to purchase certain goods or to vote a certain way.

However this brave new world is an extension of the way commercial television and radio companies have worked for years. A commercial broadcaster will allow us to watch their television shows for free provided we are prepared to sit through the adverts. These adverts will differ based on who the television company think will be watching the program; beer and cars at half time during a football match; supermarkets and detergent during a break in a soap opera. Commercial broadcasters put effort into targeting the right adverts to the expected viewing audience of a particular program because adverts are only effective if they influence behaviour; i.e. the audience will actually buy the product being advertised. If the advert is not cost-effective then the advertiser will stop placing adverts with the commercial broadcaster and so their income will be reduced.

The difference between a social media company (such as Facebook or Twitter) or a search engine (such as Google or Yahoo) and a commercial broadcaster is that the technology companies use the data the user has given them to target the advertising specifically to the user rather than use broad demographic assumptions. The obvious example is a search engine. If I search for “insurance” the first page of search results will be links to insurance comparison websites (effectively paid for adverts). It will also be recorded that I searched for insurance and for the next few days I will get adverts for insurance popping up on my screen.

This ability to target adverts is worth a lot of money. Facebook reported that it made $6.18 from each of its 2.2 billion users worldwide ($27.76 per user in US and Canada) in the final quarter of 2017. In 2017 the digital advertising revenue of Google was $95.38 billion (and remember this is just the digital advertising revenue, not the total revenue of the company).

Data, Data, Everywhere

It needs to be remembered that the use of data is not new. In fact data has been used for centuries. A Roman census is mentioned in the Bible and the Doomsday Book was a medieval collection of data that was used to make central government decisions about how much to tax a conquered population. It also needs to be remembered that the use of data is not always sinister. For example the identification that smoking was a cause of lung cancer was made through the use of data analysis techniques in 1947. The researchers (Austin Bradford Hill and Richard Doll) selected 649 patients from the London Hospital with lung cancer and 649 patients admitted to the same hospital with a different illness. In 1947 80% of middle aged British men smoked. However the researchers found that of the 649 patients with lung cancer only 2 were non-smokers whereas 27 of the non-lung cancer group were non-smokers. Giving an increased risk for smokers getting lung cancer of 14.04 times.

As the use of technology increases we are producing more data. Once upon a time my walk to the shops took about 5 minutes. Now thanks to the electronic tracker on my

---

1 Investigation into data analytics for political purposes update published by the ICO in July 2018
2 2.2 Billion users reported by Facebook
3 https://investor.fb.com/financials/?section=quarterlyearnings
5 “Big Data, Does Size Matter?” by Timandra Harkness
with the doctors and nurses treating me to help them give treatment I would expect my medical data to be shared. For example if I am in hospital undergoing medical treatment I would expect my medical data to be shared with the doctors and nurses treating me to help them give me the best treatment. This sharing of my personal data is legitimate and has my consent.

However I may not want my neighbours having access to the same medical information. If they had access to my medical history I would want to know why they needed it and who had shared it with them.

The rules around the use of personal data though are not always so clear; I may choose to allow my medical data to be used by a university to research into the causes of illness or to find a cure for disease but that should be my choice. I should also know who they are sharing it with.

An example of this was when the Royal Free hospital in London shared the medical data of 1.6 million patients with DeepMind, a subsidiary of Google. The data was used to help test an Artificial Intelligence app called Streams in the diagnosis and detection of acute kidney injury. However it was not just kidney patients whose data was shared. Furthermore this medical data was handed over to Google without the patients giving consent to share their data with Google. In fact when the ICO (Information Commissioner’s Office) investigated the use of patient data, Elizabeth Denham, the information commissioner said, “Our investigation found a number of shortcomings in the way patient records were shared for this trial. Patients would not have reasonably expected their information to have been used in this way, and the Trust could and should have been far more transparent with patients as to what was happening.”

Much of this new personal data comes from our use of social media; all the likes, petitions and photos on social media which demonstrate to the world who we are and what is important to us. In 2007 David Stillwell produced a Facebook app called myPersonality. It let people take a test that predicts their personality type based on the “Big Five” personality traits. By 2013 Michael had data on a million Facebook profiles (the figure is now over 6 million). In 2013 Stillwell, Michael Kosinski (then at Cambridge University) and Thore Graepel announced machine learning techniques could predict a person’s personality from their Facebook likes.

- With 65 likes the prediction would be “as good as a colleague’s”
- With 125 likes the prediction would be “as good as a family member”

Facebook likes have been used predict a person’s age, gender, intelligence, sexuality, political and religious views. So it is not the holding of data that makes social media different (my local shop or my bank probably have just as much of my data) but the type of data it holds. My

---

6 Elizabeth Denham was the head of the ICO at the time of their rulings against the Royal Free Hospital’s use of data.

7 “The internet knows you too well”, New Scientist article 10th March 2018
social media data is an expression of who I am because of the interaction that I have with social media. My local supermarket knows I like bananas or cheesecake, my bank knows I like pizza and how much I pay for electricity and gas each month but social media knows how I voted in the European Union referendum, my views on refugees and whether I prefer dogs or cats.

So it is not the holding of data that is important but the type of data and how it is used. For example if it were shown for example that people who like carrots supported remaining in the European Union and people who preferred peas were more likely to vote for the United Kingdom to leave the European Union then data from supermarkets could be used to target voters with political marketing in relation to the European Union. Just because it is easier to know a person's voting intentions from their social media profile it does not mean that social media is the only source of data used for political campaigning. For example the ICO have noted that the Labour Party used data taken from "Emma's Diary" an advice service for pregnant women in their campaigning.

By the way if you are beginning to think the use of personal data by commercial companies is a bit creepy then in some countries there are plans to use personal data in far more reaching ways. In China President Xi Jinping has unveiled a plan to construct a social credit system based on the principle of "once untrustworthy, always restricted." For Chinese citizens this will mean that their financial data or their social media use will be used to determine whether you are living the “life of a good citizen” and give them a corresponding social credit score. While living the life of a good citizen will bring benefits and opportunities not meeting the criteria of a good citizen will mean penalties and travel restrictions in addition to a lower credit score. Obviously the Chinese government will decide what constitutes "living the life of a good citizen".

Additionally in the USA the Trump administration has said it wants to start collecting the social media history of anyone seeking a visa to enter the USA, where they would need to disclose all social media identities used in the last 5 years. So be careful what you are posting as you will never know what a government may use the data for in the future.

Though the most worrying report on the use of Facebook data is from Myanmar. In many developing countries Facebook uses the “Free Basics” service to provide people with mobile phone access to various services without data charges. The content includes news, employment, health information and local information. Free Basics is available in 63 countries. Myanmar has a population of around 50 million people with 30 million Facebook users. Free Basics severely limits the information available to users making Facebook virtually the only source of information. In March 2018 UN Myanmar investigator Yanghee Lee accused Facebook of having morphed into a beast that helped spread vitriol against Rohingya Muslims and playing a determining role in stirring up hatred towards them. In evidence taken by the UK Parliament Digital Culture, Media and Sport (DCMS) committee enquiry into Fake News; Facebook was unable to say if it had taken any action to limit hate speech in its platform. In the view of the UN Facebook had effectively provided the conduit through which hatred against the Rohingya had been spread but took no responsibility for its spread and did little to prevent its spread.

A Mere Conduit

Facebook is regulated as a telecoms company under the Privacy and Electronic Commerce Regulation (PECR) which is the UK version of the European Union’s Privacy and Electronic Commerce Directive. Under this regulation Facebook is treated as a "mere conduit" of communication, in the same way as a telecoms company such as BT.

This means that if I am a BT customer and I make a telephone call, BT is not responsible for the content of that telephone call. I could use abusive language but BT is not responsible for my language, I am. Similarly if I post something on Facebook, under PECR; Facebook does not have editorial responsibility for the contents of my post, though they could choose to take down the post or meeting the criteria of a good citizen will mean penalties and travel restrictions in addition to a lower credit score. Obviously the Chinese government will decide what constitutes "living the life of a good citizen".

8 Democracy Disrupted by the Electoral Commission
10 http://www.bbc.co.uk/news/world-us-canada-43601557
13 https://www.bbc.co.uk/news/technology-43385677
14 DCMS Fake News Investigation
suspend the account if it does not correspond with their “community standards” (as happened with the accounts of the anti-Islamic group Britain First).16

However the main difference between a social media communication and a telephone call of course is that a telephone call is between two people and not persistent (it does not live on after the call ends). Not only is a social media post persistent but it can be shared with others; so it is a conversation that includes more than 2 people. As a result social media is often likened to publishing in that an article can be put up online and read by thousands if not millions of people. As the evidence from Myanmar has shown this means that social media companies need to face up to the responsibilities that come with the power to spread information on a mass scale.

The other difference between social media companies and telecommunications companies is that social media companies are paid for by advertising; advertising that is particularly attractive to advertisers given the ability of technology companies to offer user data to help advertisers identify the people they want to contact with a particular advert. For example Facebook has a series of tools to allow advertisers to target “lookalike” audiences17. A “lookalike” audience is one that includes Facebook users that share similar characteristics. So an advertiser can define a custom audience based on interests and a geographic location and then target an advert to that audience. So if an advertiser wanted to target a message of support for the United Kingdom to 5,000 people in Glasgow who liked a post about cats a lookalike audience could be set-up for this purpose without having to ask the permission of the Facebook users concerned.

This obviously has a particular impact with respect to election advertising. Political advertising in the broadcast media is prohibited in the UK.18 This is because it is felt that allowing political advertising in broadcast media would give an advantage to better resourced candidates. As social media companies are not considered as broadcasters then the restrictions on political advertising do not apply. This has led to calls by some journalists and politicians to change the status of social media companies (such as Twitter or Facebook) to be broadcasters instead of telecommunications companies as a way of preventing them using our personal data to target us with election and referendum advertising.

However by their very nature social media companies do not have a central organisation with overall editorial control; a post or an account can be removed but the content of posts are not changed. The other point to be remembered is that the status of a social media company as a telecommunications company is unrelated to their use of data. So while converting social media companies into broadcasters may satisfy politicians worried about the impact of social media adverts on the election it will not change how our data is used by these companies.

What is more if social media companies become broadcasters and so are prevented from carrying political adverts then this could impact our ability to post comments about the election. This is because there is no way of knowing whether a post in support of a particular candidate, party or referendum outcome is a freely given point of view or a paid for post (and so an advert). The result could be that the social media broadcaster would need to ban all discussion of the election or referendum.

One of the great benefits of social media companies is that they allow all voices to be heard. Instead of only a closed elite being published; the free to use model of social media has allowed anyone to write and publish updates (be this a picture of their dinner, a video of their rabbit or an article about sexual abuse perpetrated by rich and powerful middle aged men). Too often those calling on social media sites to be treated like broadcasters come from journalists and politicians who have no problem getting their voices heard. If social media companies become publishers of the media that is hosted on their sites then it will be too easy for them to shut down the voices of dissent and allow only the mainstream establishment voices to be heard.

However there is a dark side to this democracy. Just as the positive messages of dissent can be posted so to can abusive posts designed to intimidate people the poster does not agree with. Too often they are the electronic equivalent of a brick through a window and used to silence others; the woman who abandons social media due to misogynist abuse or the refugee activist whose voice is drowned out by racists. Too often social media companies use the freedom of expression argument and their status as a telecommunications company to allow people to continue to use hate crime language to force other people off social media with the sort of aggressive behaviour which would not be legal if spoken face to face in a public place.

One of the interim recommendations of the DCMS Committee Enquiry into Fake News was that a new category of “Tech Company” be created for social media companies18. This designation would tighten the liabilities of technology companies where they are neither a “platform” nor a “publisher”. This would allow laws to be created that
are suitable for social media that are of necessity different from telecommunications companies, broadcasters or publishers. For example one of the concerns raised about social media companies is the number of “fake accounts”. The Electoral Commission feel political parties need to be more transparent around the use of fake accounts; especially “bots” which are used to automatically like or share political adverts to give an artificial boost to the popularity of a particular message. The electoral commission feels that it is important to distinguish between “organic” sharing such as that carried out successfully by the Labour Party and Momentum during the 2017 UK Parliament election (which should not be restricted as this is the equivalent of an activist delivering leaflets and is dependent on the number of supporters a party has) and automated sharing by paid for bots (which is based on the amount of money a party has).

One advantage of creating this category is that a levy could be placed on these companies based on number of UK users which would be used to fund the work of the ICO to police the use of data by these companies. Obviously as social media companies rely on advertising for their revenues they want to maximise the number of reported users. To this end the DCMS Committee Enquiry into Fake News have asked the Competition and Markets Authority to investigate the inclusion of fake accounts in the report of the number of users by social media companies to inflate their advertising revenues.

General Data Protection Regulation

Data Protection in the UK had been controlled by the Data Protection Act since 1998. This UK law was based on the European Union Data Protection Directive. However this legislation was replaced in the European Union by the General Data Protection Regulation (GDPR) on 25th May 2018.

GDPR changes data protection. Under article 6 of GDPR a company can only lawfully process personal data based on one of six purposes:

- The person has given their consent to a company to process their data; this is why we have been bombarded with “please stay in touch” emails. The companies concerned were relying on our consent to allow them to send marketing emails to us and this consent needed to be updated.

- The processing of the data is necessary for the performance of a contract. For example if I take out a bank loan then my personal data will be needed to process the loan. So unfortunately my bank is going to keep my personal data on file until I have paid off the loan whether I want them to or not.

- My data is needed for legal reasons. For example to conform with electoral spending law political parties need to keep details of all party members who have paid a membership fee.

- Processing of the data is required to protect my vital interests; for example medical staff having access to my medical records while treating me.

- Processing is necessary for the performance of a task carried out in the public interest, for example completing the national census.

- Processing is necessary for the purposes of the legitimate interests of the data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the person which require protection of personal data, in particular where the person concerned is a child. For example a garage may keep track of people who purchased cars from them in case they need to be contact in the event of a fault recall notice.

If a company cannot demonstrate a lawful reason to hold the personal data then the person identified by the personal data can ask for the data to be deleted (known as the right to be forgotten).

Additionally article 9 of GDPR describes specific protections associated with the following personal data:

- Data revealing racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- The processing of genetic data, biometric data, for the purpose of uniquely identifying a person
- Data concerning health
- Data concerning a person’s sex life or sexual orientation

---

19 'Digital campaigning improving transparency for voters’ Electoral Commission June 2018
20 ‘Disinformation and Fake News’ Interim Report from the DCMS Committee July 2018
Additionally European Union citizens will get the following protections:

- Their personal data cannot be used for marketing data profiling without their consent
- These rights apply to data held outside the European Union (in which case the company will be prosecuted within the European Union in the event of the company being in breach of GDPR) if the company is actively marketing to European Union citizens. So GDPR will apply to a European Union citizen’s Facebook account even if they access it in New York.

What is more the fines have become much bigger under GDPR; € 20 million or 4% of worldwide turnover (whichever is greater; Facebook’s revenue in 2017 was $40.7 billion which gives a 4% figure of $162.7 million). This compares to the € 150,000 Facebook was fined in France for “unfair tracking” in 2017 (the maximum fine allowed in France at the time) or the €1.2 million fine it received in Spain for breaking privacy laws (also in 2017). So hopefully the bigger fines will mean that Facebook starts to follow data protection laws instead of paying the fine and carrying on as before. In this regard it is indicative that Mark Zuckerberg chose to meet with the EU Parliament to discuss GDPR and data protection (but not the UK parliament).

Under GDPR for Facebook to share data with a third party (such as Cambridge Analytica) it will require that person's specific consent for the use of their personal data for data profiling. If that consent has not been given Facebook could be prosecuted (again). However a person’s political opinion is furthermore classified as sensitive data under Article 9 of GDPR. As there special restrictions in place around the processing of sensitive data it may be illegal for data profiling companies to hold a derived political opinion based on profiling without the person’s explicit consent. So under GDPR it will be much harder for a company to target voters with political adverts based on their social media profiles.

The UK Government is reviewing data protection legislation after Brexit and in its future partnership paper on “The exchange and protection of personal data” it states that it would look to a data protection law that “does not impose unnecessary additional costs to business.” While there is no detail on any future UK data protection law there is clearly a danger that the UK government will give big business greater control over our data than would be the case under GDPR. This is the situation in the USA, remember the use of Facebook data by Cambridge Analytica was considered standard practice by technology firms in the USA. If we continue to abide by the European Union data protection laws then we will get the protection from the abuse of data that has happened in the Cambridge Analytica case as a result of GDPR, if we no longer abide by GDPR then our data could be used to maximise the profits of technology companies.

Indeed on 19th April 2018 it was announced that Facebook was moving 1.5 billion Facebook users out of the European Union to evade GDPR and the potentially larger fines. Instead responsibility for these users will be managed from the California HQ of Facebook and they will be covered by US privacy laws which are less strict than those of the European Union. This will allow Facebook to continue to monetise the data held within those profiles free of the constraints of GDPR. Facebook has not confirmed where UK personal data will be held after Brexit.

Data, Political Parties and Election Expenses

In democracies parties have long used data in election campaigns. Before computers this data was collected at election time by party members and supporters. They would knock on doors armed with the electoral register and canvass the opinions of voters. They would record the responses and use the results of this canvassing to record who supported their party, who did not and who could be persuaded. This data would then be used during the campaign with reminders to vote delivered to their supporters and perhaps a visit from the candidate to those voters who were not yet supporters but appeared to be open to persuasion to vote for the candidate.

This old style campaigning was very human. If a party did

---

21 https://www.theguardian.com/technology/2017/may/16/facebook-facing-privacy-actions-across-europe-as-france-fines-firm-150k
not have supporters in an area they would not be able to campaign so the amount of campaigning reflected a party’s support. Similarly any information given by a voter would be under the voter’s control; they could decide what to tell the canvasser.

With the advent of new technology it became possible for political parties to use that technology to reach voters without the need of supporters to knock on doors and speak to voters face to face. Indeed figures released by the Electoral Commission\(^\text{25}\) show that reported spending by campaigners on digital advertising as a percentage of total advertising spend in an election or referendum campaign has risen from 0.3% in 2011 to 42.8% in 2017.

One of the areas of concern highlighted in the DMCS Committee enquiry into Fake News\(^\text{26}\) is the use of “lookalike” audiences on Facebook. This allows micro targeting of precise messages to be sent to specific groups; for example pensioners in a particular council area could be targeted with a fake news story highlighting cuts in social care by a specific council or people living in a particular council ward could be targeted with a fake news story about a crime wave from newly arrived refugees. The problem with a lot of micro-targeted adverts is that the number of people seeing the advert could be so small that it will not be possible to identify the advert as part of a particular campaign or who paid for it.

For this reason the Electoral Commission has made a series of recommendations\(^\text{27}\):

- Any election material should have a digital imprint saying who is behind the campaign and who created it (note this recommendation was first made in 2003). This was done in the Scottish Independence referendum but is not required for other elections and referenda.
- UK election and referendum adverts should be labelled to make the source clear if the advert is paid for by a group not directly part of the election or referendum.
- Social media companies should publish an online database of political adverts run during a campaign.

However political parties do not have a good track record when it comes to data protection. Some of the data protection breaches by political parties reported by the ICO are:

- Leading up to the 2005 general election the SNP made a number of automated calls to Scottish households (including some households that had registered with the Telephone Preference Society not to receive marketing calls). As the voters had not given their consent to such calls the ICO ruled that the SNP were in breach of data protection law.
- During the 2017 general election the ICO found that phone calls made on behalf of the Conservative Party “crossed the line from legitimate market research to unlawful direct marketing”\(^\text{28}\).
- An enforcement notice was issued against the Labour Party on February 4th 2010 for placing automated calls to a compiled list of just under 500,000 telephone numbers in the days before the 2009 election (having already been warned not to make automated telephone calls after a previous incident in 2007).
- It is not just political parties who are breaching data protection laws at elections. The Telegraph newspaper was fined £30,000 after its editorial team sent thousands of emails to individuals on its marketing database urging subscribers to vote for the Conservatives.

Additionally it is not just data privacy legislation that political parties are ignoring. The Cambridge Analytica scandal is about the use of data (often without the knowledge of the person whose data is being used) but the investigation by Carole Cadwallader\(^\text{29}\) also uncovered breaches of election finance rules by “Leave.EU” who have subsequently been fined £70,000 breaking election spending limits\(^\text{30}\) and “Vote Leave” has been fined £61,000 and is under investigation by the Electoral Commission\(^\text{31}\). Sadly this is just another in a long list of candidates and parties that have ignored the rules on election spending. Some of the recent incidents are:

- In 2017 the Ulster Unionist party was fined £3,000

25 Digital Campaigning Improving Transparency for Voters published by the Electoral Commission June 2018
27 ‘Digital Campaigning Improving Transparency for Voters; Electoral Commission June 2018
28 https://iconewsblog.org.uk/2017/10/23/when-political-market-research-crosses-the-line/
29 Observer newspaper dated 1st April 2018
30 http://www.bbc.co.uk/news/uk-politics-44080096
as it submitted an inaccurate spending return for the 2016 Northern Ireland Assembly election.

- The Conservative Party was fined £70,000 in 2017 for breaking election expense rules at the 2014 European Parliamentary Election, the 2015 UK Parliamentary General Election and the 2014 By-elections held at Clacton, Newark, and Rochester and Strood. In its report on the breaking of election expense rules The Electoral Commission said there was a "realistic prospect" the money had given the party an advantage.

- In 2016 the Liberal Democrats were fined £20,000 by the Electoral Commission for failing to declare all their spending in the 2015 general election campaign.

- In 2016 the Labour Party was fined £20,000 by the Electoral commission for failing to declare all their spending in the 2015 general election campaign (including the “Ed stone”).

- In 2016 the “Better Together” campaign was fined £2,000 by the Electoral Commission for failing to provide a full and complete report on its spending.

It seems we have got to the stage that political parties feel that they can ignore spending limits and election expense reporting requirements. In its June 2018 report the Electoral Commission makes a recommendation that the maximum fine for breaking electoral law (which currently stands at £20,000) be increased as many political parties view this as "the cost of doing business". It would appear that it is the Electoral Commission’s view that many political parties take the view that if a few thousand pound fine is the price for an MP to get elected then that is a price they are willing to pay.

Foreign Interference

As the nature of campaigning moves from physical to digital there is a corresponding increase in the threat of interference in an election by other countries. One of the reasons the Electoral Commission is recommending greater transparency of who is behind a campaign is that it is not always obvious if an advert is an attempt to influence an election from outside the country where the vote is taking place or part of a legitimate campaign. It is very easy for a country to use a social media company such as Facebook to create adverts which can then be targeted at UK or Scottish voters. Unless there is a clear imprint of who a campaign advert is from then it is not possible for a social media to distinguish between an advert that is party of a campaign from a registered UK party and declared on their election spending return and propaganda that has originated from outside the UK and is part of an attempt to influence an election.

A report from University of Oxford has found evidence of formally organised social media manipulation campaigns in 48 countries in 2017. In many cases the campaign included support from outside the country whose democracy was being manipulated.

It is perfectly possible for social media companies to block campaign adverts that have been placed by foreign organisations or individuals. Examples of this include:

- In the 2018 US mid-term elections Facebook, Google and Twitter have said they will check whether campaigners are based in the USA and campaigners who are not will not be allowed to place campaign adverts.

- Both Facebook and Google made changes to their policies on political adverts before the May 2018 referendum in Ireland. Facebook stopped campaigners from outside Ireland buying campaign adverts and Google banned all paid adverts about the referendum.

Indeed Google has begun publishing lists of who have paid for campaign adverts in the USA so it is perfectly possible for social media companies to both block election.

---


34 http://www.bbc.co.uk/news/uk-politics-38234883

35 http://www.bbc.co.uk/news/uk-politics-37760562


37 http://comprop.oii.ox.ac.uk/research/cybertroops2018/

38 https://transparencyreport.google.com/political-ads/overview
and referendum adverts from outside the UK and to report who has funded the adverts that are displayed on the social media platforms.

For this reason in their report on digital campaigning the Electoral Commission recommend that all the UK’s governments and legislatures should clarify that spending on election or referendum campaigns by foreign organisations is not allowed. So for example the Scottish government should clarify whether spending in Scottish Parliamentary elections by groups based outside of Scotland is allowed. Should parties use money collected in England on Scottish elections for example?

However it is not just social media adverts, it is also the source of donations. In their report on digital campaigning the Electoral Commission recommend that:

- UK Government and Parliament should make it clear that campaigners cannot accept money from companies that have not made enough money in the UK to fund the amount of their donation or loan
- UK Government and Parliament should consider how to improve the controls on donations and loans to prevent foreign money being used in UK politics

The Electoral Commission are concerned that foreign money could be channelled through a UK individual or company to make a campaign donation. Thus the money appears to come from a UK based source but the money originally comes from a foreign source to influence a UK election. To counter this they make the suggestion that money laundering regulations could be adapted to trace the source of campaign donations particularly if they are above a certain amount.

### Algorithms

So far we have looked at the use of data and how this is used to influence us when we make decisions. Increasingly though algorithms are being used to make decisions that can have a major impact on our lives. An algorithm is a set of instructions to tell a computer how to process a task. However it is the control of these algorithms and the power that they have to impact our lives that is behind a lot of the concerns over the use of data by companies such as Google, Facebook or Cambridge Analytica.

While algorithms are complex we are used to their impact; “the computer says no”.

They generally work by taking in data about us and making a decision based on that data. So for example a bank will use an algorithm to calculate whether or not I am eligible for a loan based on my job, my income, my age, my credit history, etc. If I am a married, home-owning man in my forties with a salary of £50,000 applying for a £10,000 loan the computer is likely to say “Yes”. If I am a single woman employed on a zero hours contract currently in private rented accommodation the computer may well say “No”.

Algorithms reduce us to a series of data points. They are often heralded as being fairer than a decision being made by a human being due to the prejudices too often present in human decision making (for example using an Islamic or a Christian name on a CV can mean the difference between someone getting an interview for a job). It is thought that the non-human nature of algorithms mean that such prejudices will be eliminated. However what this misses is that algorithms are programmed and tested by humans. This means that a human creating and testing the algorithm would expect the algorithm to come up with similar results to themselves; thereby embedding the prejudices within the algorithm to ensure that it comes up with the “expected” results.

This situation could get worse with the advent of Artificial Intelligence (AI). What Artificial Intelligence does is learn the “correct” result. With Artificial Intelligence the human oversight of the algorithm is removed but because of the way AI uses existing data to look for patterns to identify the “correct” result then it can mean that existing prejudices are reinforced. More worryingly as AI will be learning how to use the data free of human input then it will not be possible to identify why a particular result was reached.

A good example of this going wrong is the sentencing of convicted criminals in the state of Wisconsin based on an assessment by the secret algorithm in the COMPAS software.

COMPAS is software developed by a private company, Northpointe Inc., which calculates the likelihood of someone committing another crime based on his or her past conduct. It then suggests the sentencing based on this result. COMPAS assessments are a data-driven complement to the written presentencing reports long compiled by law enforcement agencies in the USA. One of the big issues with the algorithm at the heart of this software is that it is proprietary software; meaning the calculation is a commercial secret. Thereby making it impossible to challenge the result. However the non-profit

---

39 Electoral Commission “Digital Campaigning Improving Transparency for Voters” June 2018
40 Electoral Commission “Digital Campaigning Improving Transparency for Voters” June 2018
news organisation ProPublica\textsuperscript{44} investigated COMPAS by comparing the sentences that came from the software against the actual re-offending rates of criminals sentenced by the software. They discovered:

- “black defendants who did not recidivate over a two-year period were nearly twice as likely to be misclassified as higher risk compared to their white counterparts (45 percent vs. 23 percent)"
- White defendants were often predicted to be less risky than they were.
- Black defendants were also twice as likely as white defendants to be misclassified as being a higher risk of violent recidivism

Indeed Northpointe have admitted that men and women receive different assessments\textsuperscript{42}.

As secret algorithms proliferate there needs to be policies in place to ensure that if they are used that not only are they transparent (and so open to challenge) but also that the algorithm can demonstrate that is does not perpetuate social bias based on gender, sexual orientation or ethnicity.

Again there is some protection offered by GDPR for algorithms. If there is a decision made purely on the basis of automated decision making that significantly effects that person then they have a right to challenge the result and for the challenge to be heard by a person rather than a machine. However this is reliant on people knowing their rights and being prepared to challenge the automated decisions of big business.

Next Steps

The Cambridge Analytica scandal consists of two things:

- The use of personal data by technology companies
- The impact of new technology on elections

Whilst politicians and political commentators have been focussed on the latter, many people have been focussed on the former with hashtags such as “#deletefacebook” trending on social media. For this reason I have divided the conclusion section of this document into the steps required to protect our data and the next steps to protect our democracy.

Steps to Protect Our Data

If the United Kingdom was staying in the European Union then I believe we should wait for a few years to see what the impact of GDPR is on the use of personal data by large technology companies. Indeed many other nations around the world are adopting this position, while some (such as Australia) are already adopting some of the GDPR regulations to update their own data protection laws. However if the United Kingdom does leave the European Union we need to ensure the protections given to us by GDPR are not lost when the United Kingdom leaves the European Union. As a minimum this should include the following:

- Retention of the 6 purposes of holding data including the right to restrict the use of our personal data in marketing without our consent
- Retention of the specific classification of “sensitive” data
- Continuation of our effective ownership of our own personal data through the right to be forgotten
- Retention of the large fines for data protection breaches

However it also needs to be remembered that the use of data can help us achieve great things. As the example of smoking shows, data analysis can help us achieve medical breakthroughs. In many cases recommendations for healthy eating and taking more exercise are based on data studies, as is the identification of the increased risk of getting breast cancer due to mutations in the BRCA gene. Even 200 years ago the discovery of the smallpox vaccine was based in data profiling (milk maids got cowpox but not smallpox).

One of the regular complaints regarding analysis of Scotland is the lack of “Scottish” data. Too often “Scottish” data is an extrapolation of United Kingdom figures rather than data that is purely Scottish, a point made in papers such as the Common Weal paper “Scotland’s Data Desert” which argues the case for a Scottish Statistics Agency\textsuperscript{43}. As has been described in this paper the discussions, comments, likes and petitions on social media are a great

\textsuperscript{41} https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm
\textsuperscript{42} Quoted in New York Times June 22nd 2016
source of data to such an extent that some local authorities (such as the city of Ghent in Belgium) are investigating setting up local social media organisations. The data from these local social media would then be used as a source of data to help analyse the problems the local area is facing and be used to help solve them. For example if there were a number of complaints about a redevelopment scheme or a number of likes connected to a proposed sports complex or swimming pool this can be used to gauge a level of support or opposition. This would be more scientific than 3 letters published in a local paper. I believe the Scottish government should investigate some of these experiments to see if there is anything that Scotland can learn from them and whether we should create a similar social media platform in Scotland.

To achieve a vibrant society social media needs to remain free but we need its use to be transparent and inclusive. We want to maintain the ability for all of us to post our thoughts and give our point of view but this should be done in such a way that it does not prevent anyone else from similarly feeling safe enough to speak out.

To achieve this I would suggest that Scotland / UK follows Germany’s example and passes a law along the lines of the Netzwerkdurchsetzungsgesetz (or NetzDG) that ensures the safety of our data.

Additionally a new category of “Technology Company” should be established so that specific rules around technology companies and their use of data can be established. A levy should be raised against technology companies based on the number of UK users. This levy should be used to pay for the Information Commissioner’s Office to enable them to be properly resourced to ensure the safety of our data.

Steps to Protect Our Democracy

The Cambridge Analytica scandal and associated issues with “fake news” and micro targeted campaign adverts have led to a number of ongoing enquiries; some of which have been referenced in this document. These include:

- Electoral Commission – Digital Campaigning Increasing Transparency for voters
- Information Commissioners Office – Investigation into Data Analytics for Political Purposes
- Information Commissioners Office – Democracy Disrupted
- UK Parliament Digital Culture Media and Sport Committee Investigation into Fake News

Many of these enquiries produced interim reports in June or July 2018 and are scheduled to report final conclusions in late 2018. These interim reports have made a series of recommendations. However these should be treated with caution as some of the recommendations have been made before and ignored by successive governments (the recommendation for imprints on digital adverts was made by the Electoral Commission in 2003 for example) and some of the enquiries are being run by politicians from the same parties that consistently ignore the existing rules; for example the Digital Culture Media and Sport Committee is currently made up of 5 Conservative MPs, 5 Labour MPs and 1 SNP MP.

Social media sites remove “obviously illegal” hate speech and fake news within 24 hours or face a 50 million Euros fine. Essentially if a post is illegal then the social media company has to take it down or face big fines. This will force the companies to take action against the abusers while still allowing the rest of us to have the ability to communicate to anyone who chooses to listen to us. It would be up to democratically elected parliaments to decide where the boundaries between legal and illegal posts as part of the drafting of such a law (in the same way that there are laws against incitement to racist and religious hatred). As a result of the introduction of NetzDG, 1 in 6 Facebook moderators works in Germany which demonstrates if the fines are large enough the abuse on social media will be taken seriously by social media companies.

The original ban on political advertising was instigated to ensure the fairness of our elections. It would ensure that elections were not decided based on how much money a campaign had. If our democracy is not to be sold to the highest bidder then we need to return to a position of fairness. We also need to ensure that our elections continue to be decided by those citizens who will be governed by the elected representatives. We need to ensure that our political campaigning is not influenced by foreign governments for their own benefit. To this end I feel we should do the following:

- A ban on foreign sponsored advertising on social media during the election period. The definition of “foreign” should be based on the election. So for a UK Parliamentary election this would be any advertising sponsored from outside the United Kingdom whereas for Scottish Elections (including any future independence referendum) this would ban any advertising sponsored by an organisation or individual based outside of Scotland
- A cap on donations as proposed by the Electoral Commission. For example no individual or organisation could make a political donation of over £20,000 in a single year. The alternative; to make all donations traceable to avoid the risk of foreign
donations being laundered through UK individuals or organisations, would be difficult to administer and expensive to investigate.

- The costs of directly employed staff working on election and referendum campaigns should count towards political parties' and referendum campaigns spending limits (as recommended by the Electoral Commission in 2013).

- All election or referendum campaign materials (whether in digital or physical form) to carry the imprint of the organisation that paid for the material (as recommended by the Electoral Commission in 2003).

- A declaration from all technology companies of the amount spent on political adverts during an election period. This accompanied with a more detailed breakdown of advertising spending on election returns will allow greater transparency of spending on digital campaign materials.

- Due to the targeting of social media adverts the number of people receiving a particular advert may be small and the adverts will be specifically designed to appeal to the people receiving the advert. Due to this they could contain misleading or indeed libellous claims which may not be challenged. For this reason all social media adverts should be registered with the electoral commission and held in a publically available database. This database would include where it was deployed (social media platform, post-codes, etc.) and the profiling used (for example males aged 35-45). This would allow voters to know who had their data, what they were using it for and to object to its use.

- Finally the election rules will only be followed when the punishment is severe enough. Fining parties spending millions on an election £20,000 means that the parties feel the fine is “just the cost of doing business”. Consequently I suggest any successful candidate that breaks election law should be barred from the office they have been elected to for a period of the lifetime of the council or parliament and the election re-run. Similarly if campaign rules are found to be broken during a referendum the possibility of rerunning the referendum should be a potential outcome of an investigation in addition to larger fines.