Daanish Ahsan
Data Ethics and Governance ECMM438
Candidate Number: 124070

The Cambridge Analytica Scandal: How Data Endangers Democracy

Introduction

The term 'Data Science' was first coined by computer scientist Peter Naur (Naur, 1974). Yet over the following decades the field and term were never clearly defined due to the interdisciplinary nature of it. Today however, data science and its associated subfields are much more clearly defined. One could point to Harvard Business Review's famous article, 'Data Scientist: The Sexiest Job of the 21st Century' (Davenport and Patil, 2012) as being the primer for bringing the previously shadowy field to the public eye. Eight years on from that article, the field of data science, is exploding at incredible speed, leading to predictions that data science would become the fourth paradigm of science, alongside empirical, theoretical, and computational (Tansley, Tolle and Hey 2011). The exponential growth of data science over the past decade is not simply due to its uses in science, but goes hand in hand with 'datafication' (Cukier and Mayer-Schoenberger, 2013) and the data deluge.

Data Science has vast applications, from fraud detection to image recognition, to healthcare, that benefit not only companies, but also society. Yet alongside the information explosion, the risk of data misuse has also risen, and data science has provided the perfect tools for data to be purposefully weaponised. In just the first half of 2019, there were 3800 publicly disclosed data breaches, with over 4.1 billion data records exposed (Rafter, 2019); there are likely many more undisclosed breaches. Arguably the king of these data scandals, was the Cambridge Analytica Scandal (henceforth CA). Data from around millions of Facebook accounts were harvested and analysed without consent; the data was used for 'psychographic marketing (Gibney, 2018), whereby specific ads were targeted at specific users based on their Facebook information. Numerous documents and evidence have since come to light showing CA was hired to use these techniques to influence and interfere in the highly controversial Brexit vote and Trump win (Cadwalladr and Graham-Harrison, 2018). Further links have been shown with Russian interference groups in tampering with political events. The case can be made then that data endangers democracy, which has huge ramifications for free will and international electoral systems. This essay will explore how CA accessed the data and what they did with it. The second part of this essay will examine the literature for the effectiveness of psychographic targeting, (also known as microtargeting), and touch upon the ethics and implications of it, before concluding where literature can further expand on the field of microtargeting.

Context

'Data science focuses on exploiting the modern deluge of data for prediction, exploration, understanding, and intervention' (Blei and Smyth, 2017). CA claimed to be able to "change audience behaviour" (Osborne, 2018) for its clients, by using data science alongside behavioural science for psychographic marketing. It is common knowledge today that companies and platform focus specific ads on specific audiences; for example, Facebook can stratify its users by demography, age, location, and a plethora of other characteristics. Psychographic marketing is more disturbing in that it 'targets people on the basis of their personality traits' (Gibney, 2018); CA aimed to use this to boost support for their clients, namely Leave.EU, and the Trump campaign. Steve Bannon, the man who would become Trump's chief strategist of his political campaign in 2016, was vice president of CA, and it was under his and CA CEO Alexander Nix's authority that the scandal began. CA hired Cambridge University data scientist Aleksandre Kogan to design an app to build up pictures

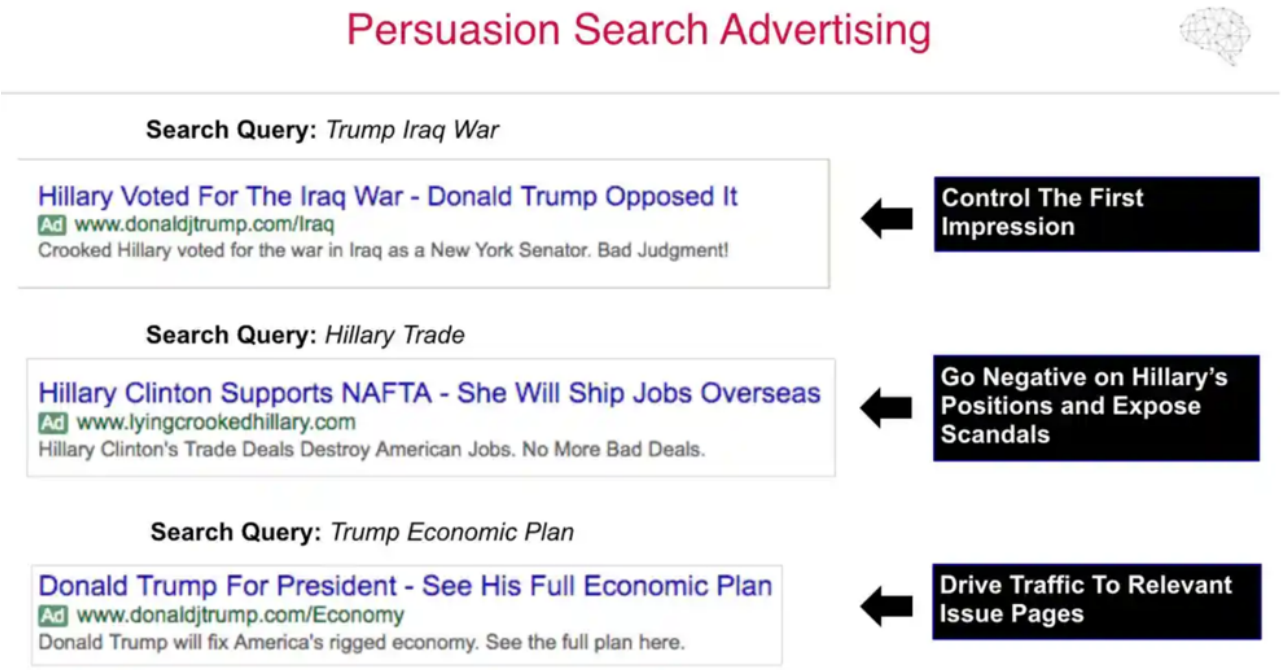
of users' personalities based on their Facebook data- ie preferences and likes. Users of the app were to connect via their Facebook profiles, and were paid for taking a personality quiz; this part of the process included informed consent from CA. Around a quarter of a million Facebook users used the app, and were notified that the data collected was to be used for purely academic purposes. Yet unbeknownst to the the users was that by connecting through their Facebook accounts linked their Facebook friends through the app as well, providing CA with millions of unconsented users' data. It is unknown if the app was purposely designed in such a way, but what is known is that Facebook's platform policy at the time did not prohibit collecting app users' friends' data, as long as the data was used to improve the performance of the application (Cadwalladr and Graham-Harrison, 2018, The Guardian). This was among several of Facebook's high profile mistakes regarding the scandal, and allowed CA to harvest data information on around 87 million users (Hern, 2018); each app user brought along the data of around 340 friends on average (Boldyreva, 2018).

Methods

The company proceeded to use peoples' data to build "models to exploit what we knew about them and target their inner demons", according to former CA employee-turned-whistleblower Chris Wylie (Cadwalladr and Graham-Harrison, 2018). In other words this was political microtargeting on a scale hitherto unseen, with sophistication and efficacy provided by cutting edge data science techniques, that in decades prior simply did not exist. The blueprints for assisting the Leave campaign and the Trump campaigns were broadly the same in that they involved 'intensive survey research, data modelling, and performance-optimising algorithms' (Lewis and Hilder, 2018), to come up with a final algorithm which could analyse Facebook profiles and confirm personality traits linked to voting behaviour. The vast database that had been accumulated was then extrapolated in order to predict voting patterns of users that CA had not been able to collect. The algorithm, database and prediction information in tandem, allowed the company to make recommendations to its clients in advertising to specific segmentations of Facebook users, to maximise the impact of political adverts. Examining this from a political science perspective, partisan votes are often viewed as "secure" or "locked in", because these types of voters have a strong affiliation with a particular party, and so tend to always vote for them. Partisans can thus be viewed as party's base of support, and so there is little point in opposition parties, nor their own parties, blasting them with campaign messages and political incentives. The real influence in political votes lies with swing voters; examples of these are first time voters or people who vote differently in every campaign based on certain things that appeal to them. In this view, CA was essentially identifying the most persuadable voters, methods, and would then 'bombard these psycho-profiled targets, to push these persuadable' buttons and tip them over the edge' (Bradshaw, 2019) into voting for whichever client was paying CA.

A leaked CA presentation obtained by the Guardian in 2018 (Lewis and Hilder), details some of the microtargeting techniques used to assist the 2016 Trump campaign. The Youtube homepage was used as an advertising space by the Trump campaign, after Clinton's campaign gave it up because they were so sure of victory. Visitors to the site were shown different ads based on whether algorithms and data suggested that they were Trump supporters or not. If they were, a large triumphant Trump was shown, along with directions to the nearest polling station; if not, they were shown his most famous supporters, such as Kanye West or UFC president Dana White. The slide below (The Guardian, 2018) shows how the company implemented persuasion search advertising, in order to push a pro Trump

and anti Clinton narrative when voters searched Google for political matters relating to the two candidates.



CA also worked with the Trump campaign to produce an interactive graphic (The Guardian, 2018) on Politico (shown to the right), which appeared only to site visitors identified as key swing voters who could potentially decide the election (Lewis and Hilder, 2018). Through these methods and more, CA were attempting to mass manipulate the free will of swing voters by using their very own data against them, having obtained that data illegally and without consent in the first place. This strange free reign CA seemed to have been given by Facebook and a distinct lack of rigorous data privacy laws thus allowed CA to carry out their goal of an 'ultimate gold standard of understanding personality from Facebook profile information' according to a leaked CA contract (Cadwalladr and Graham- Harrison, 2018). Before moving on to the next part of the essay where the effectiveness and ethics of microtargeting will be explored, it is important to wrap up the CA story by concluding what their impact was; as Bradshaw (2019) notes, 'Trump and Brexit won on a knife edge'. CA closing down, and the webs of lies and document destruction that subsequent investigations have attempted to navigate have further clouded the exact impact of their work. Only by examining the efficacy of politically motivated microtargeting, can it be somewhat determined as to what extent CA effectively rigged Brexit and the Trump campaign.

Profiling

CA's model of using social media data to build up personality profiles of users is thought to have been inspired by the work of Cambridge psychology researchers Kosinki, Stillwell and Greapel (2013). In their research, they used Facebook likes provided by over 58,000 volunteers, and applied dimensionality reduction alongside logistic and linear regressions, to predict sensitive attributes. Some examples of these attributes included satisfaction with life, political views, and whether an individual's parents had stayed together until the individual was 21 or not. The model predicted attributes surprisingly well, correctly classifying between African Americans and Caucasian Americans (95%), relationship status (65%), substance abuse (73%), and if users' parents had divorced before users were 21 (60%). Indeed, as Kosinki et al (2013) note in terms of users' parents divorcing before 21, "it is remarkable that this is detectable through Facebook likes". It is also fascinating to note that attributes could be predicted based on likes which have no explicit correlation to the attribute; for example, high IQ is associated with liking Curly Fries and having fewer friends is associated with liking In'n'out Burger Restaurant. The predicted attributes were then fed into a personality scale based on five well established traits; 'agreeableness, neuroticism, openness to new experiences, extroversion and conscientiousness (Resnick, 2018). Based on this study, it is clear then that the digital prints left by social media users can be analysed to accurately build up a picture of users' personalities; doing this without consent to use this data, or to build personality databases as CA did was clearly a vast breach of data privacy.

Effectiveness

Evaluating how effective microtargeting itself is in swaying voter decisions is pivotal in measuring the scale of danger that democracy is in from data; the literature on this exact impact is very limited. One study during the 2008 US presidential election used the Big 5 personality traits to predict likelihood of 743 college students changing their vote to Obama, and concluded that Obama won the election not by winning over massive chunks of the population, but by tactically winning over potential converts (Tost et al, 2009). Nevertheless, the research also notes that the students' parent's political views were far more predictive of voting behaviour in the election, than any personality traits. Kosinki et al (2017), follow up on their 2013 work by examining the effectiveness of psychological targeting in enhancing mass persuasion. The authors carried out three field experiments to target over 3.5 million people with psychographic advertising, tailored to people by their personality profiles which were informed by their internet and social media behaviour. It was found that psychographic targeting as opposed to randomised adverts, boosted internet purchases by up to 50% and increased clicks by around 40%, suggesting that it is 'possible to influence large groups of people' via microtargeting (Kosinki et al, 2017). However, it should be noted that people's political identities choices are informed by our personalities, partisan identities, ideologies, and our personal history (Resnick, 2018), and so are much more complicated compared to decisions in buying internet products.

Kalla and Broockman (2017) analysed 40 field experiments and carried out 9 original experiments to estimate the impact of advertising and political campaigning. They conclude that the average effect of these experiments on Americans' political choices was zero, with 2 exceptions. These are when political candidates take unusually unpopular positions and their campaigns invest heavily in identifying swing voters (as the Trump campaign did), or when campaigns advertise to voters well before elections, and measure the effects immediately. Additionally, a randomised controlled trial of 61 million people who were sent political

mobilisation messages found that the overall voter persuasion rate was just 0.39%; although strikingly, the 'effect of social transmission on voting was greater than the direct effect of the messages themselves' (Bond et al, 2012), highlighting the role of communication with close contacts in voting behaviour. The method of microtargeting then, seems "more of an art than a science" (Resnick, 2018) and the behavioural, political and data scientists responsible for creating political microtargeted ads may be better than the average person at trying to convince swing voters, but the overall impact of microtargeting is still incredibly hard to assess.

Ethics and Implications

One could argue that the debate over the effectiveness of microtargeting is of less significance; the emphasis should surely be on the ethics of trying to psychologically mass manipulate people's free will, and the lack of laws in preventing microtargeting. Political voters wield the vast power in their ability to push their country forward economically, technologically and in terms of soft power, depending on the type of government that is voted in. Thus poorly performing governments such as the Trump administration can be massively damaging to the overall status of a country; since the election of Trump, the USA- once viewed as the world's policeman and chief champion of freedom and democracy, has since become a shadow of what it once was- few economists and political scientists would argue against this. Microtargeting as a form of mass persuasion, could be employed to do things such as help people lose weight or avoid drugs; yet its chief use seems to be political, in 'exploiting weaknesses in people to make them take action against their own best interest' (Kosinki et al, 2017). Indeed, swathes of economists have argued against Brexit and the Trump administration, and have pointed out the clear economic damage each will cause to the majority of the public, only to be ignored by the very people they are trying to protect.

In the case of CA, its chief funder, billionaire Robert Mercer is a close friend of Trump's, and vice president Bannon was Trump's chief campaign strategist, whilst multiple documents have revealed that CA also worked for UKIP and the Leave campaign. Thus far then, it seems that the ultra rich, who have obvious motivations for trying to promote right wing parties to power, are those that are wielding their financial clout to microtarget ordinary people, for their own selfish gain. Indeed, in the UK, these ultra rich people are the very same who campaigned for a Brexit supposedly for the people; MP Rees-Mogg and Arron Banks (Leave.EU cofounder) were two of the loudest voices, who conveniently hold their vast wealth offshore (Garside, Osborne, and MacAskill, 2017). Their hedge funds operate via tax havens that stand to benefit enormously from a lack of EU regulations and taxation, and the pair, along with many other right wing rich, are in line for a 'huge personal windfall' (Shubber, 2018) after Brexit, thanks to their investments that hinge on Britain leaving the world's most powerful economic bloc. Microtargeting also has further implications for the agendas of purposeful disinformation Russia has embarked on, by enhancing the ability of the state to tailor disinformation to make it more believable for viewers. In the run up to the European elections 250 million Europeans were exposed to location tailored social media disinformation, (Boffey, 2019), but as with microtargeting, it is near impossible to gauge the exact impact of disinformation campaigns.

Attempting to tamper with the free will of voters via political microtargeting is grossly unethical, but political consultants would counter that it is unreasonable to demand businesses to forego potential profits by preventing their use of targeted ads; in the case of political consultants their profits are dependent on their clients winning. Yet whilst Cadbury's

may target their ads at demographics more likely to eat chocolate, there is exponentially more danger in political targeting, where the future of society hinges on voter choices. There is no clear consensus in the literature for the effectiveness of microtargeting; but Linden (2018) makes an excellent point in regards to Bond et al's 2012 study. The small 0.39% effect on voter behaviour translates to 282,000 adjusted votes in the 61-million-person trial, and applying this rate to the US population would result in approximately 1.283 million adjusted votes. In the case of the 2016 Presidential election that Clinton lost by 77,000 votes, CA's work in microtargeting on behalf of the Trump campaign, may well have proved pivotal in his win. Political microtargeting encompasses multiple fields of political science, data science, statistics and psychology; and the answer of how ethical it is is an incredibly complex one; it is also important to note that CA's story went viral largely on the basis that they had illegally obtained unconsented Facebook data, not on the basis of political microtargeting. So there are multiple levels of ethics in political microtargeting that need to be explored; perhaps a field that encourages methodological and rigorous thinking over relentless progress and technological innovation might provide a clearer answer. Philosophy would suggest employing a utilitarian or deontological framework to search for answers, with the latter being more suitable (Gizzi,2018) as it is based on morality of individual actions rather than satisfaction maximisation. A logical view is that 'data is morally neutral; the tool is morally neutral; it is the application that matters' according to CA whistleblower Wylie (2018).

Concluding Remarks

CA exploited data loopholes in Facebook's own personal policies which have supposedly since been expanded and reinforced according to CEO Zuckerberg's promises when he was grilled by Congress, and they were also slapped with a $5 billion fine for their role in the CA scandal. The CA scandal hastened the implementation of Europe's GDPR regulations, which may have prevented the scandal in the first place had they been set up earlier (The Economist, 2018) though ironically, Britain's implementation of it may be at risk thanks to Brexit. Social media datafication is rising at an exponential rate, thus there remains vast scope for literature to examine government regulations and economic policy in preventing both the use of unconsented data, and political mass manipulation. Indeed, CA whistleblower Kaiser (2019) makes the point that "Our data is the world's most valuable asset, we're the ones who created it and yet we have no rights over it". A first step may lie in simply making the public aware that any of their seemingly innocent social media activity can be analysed easily to build a personality of themselves; the second should perhaps involve making them aware of how this profiling is used in targeted advertising. A bolder approach would advocate the break up of the titans of big tech, largely on the basis of monopolistic economic structures (Foroohar, 2019) in the tech market leading to the so called FAANG companies paying minuscule sums of tax whilst also avoiding regulations; indeed, Facebook's fine was small change compared to its revenues.

As discussed, microtargeting enhances disinformation campaigns, which will 'reduce the common ground upon which reasoned debate, based on objective facts can take place' (Boffey, 2019); with the 2020 US presidential elections about 7 months away, "this is a very scary prospect, something radical needs to be done about it, and fast" according to Patrick Steele, ex-head of MI6's Russia department (Cadwalladr, 2020). Bunting (2015) asserts that 'Vibrant democracy requires that citizens remain highly informed and can voice their opinions through voting', but political microtargeting works against these pillars, and whilst

it may win campaigns, it will 'ultimately lead to the undermining of democracy'. CA has since shut down thanks to the scandal; but another firm has been born, utilising the same pioneering behavioural data science methods, Data Propria has been set up by multiple CA former employees (Lapowsky, 2018). The company is working on the US 2020 presidential election- for Trump's campaign. CA is just one of a global industry of behavioural data science firms whose expertise lie in mass manipulation; that we have not heard of the others is simply suggests they haven't been caught yet, a sobering thought. Overall then, democracy, and particularly democracy in the most powerful country in the free world, is truly in danger from data:

'Power is in tearing human minds to pieces and putting them together again in new shapes of your own choosing' (Orwell, '1984', 1949).

Bibliography

Davenport, T. and Patil, D., 2020. '*Data Scientist: The Sexiest Job Of The 21st Century'*. [online] Harvard Business Review. Available at: https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century [Accessed 21 February 2020].

Rafter, D. 2019. *'2019 Data Breaches: 4 Billion Records Breached so far'*. [online] Norton.com. Available at https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html [Accessed 21st Feb, 2020]

Gibney, E. 2018. *'The Scant Science behind Cambridge Analytica's Controversial Marketing Techniques'*. [online] nature.com. Available at https://www.nature.com/articles/d41586-018-03880-4 [Accessed 21st Feb, 2020]

Prokop, A. 2018. '*Cambridge Analytica Shutting Down: The Firm's Many Scandals, Explained'*. [online] vox.com. Available at https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-CA-trump-russia-mueller [Accessed 21st Feb, 2020]

Bond, R., Fariss, C., Jones, J. et al. 2012. *'A 61-million-person experiment in social influence and political mobilization'*. [online] Nature 489, 295–298 (2012). Available at https://doi.org/10.1038/nature11421 [Accessed 21st Feb, 2020]

Naur, P. 1974. '*A Concise Survey of Computer Methods'*. 1st Edition, Petrocelli Books. Section 1.2.

Tolle, K., Tansley, D. and Hey, A. 2011. *'The Fourth Paradigm: Data-Intensive Scientific Discovery'*. [online] *Proceedings of the IEEE*, 99(8), pp.1334-1337. Available at: https://www.researchgate.net/publication/260686305_The_Fourth_Paradigm_Data-Intensive_Scientific_Discovery_Point_of_View [Accessed 8 March 2020].

Cukier, K. and Mayer-Schoenberger, V. 2013. *'The Rise of Big Data: How It's Changing the Way We Think About the World*'. [online] Foreign Affairs 92, no. 3 28-40. Accessed Feb 21, 2020. Available at www.jstor.org/stable/23526834.

Graham-Harrison, E. and Cadwalladr, C. 2020. '*Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach'*. [online] The Guardian. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [Accessed 26 February 2020].

Blei, D. and Smyth, P. 2017. *'Science and Data Science'*. [online] Proceedings of the National Academy of Sciences, 114(33), pp.8689-8692. Available at https://www.pnas.org/content/114/33/8689 [Accessed 26th Feb, 2020]

Osborne, H. 2020. '*What Is Cambridge Analytica? The Firm at the Centre of Facebook's Data Breach'*. [online] The Guardian. Available at: https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach [Accessed 21 February 2020].

Hern, A. 2020. '*How to Check Whether Facebook Shared Your Data With Cambridge Analytica'*. [online] The Guardian. Available at:

https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica> [Accessed 2 March 2020].

Boldyreva, E. 2018. '*Cambridge Analytica: Ethics and Online Manipulation with Decision-Making Process'*. [online] Available at: https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process [Accessed 27 February 2020].

Lewis, P. and Hilder, P. 2020. *Leaked: Cambridge Analytica's Blueprint for Trump Victory*. [online] the Guardian. Available at: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory [Accessed 22 February 2020].

Bradshaw, P. 2020. *The Great Hack Review – Searing Exposé of The Cambridge Analytica Scandal*. [online] the Guardian. Available at: https://www.theguardian.com/film/2019/jul/23/the-great-hack-review-cambridge-analytica-facebook-carole-cadwalladr-arron-banks [Accessed 21 February 2020].

Kosinski, M., Stillwell, D. and Graepel, T. 2013. *'Private traits and attributes are predictable from digital records of human behaviour'*. [online] Proceedings of the National Academy of Sciences. 110(15), pp.5802-5805. Available at https://www.pnas.org/content/110/15/5802. [Accessed 26th Feb, 2020]

Resnick, B. 2020. '*Cambridge Analytica's "Psychographic Microtargeting": What's Bullshit And What's Legit'*. [online] Vox.com. Available at: https://www.vox.com/science-and-health/2018/3/23/17152564/cambridge-analytica-psychographic-microtargeting-what [Accessed 26 February 2020].

Matz, S., Kosinski, M., Nave, G. and Stillwell, D. 2017. '*Psychological targeting as an effective approach to digital mass persuasion'*. [online] Proceedings of the National Academy of Sciences. 114(48), pp.12714-12719. Available at: https://www.pnas.org/content/114/48/12714 [Accessed 8 March 2020].

Kalla, J. and Broockman, D. 2017. *'The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments'*. [online] American Political Science Review. 112(1), pp.148-166. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042867 [Accessed 8 March 2020].

Garside, J., Osborne, H. and MacAskill, E. 2020. '*The Brexiters Who Put Their Money Offshore'*. [online] The Guardian. Available at: https://www.theguardian.com/news/2017/nov/09/brexiters-put-money-offshore-tax-haven [Accessed 21 February 2020].

Shubber, K., 2020. '*Jacob Rees-Mogg's "Huge Personal Windfall" After Brexit'*. [online] Financial Times. Available at: https://ftalphaville.ft.com/2018/02/08/2198570/jacob-rees-moggs-huge-personal-windfall-after-brexit/ [Accessed 8 March 2020].

Boffey, D. 2020. '*241M Europeans 'May Have Received Russian-Linked Disinformation'*. [online] the Guardian. Available at: https://www.theguardian.com/world/2019/may/08/241m-europeans-may-have-received-russian-linked-disinformation [Accessed 26 February 2020].

Linden, S. 2020. '*Psychological Weapons of Mass Persuasion'*. [online] Scientific American. Available at: https://www.scientificamerican.com/article/psychological-weapons-of-mass-persuasion/ [Accessed 5 March 2020].

Gizzi, D. 2020. '*The Ethics of Political Micro-Targeting'*. [online] Medium. Available at: https://medium.com/datadriveninvestor/the-ethics-of-political-micro-targeting-c3b0be245607 [Accessed 21 February 2020].

The Economist. 2020. '*Britain Moves to Rein in Data-Analytics'*. [online] Available at: https://www.economist.com/britain/2018/03/28/britain-moves-to-rein-in-data-analytics [Accessed 8 March 2020].

Cadwalladr, C. 2020. '*Fresh Cambridge Analytica Leak Shows Global Manipulation Is Out of Control'*. [online] the Guardian. Available at: https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation [Accessed 26 February 2020].

Bunting, Luke. 2015. *'The Evolution of American Microtargeting: An Examination of Modern Political Messaging'. [online]* Butler Journal of Undergraduate Research. Vol.1, Article 2. Available at: https://digitalcommons.butler.edu/bjur/vol1/iss1/2 [Accessed 5th March 2020]

Lapowsky, I. 2020. '*Data Propria Is a New Firm From A Cambridge Analytica Alum'*. [online] Wired. Available at: https://www.wired.com/story/data-propria-data-cambridge-analytica/ [Accessed 5 March 2020].

Orwell, G. 2004. '*Nineteen Eighty-Four'*. Penguin Classics, pp.Part 3, Chapter 3.