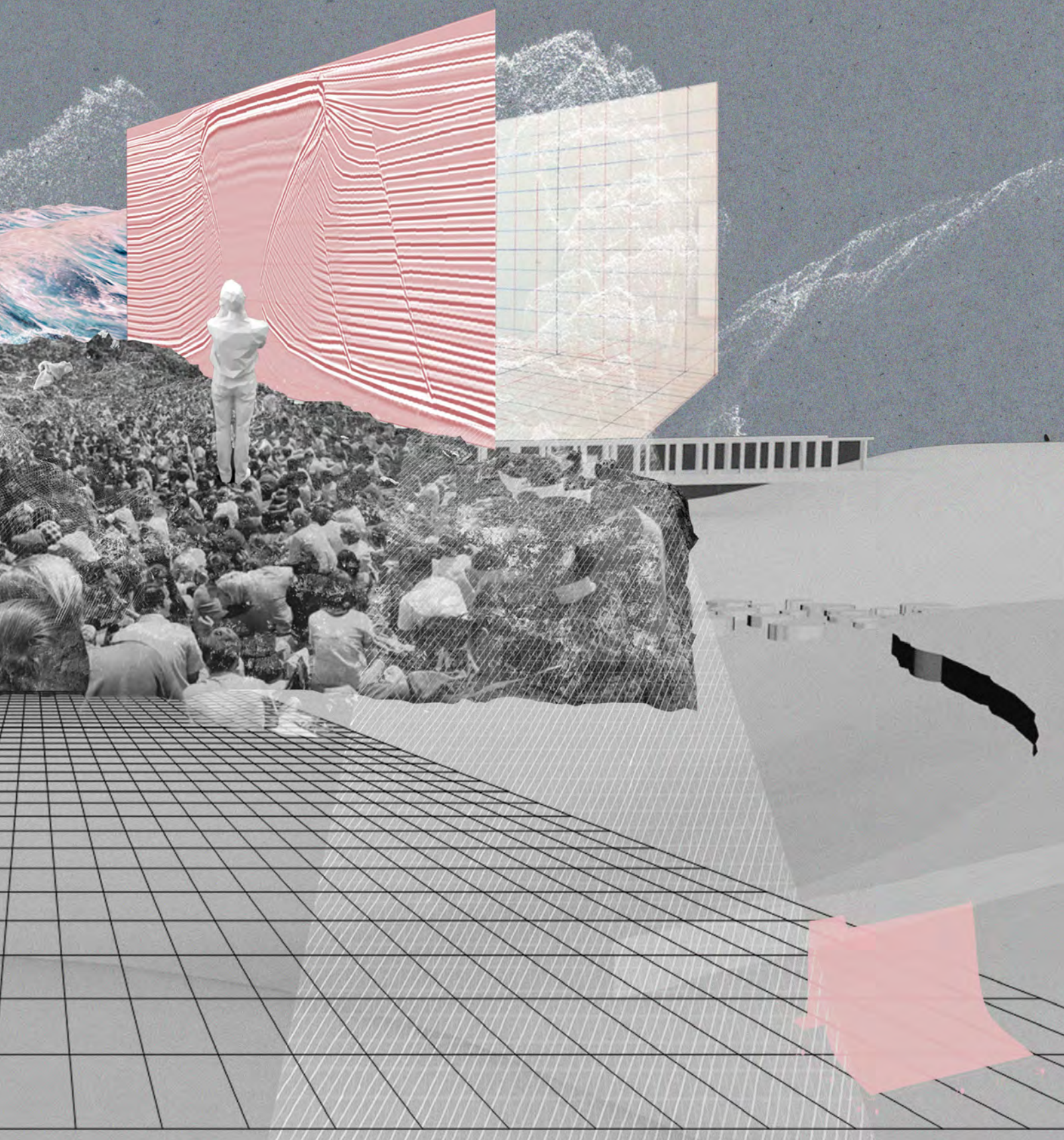**TACTICAL TECH**

Personal Data: Political Persuasion
Inside the Influence Industry. How it works.

Personal Data: Political Persuasion

Inside the Influence Industry. How it works.

By Tactical Tech's Data and Politics team
Published March 2019

TACTICAL TECH

Making sense of
the digital

Authors
Varoon Bashyakarla
Stephanie Hankey
Amber Macintyre
Raquel Rennó
Gary Wright

Creative Direction
Stephanie Hankey

Editor
Christy Lange

Copy Editor
Michael Runyan

Graphic Design
Yiorgos Bagakis

Cover and Illustrations
Maria Kassab

Design Support
Philipp Dollinger

Research Support
Nicole Ayo von Thun
Sascha Gubskaya
Morana Miljanovic

Communications
Daisy Kidd

Tactical Tech's country-study partners:
Boo Su-Lyn (Malaysia)
Bruna Martins dos Santos & Joana Varon, Coding Rights (Brazil)
Cédric Laurant, Ernesto Ángeles Guerrero, José Alberto, Hernández Jiménez & Sebastián Irigoyen, Artículo 12 (Mexico)
Claudio Agosti & Fabio Chiusi (Italy)
Colin J. Bennett & Robin M. Bayley (Canada)
Elonnai Hickok (India)
Eticas Foundation (Catalonia)
Grace Mutung'u (Kenya)
Jeff Chester & Kathryn Montgomery, Center for Digital Democracy (United States)
José Luis Peñarredonda, Fundación Karisma (Colombia)
Judith Duportail (France)
Marianela Milanes, Asociación por los Derechos Civiles (Argentina)
Romina Garrido, Fundación Datos Protegidos (Chile)

For the online version of this guidebook visit tacticaltech.org/#/projects/data-politics

Licenses for further distribution of this guide are available on request at ttc@tacticaltech.org

Thanks to The Tactical Tech team for support and our project partners and collaborators

Contents

Introduction

The scandal surrounding Cambridge Analytica that broke on 17 March 2018 was a watershed moment. For many voters, it created a unique insight into how their data was being traded and utilised to target them for political influence: voters realised the effects the technologies were having on them.

Despite widespread global attention, there is still very little known about the techniques that are applied to sway citizens' political views by leveraging the data they give away. While much of the media coverage focused on Cambridge Analytica's use of psychometric profiling, this was not the only technique they used; in fact, there were many. Furthermore, as their staff took the stand in a series of enquiries by the UK parliament, they pointed out that these methods were fairly commonplace within a vast industry of influence.[2] Beyond 2018, understanding this industry and how it works is essential for deciding how the industry should be regulated and learning how effective its techniques really are.

The Data and Politics team at Tactical Tech spent twelve months investigating these technologies and methods: who is selling them, what they promise and how exactly they extract value from personal data. The team has attended events, interviewed practitioners and worked with partners spanning multiple countries[3] to piece together a puzzle of the workings of the industry and the mechanisms they use. The result of our research is a unique overview of the who, what and how of the influence industry, with a focus on the different ways that personal data is used in efforts to understand, engage and influence citizens in political campaigns. Going beyond the more widely covered services of Facebook that enable political parties to target users based on their personal data, we look at the lesser covered but equally widespread techniques that use personal data for political campaigning. This guide focuses on the use of personal data in political campaigns and how it works and is accompanied by a visual gallery that focuses on what's for sale.[4] It is only by getting a view of the breadth, depth and scale of the techniques that we can begin to understand their relevance to the current political moment.

How do they work?

Data-driven technologies are an inevitable feature of modern political campaigning. Some argue that they are a welcome addition to politics as normal and a necessary and modern approach to democratic processes; others say that they are corrosive and diminish trust in already flawed political systems. The use of these technologies in political campaigning is not going away; in fact, we can only expect their sophistication and prevalence to grow. For this reason, the techniques and methods need to be reviewed outside the dichotomy of 'good' or 'bad' and beyond the headlines of 'disinformation campaigns'.

All the data-driven methods presented in this guide would not exist without the commercial digital marketing and advertising industry. From analysing behavioural data to A/B testing and from geotargeting to psychometric profiling, political parties are using the same techniques to sell political candidates to voters that companies use to sell shoes to consumers. The question is, is that appropriate? And what impact does it have not only on individual voters, who may or may not be persuaded, but on the political environment as a whole?

The practice of political strategists selling candidates as brands is not new. Vance Packard wrote about the 'depth probing' techniques of 'political persuaders' as early as 1957. In his book, 'The Hidden Persuaders', Packard described political strategies designed to sell candidates to voters 'like toothpaste', and how public relations directors at the time boasted that 'scientific methods take the guesswork out of politics'.[5] In this sense, what we have now is a logical progression of the digitisation of marketing techniques and political persuasion techniques.

Digging deeper into the differences that the new technologies bring—such as the granularity, scale and speed at which they can target messages—is an essential first step. Our research reveals more about how various methods work, how they have been used to-date and how they could be used in the future. This helps to show which attributes may differentiate between methods which are relatively benign and which need curtailing in the context of political persuasion. Detailing them enables checks and balances to be put in place that ensure that political actors with varying value systems, working in different political contexts and at different political moments, stay within ethical lines and do not create unjust advantages and inequities. Such an independent, in-depth and nuanced knowledge of the tools at play is crucial for making decisions about how to keep elections and political processes open, free and fair.

The challenges of getting inside the influence industry

Tactical Tech's research project 'Inside the Influence Industry' reflects what can be seen 'from the outside', working on multiple levels, but never within political campaigns or for the influence industry itself. For this reason, any gaps and anomalies in the research are in and of themselves meaningful: they represent the parts of the industry and the practices that cannot be discovered from the outside. The project shows what can be found as technologists and researchers working external to the industry and, perhaps more poignantly, as determined voters.

Our research was carried out at an international level by the Data and Politics team at Tactical Tech and at a national level in collaboration with our partners in Argentina, Brazil, Canada, Catalonia, Chile, Colombia, France, India, Italy, Kenya, Malaysia, Mexico and the US.[6] These studies highlight how the variations in electoral and data protection laws impact what can be done in different contexts. They also draw attention to the differences in the extent to which data-driven technologies are used, as well as the similarities. For example, WhatsApp is widely used for political outreach in Asia and Latin America but less so in Europe or North America. By contrast, in all the contexts we researched, political campaigns made use of the data-driven targeting services of large-scale platforms, such as Google and Facebook's micro-targeted advertising services.

The influence industry is made up of a wide range of digital and political strategists and consultants, technology services providers, data brokers and platforms. Some companies are specifically focused on analysing and utilising personal data for

political campaigns; others are data brokering services that are utilised by political campaigns, as well as other clients who use their services for marketing, advertising and sales for a range of products and services not related to politics.

The United States can be seen as the industry's primary innovator, with the most dominant companies exporting their technologies and the largest political campaign budgets for experimentation. The fact that data-driven campaigning techniques originated in the US, with George W. Bush's 2004 presidential campaign[7] and Barack Obama's 2008 presidential campaign[8] paving the way, has also set precedents in the way that data is used by campaigns in other countries.

Broadly speaking our research showed that at this point in its development, the use of data-driven political campaigning techniques worldwide largely originates from and is facilitated by the widespread export of technologies that are developed in the US and then adapted and iterated into local contexts. In researching the practices, we found that the data companies and the political parties that purchase their services vary in their degrees of openness and transparency.

Some companies offer online demos of their technologies and/or present case studies of their political work, while others do not represent their political work or clients at all. In these cases, we found their work through journalistic research, industry events, interviews or by discovering that their services were used by political clients (in some cases this may even be something they themselves were not aware of as they buy and sell data analysis to a broad range of clients outside the political domain).

The same varied approach is true of political parties: some talk openly to the media and researchers about their practices, others refuse interviews, obscuring the nature of their activities by working through intermediaries. There are multiple reasons for this inconsistent approach to transparency, from intellectual property and trade secrets to the discreet nature of political strategies. In some cases the reasons are more banal, including the fact that decision-making about detailed data and advertising strategies can be far removed from politicians during the height of a campaign.

"Despite widespread global attention, there is still very little known about the techniques that are applied to sway citizens' political views by leveraging the data they give away."

More information is readily available in the political context of the US, with a variety of case studies, journalistic reports and more in-depth academic research published. The variations in openness about, and documentation of these methods, particularly outside the US, creates significant challenges in conducting research and leaves a gap in knowledge and understanding of the effects of these technologies as they are exported and adapted in different political contexts. As this technology proliferates, greater openness is necessary internationally and more comparative research is essential for assessing the impact on democratic processes.

What is political data?

Tactical Tech identified a multitude of technologies that make use of personal data at some point in the process of political campaigning, from building repositories of voter databases as a competitive edge against the opposition to learning about what voters are motivated by in order to tailor messages to what they want to hear.

We looked at personal data in its broadest sense, including any data that can be used to identify or re-identify an individual,[9] and any large-scale data sources that are produced by the behaviours and actions of individuals. This includes things like data generated by surveys or online polls, in chatrooms or on social media, and even data generated passively, such as satellite imagery of buildings and homes which can be used to make assertions about occupants' political positions.[10] Similarly, we took a broad approach to the term 'political data': going outside the current legal definition of sensitive data about individuals' 'political opinions'[11] to incorporate a wider range of assertions that are made when interpreting the political relevance of data and the nature of consent—for example, how a data point on the type of car you own or the fact that you have a low credit rating may be utilised to interpret and predict your political opinions.

Getting to know the methods

Over the course of our research, we organised the use of political data in three categories: asset, intelligence and influence. These themes are used to organise the techniques in this guide. We categorise them not by how they are commonly referred to in the industry, but rather based on their political value. This is an intentional decision that attempts to assert a key finding of our research. Thinking about data technologies in these terms allows us to not only imagine them as a set of tools with one end result—persuading an individual to vote a certain way—but also to evaluate each method individually, for its own strategic value. Each one is a tool that can be leveraged at any point in the process with or without other digital technologies. For example, mass digital message testing could then be used to tailor a speech given on television. The key factor is that a technique could be used by itself or in combination to give a political campaign its leading edge.

As with all categorisations, there are no perfect solutions. Some methods do not fit neatly into one category. In deciding what methods to include, we used simple criteria:

↘ Does the method somehow utilise personal or individual data in a political campaign?

↘ Can the method be found in more than one case or offered by more than one service provider?

↘ Is the method stand-alone (i.e. can it be used by itself without any of the other methods)?

This guide categorises data-driven campaigning methods to loosely reflect how value is created along the data pipeline, from acquisition (asset), to analysis (intelligence) to application (influence).

Data as a political asset: valuable sets of existing data on potential voters exchanged between political candidates, acquired from national repositories or sold or exposed to those who want to leverage them. This category includes a wide range of methods for gathering or accessing data, including consumer data, data available on the open internet, public data and voter files.

Data as political intelligence: data that is accumulated and interpreted by political campaigns to learn about voters' political preferences and to inform campaign strategies and priorities, including creating voter profiles and testing campaign messaging. This includes techniques such as A/B testing, digital listening and other techniques for observing, testing and analysing voters and political discussions.

Data as political influence: data that is collected, analysed and used to target and reach potential voters with the aim of influencing or manipulating their views or votes. This includes a diverse set of micro-targeting technologies designed to reach individual types and profiles, from psychometric profiling to Addressable TV.

The artful use of these techniques in unison has been claimed by some campaigners to be key to their success.[12] Whilst the methods we have identified can at times be applied together, or even in combination with analogue campaigning techniques, we have examined them here individually to describe how they work, how they use personal data, and what the potential consequences of their use might be. It is only then that their political relevance and value can be truly understood.
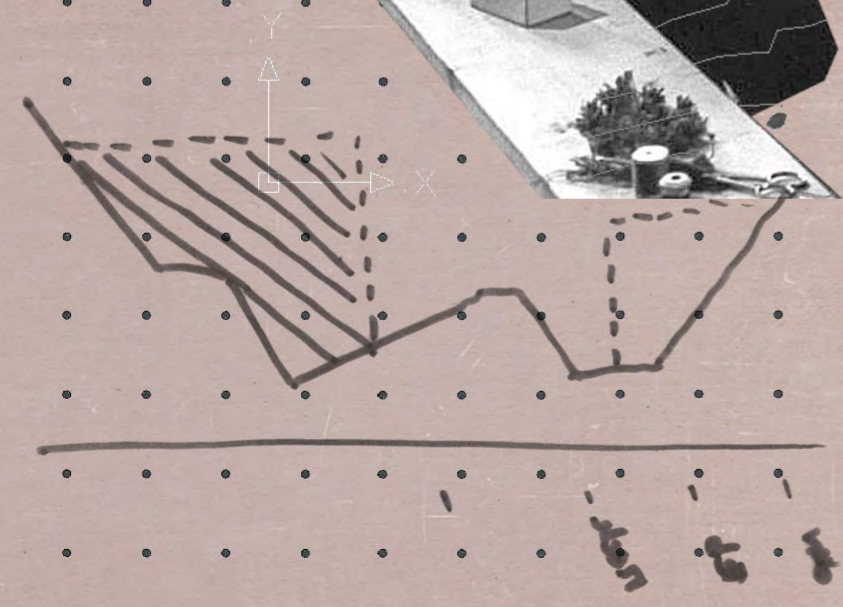
1
'Oral Evidence - Fake News - 27 Feb 2018', accessed 12 March 2019, https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-andsport-committee/fake-news/oral/79388.html.

2
See testimony of Brittany Kaiser by the Commons Select Committee on Fake News, 'Brittany Kaiser Written Evidence Published - News from Parliament', UK Parliament, accessed 12 March 2019, https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-newskaiser-written-evidence-17-19/.

3
See Tactical Tech's country studies at https://ourdataourselves.tacticaltech.org/chapters/dap-ii-country-studies/.

4
See https://tacticaltech.org/projects/data-politics/.

5
Vance Packard, The Hidden Persuaders, New York: D. McKay Co, 1957.

6
The country study for the UK was researched and written by Tactical Tech. For the list of other country study contributors, see page 2.

7
Newman, Bruce. 2016. The Marketing Revolution In Politics: What Recent U.S. Presidential Campaigns Can Teach Us About Effective Marketing. Toronto Buffalo London: Rotman-UTP Publishing.

8
Ambinder, Marc. 'Exclusive: How Democrats Won The Data War in 2008', 5 October 2009, https://www.theatlantic.com/politics/archive/2009/10/exclusive-how-democrats-won-the-data-war-in-2008/27647/.

9
See for example, the ICO definition that defined personal data as any data that can identify an individual; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

10
'HaystaqDNA', accessed 14 March 2019, https://haystaqdna.com/author/haystaq/.

11
See the EU's definition of sensitive data, including 'political opinions' at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/howdata-my-religious-beliefs-sexual-orientation-health-political-views-protected_en.

12
Dominic Cummings, 'On the Referendum #20: The Campaign, Physics and Data Science – Vote Leave's "Voter Intention Collection System" (VICS) Now Available for All', Dominic Cummings's Blog, 2016. accessed 12 March 2019, https://dominiccummings.com/2016/10/29/on-thereferendum-20-the-campaign-physics-and-data-science-vote-leaves-voter-intention-collection-system-vics-now-available-for-all/.
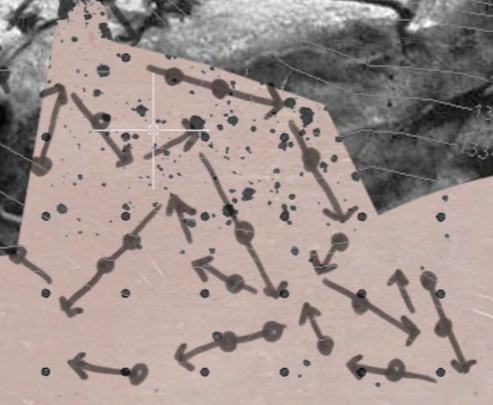
Data as
an Asset

As massive amounts of data on individuals is accumulated and used in political processes, it creates significant assets and liabilities. In the race to accumulate data on voters, campaigns rely on purchasing data from the commercial sector as well as collecting individual data through campaign apps and even, at times, speculation about data 'donations' from the business and public sector in different contexts. Voter data can also become a liability as it is leaked or exposed for a wide variety of actors to utilise.

When data is purchased on the open market, it can mean that political parties with more money or access to resources can gain advantages, potentially changing who can participate in a race. The accumulation and intra-party trade of data over time can also create inequities between candidates and across political parties.

Voter databases can become assets, traded or 'gifted', creating significant advantages across political parties and elections. The long-term value of this data, particularly if the quality of it erodes over time, is debated within the industry. Outside of the official political party system, other actors, for example those with private and business interests in political power, can also accumulate their own data assets that could then be gifted or sold at a reduced price to the right candidate.

Consumer Data: The fuel of digital campaigns

"Our goal is to connect every piece of data with every person on the planet with every available use case that matters…If we can accomplish that, amazing things can happen."

SCOTT HOWE, PRESIDENT & CEO, ACXIOM [1]

What is consumer data?

Broadly, consumer data is defined as information that will help a service provider, merchant or marketer better understand the needs and preferences of individual customers or groups of customers. Consumer data helps data brokers create detailed profiles of certain audiences, which are subsequently sold or made available to companies that want to target their customers—or in the political context, potential voters—according to their perceived preferences or attributes.

In its 'Audience Lookbook', the data broker Experian claims its US database has access to 'the freshest data' from 'more than 300 million individuals and 126 million households, more than 50 years of historical information, thousands of attributes to reveal demographics, purchasing habits, lifestyles, interests and attitudes'.[2] Using that data, Experian boasts it can 'address 85% of the US, link to 500 million email addresses'[3] and segment individuals into 71 unique types according to categories like 'Financial Personality' and 'Ethnic Insight'. Experian claims this data will help companies reach the 'right audiences' with the 'best messages'.[4] But the company is not only offering their data to marketers: their 'Political Personas' segmentation defines categories like 'Super Democrats' and 'Green Traditionals' to give political parties insights into issues, attitudes and trends among voters.[5] Consumer data is not just touted as the key to understanding buyers or customers, but also a key to unlocking valuable political audiences.

The vast amount of consumer data that is available today is growing exponentially. According to a Demos report on the future of political campaigning, IBM estimates that around 2.5 quintillion bytes of data are produced each day from almost every sector of the economy.[6] The kinds of data being aggregated ranges from basic attributes such as your age or family size, to minute details like what types of movies you like or the kind of car you drive.[7] In fact, General Motors has patented the usage of 'vehicle trace data', ranging from driving habits to in-car media consumption to targeting advertising at the vehicle.[8] In a deep-dive on this topic, technologist and researcher Wolfie Christl's report 'Corporate Surveillance in Everyday Life' categorises consumer data into several flavours, including: volunteered data, observed data, actual data and modelled/inferred data, which is based on analysed activities and behaviours.[9] A vast range of industries serve as sources, including digital platforms like Google, Facebook and Amazon, telecom service providers (SAP, for example, operates an analytics tool which analyses billions of consumer data points from mobile operator networks), media outlets, publishing houses, retailers and financial services like banks and credit agencies.[10] Spotify, for example, not only sells data about its users' listening habits but also insights into its users' moods and locations. In the digital era, digital-driven companies such as internet service providers[11] and vendors of 'smart' devices[12] have also become data brokers in their own right.

How is my consumer data being used in elections?

Consumer data is the fuel of digital-driven campaigning.[13] It drives the various methods and tools with which a political campaign can analyse, segment, target and evaluate voters. Across the globe, political campaigns are increasingly using the data and targeting tools designed for commercial advertising and consumer engagement in order to inform and shape their campaigns.

The main sources of consumer data for political campaigning are:

↘ **Traditional data brokers:** Campaigns can acquire consumer data directly from major data brokers such as Acxiom,[14] Epsilon[15] and Experian (including Brazil-based Serasa Experian, which holds the largest consumer data sets in the Latin American region[16]) all of whom count political parties among their clients. Following the UK's 2017 general election, the website Emma's Diary, which provides 'baby & pregnancy advice for mums to be',[17] was fined by the country's Information Commissioner's Office (ICO) for breaching data protection laws by collecting and selling consumer data to the Labour Party, by way of a data supply agreement with Experian.[18] Names of parents, addresses, number of children per household, dates of birth: the website collected and sold over one million records to Experian, who, in turn, was building a database for the Labour Party for targeted campaign outreach. This case gained attention due to the ICO's finding that data laws were broken; however, the practice of political parties obtaining consumer data from large data brokering houses is widespread. The UK Electoral Commission's publicly available database on campaign spending shows that both the country's largest political parties spent significant amounts on Experian.[19]

↘ **Internet platforms:** While traditional data brokers are a rich source of consumer data for political parties, large internet platforms have caught up with the broker industry. Companies like Facebook and Google and their product ecosystems (such as Gmail, YouTube, Instagram and Facebook Messenger), enable advertisers and marketers to reach their users and gain insights about them. In mid 2018, the total number of monthly users of all of Facebook's services, including WhatsApp, Instagram and Messenger, was 2.5 billion.[20] Google, meanwhile, claims that eight of its products reach over a billion users each, along with two billion active Android users.[21] Not only do these two companies have enormous userbases, they also dominate the digital advertising landscape, with close to 65% of the market share in 2017.[22] Their business models rely largely on enabling their customers to target ads to their users. The primacy of Google and Facebook is also enhanced by the ability of traditional data brokers to merge their consumer data into them: audience data was provided by both Acxiom[23] and Serasa Experian[24] for Facebook's marketing platform. With the combined power of reach and the wealth of consumer data available to them, internet platforms serve political campaigns on a global scale and provide them with tailored services.

Two powerful techniques offered by the platforms include customer database matching (Facebook's 'custom audiences'[25] and Google's 'customer match'[26]) and extended 'searches' for customers (Facebook's 'Lookalike Audiences'[27] and Google's 'Similar Audiences'[28]). By uploading their customer or supporter list directly, advertisers or political campaigns are able to 'match' these individuals to users on these respective platforms, based on data such as names, phone numbers and email and mailing addresses, and target them with content. With the second technique, both platforms offer a system where their users' activities and attributes are analysed for shared interests and characteristics among an advertiser's or campaign's marketing or outreach list. Once identified, this newly generated audience can be targeted for advertising.

↘ **Political data consultants:** While traditional data brokers and internet platforms count many other kinds of industries in their client base, political consultancy firms, like i360 — a US conservative-leaning data firm largely funded by the Koch brothers[29]—use their knowledge of consumer data especially for political clients and their campaigns. i360 advertises a database of 290 million American consumers and over 700 unique data points; all of which are sourced from 'voter data from every state and multi-source lifestyle and consumer data from top tier providers'.[30] Similarly, Advocacy Data advertises its ability to match a campaign's existing data to consumer data ranging from group memberships, such as gun owners or military veterans, to magazine subscriptions, to financial status and more.[31] Aristotle provides datasets 'complete with donor history, demographics and lifestyle information'.[32] Political data consultants who use consumer data as part of their data strategies have been identified in elections in Brazil,[33] Argentina[34] and India[35] to name a few.

↘ **Other sources:** Beyond typical commercial data, political data consultants are turning to more novel sources to help augment their understanding of voters. The sourcing and analysis of open data has become an asset for political campaigning. As a team of Stanford University artificial intelligence researchers demonstrated, it is possible, for example, to predict demographics and voting patterns in the US based solely on Google Street View images of cars.[36] Their findings include that neighbourhoods with more sedans than pickup trucks were more likely to lean towards the Democratic Party.[37] Satellite data has been actively implemented by political data consultants in their offerings to customers. HaystaqDNA, a data firm that has worked with Barack Obama and Bernie Sanders' campaigns, has analysed satellite images to identify and model owners of solar panels—which can be valuable data for political clients looking to reach voters with an affinity for environmental issues.[38]

Considerations

↘ Consumer data on voters is a key element in data acquisition in political campaigns.

↘ Political campaigns and political candidates can gain an increasingly detailed insight into voters' opinions, needs and leanings on issues, thus informing the campaign about perceived attitudes. A more informed candidate can talk more directly to actual concerns of the voter, and consumer data can improve accuracy.

↘ The ability, in the age of big data, to link and combine consumer data from any number of data sets from numerous companies, platforms, devices and services is establishing a norm where voters are 'constantly surveyed and evaluated, investigated and examined, categorized and grouped, rated and ranked, numbered and quantified, included and excluded'.[39]
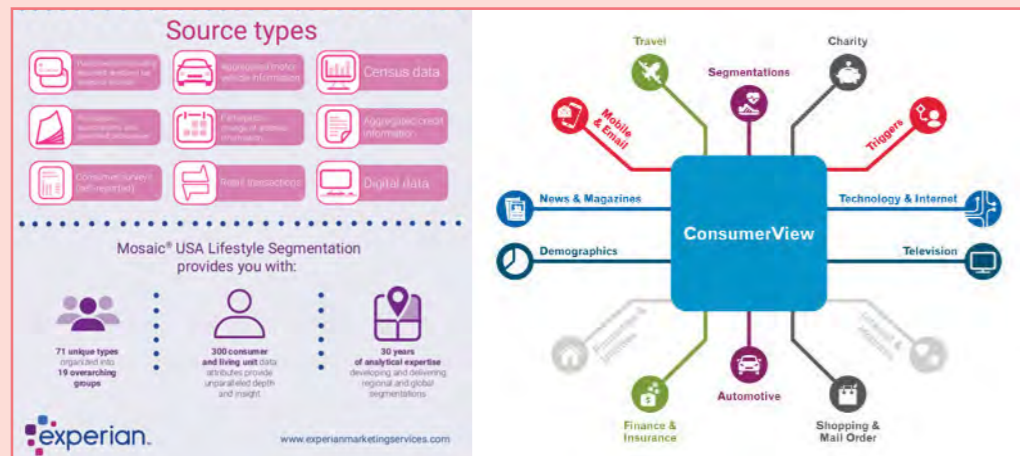
Sources of data and how they are implemented as advertised by Experian.

Source: 'ConsumerView - Data by the Numbers.' Experian Marketing Services, accessed 22 February 2019. https://www.experian.com/assets/marketing-services/infographics/consumerview.pdf (left)

Source: Experian. 'Consumer View Data | Experian Marketing Services,' 2 May 2018. https://www.experian.com/marketing-services/targeting/data-driven-marketing/consumer-view-data.html (right)

SP0349015	Labour Party	UK Parliamentary general election 08/06/2017	Political Party	£24,960.00	31/05/2017	Experian	Sir John Peace Building, Experian Way, Nottingham, NG80 1ZZ, United Kingdom	06/05/2017	Download
SP0223283	Conservative and Unionist Party	UK Parliamentary general election 07/05/2015	Political Party	£21,877.13	30/03/2015	Experian Ltd	Experian Way, Nottingham, NG80 1ZZ, United Kingdom	30/03/2015	Download
SP0349889	Labour Party	UK Parliamentary general election 08/06/2017	Political Party	£21,516.00	25/05/2017	Experian	Sir John Peace Building, Experian Way, Nottingham, NG80 1ZZ, United Kingdom	26/05/2017	Download
SP0349902	Labour Party	UK Parliamentary general election 08/06/2017	Political Party	£17,436.00	28/09/2016	Experian	Sir John Peace Building, Experian Way, Nottingham, NG80 1ZZ, United Kingdom	30/09/2016	Download
SP0223288	Conservative and Unionist Party	UK Parliamentary general election 07/05/2015	Political Party	£16,085.38	27/05/2015	Experian Ltd	Experian Way, Nottingham, NG80 1ZZ, United Kingdom	27/05/2015	Download

A screenshot showing an excerpt of search results after querying the UK's Electoral Commission's public database for party spendings at Experian.

Source: 'The Electoral Commission - Spending on Data Brokers.' Search - The Electoral Commission. Accessed March 7, 2019. http://search.electoralcommission.org.uk/Search/Spending?currentPage=1&rows=30&query=Experian&sort=TotalExpenditure&order=desc&tab=1&closed=common&et=pp&et=ppm&et=tp&et=perpar&et=rd&includeOutsideSection75=true&evt=ukparliament&evt=tp&evt=referendum&evt=europeanparliament&ev=3568&ev=2514&ev=445&ev=410&ev=404&ev=289&ev=281&ev=217&ev=207&ev=205&ev=74&ev=68&ev=62&ev=60&ev=4&optCols=CampaigningName&optCols=FullAddress&optCols=DateOfClaimForPayment

Screenshot of political success stories as advertised by Facebook Business in October 2016. The "Government and Politics" subcategory has since been removed.

Source: 'Success Stories about Facebook Advertising: Government and Politics | Facebook for Business.' Success Stories about Facebook Advertising, 22 October 2016. https://web.archive.org/web/20161022041114/www.facebook.com/business/success?categories[0]=government-politics

The composition of its database for political campaigning, including over 700 consumer data points, as advertised by i360.

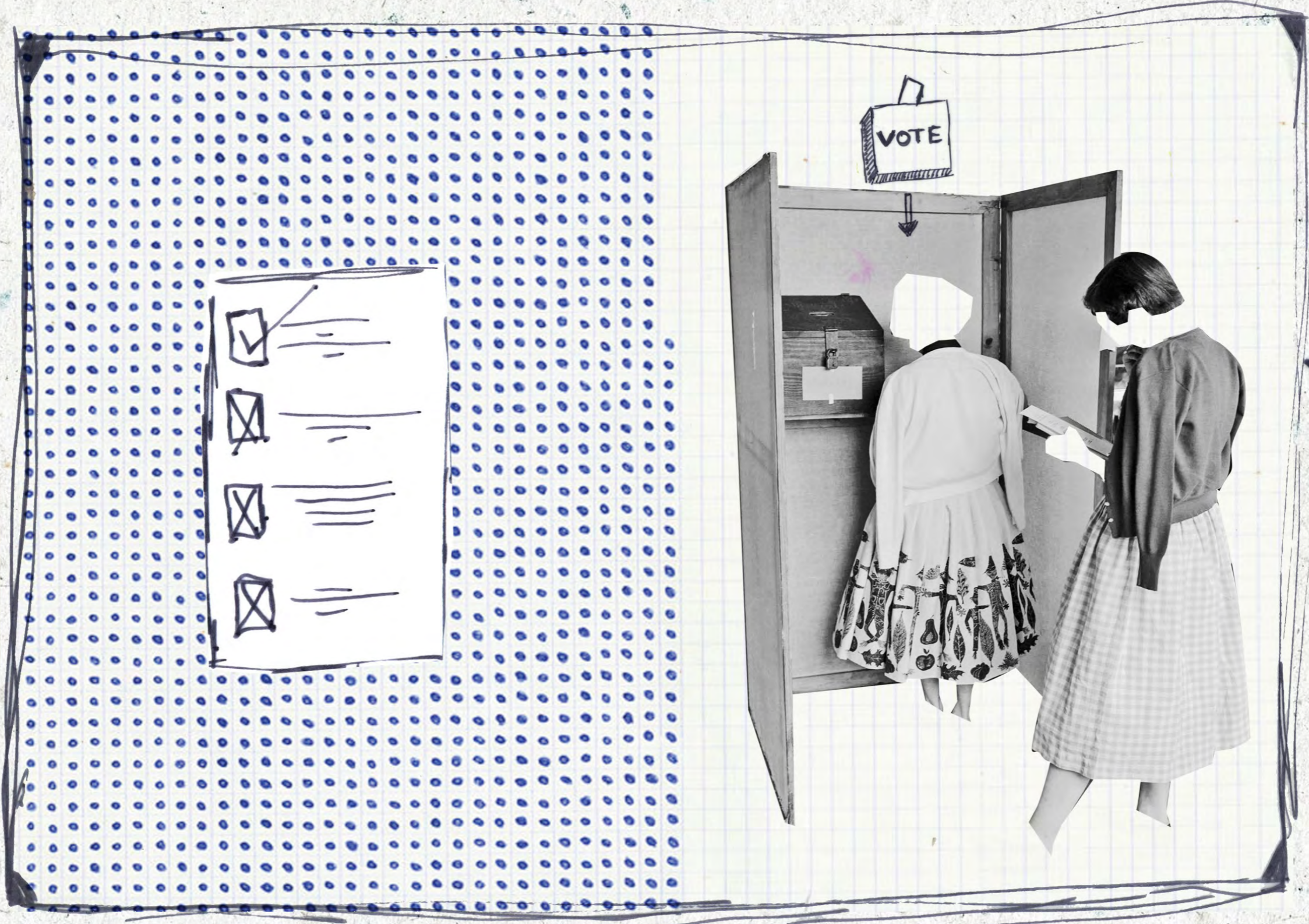*Source: 'The Database - i-360.' i360, accessed 1 March 2019. https://www.i-360.com/the-database/*

"Across the globe, political campaigns are increasingly using the data and targeting tools designed for commercial advertising and consumer engagement in order to inform and shape their campaigns."

1

Acxiom Corporation, Acxiom CEO: 'GDPR Is Just the First Step in the Journey' (YouTube), accessed 26 February 2019, https://www.youtube.com/watch?v=OumaJaBNidY.

2

'Experian Audience Lookbook' (Experian Marketing Services, January 2019), https://www.experian.com/assets/marketing-services/product-sheets/audience-lookbook.pdf.

3

'ConsumerView - Data by the Numbers' (Experian Marketing Services), accessed 22 February 2019, https://www.experian.com/assets/marketing-services/infographics/consumerview.pdf.

4

'Mosaic USA Consumer Lifestyle Segmentation by Experian', accessed 26 February 2019, https://www.experian.com/marketing-services/consumer-segmentation.html.

5

'Experian Audience Lookbook'.

6

Jamie Bartlett, Josh Smith and Rose Acton, 'The Future of Political Campaigning' (DEMOS, July 2018), https://demosuk.wpengine.com/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf.

7

Experian, 'Consumer View Data | Experian Marketing Services', 2 May 2018, https://www.experian.com/marketing-services/targeting/data-driven-marketing/consumer-viewdata.html.

8

Bartlett, Smith and Acton, 'The Future of Political Campaigning'.

9

Wolfie Christl, 'Corporate Surveillance in Everyday Life - How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions' (Vienna: Cracked Labs, 2017), https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.

10

Christl, 'Corporate Surveillance in Everyday Life.'

11

Jon Brodkin, 'Senate Votes to Let ISPs Sell Your Web Browsing History to Advertisers', Ars Technica, 23 March 2017, https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-ispssell-your-web-browsing-history-to-advertisers/.

12

Philippa Lawson, 'The Connected Car: Who Is in the Driver's Seat?' (Vancouver: British Columbia Freedom of Information and Privacy Association, March 2015), https://fipa.bc.ca/wordpress/wp-content/uploads/2015/03/CC_report_lite.pdf.

13

Consumer data usually augments publicly held data, such as census records and voter files.

14

Acxiom Corporation, 'Acxiom - US Products Privacy Policy', accessed 27 February 2019, https://www.acxiom.com/wp-content/uploads/2017/03/US-Products-Privacy-Policy_072516.pdf.

15

Heather Schichtel, 'Epsilon - The Role of Digital Marketing for Political Campaigns', accessed 27 February 2019, https://us.epsilon.com/a-brand-new-view/region/us/the-role-of-digitalmarketing-for-political-campaigns.

16

Raquel Rennó, 'Brazilian Elections and the Public-Private Data Trade', accessed 1 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-brazil/.

17

'Baby & Pregnancy Advice for Mums to Be | Emma's Diary', accessed 26 February 2019, https://www.emmasdiary.co.uk/.

18

'Emma's Diary Fined £140,000 for Selling Personal Information for Political Campaigning', Information Commissioner's Office, 13 August 2018. https://ico.org.uk/about-the-ico/news-andevents/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-forpolitical-campaigning/.

19

The Electoral Commission, 'Experian - Search - The Electoral Commission', accessed 1 March 2019, http://search.electoralcommission.org.uk/Search/Spending? currentPage=1&rows=30&query=Experian&sort=TotalExpenditure&order=desc&tab=1&open=filter&et=pp&et=ppm&et=tp&et=perpar&et=rd&includeOutsideSection75=true&evt=ukparliament&evt=referendum&optCols=CampaigningName&optCols=ExpenseCategoryName&optCols=FullAddress&optCols=AmountIn England&optCols=AmountInScotland&optCols=AmountInWales&optCols=AmountInNorthernIreland&optCols=DateOfClaimFor Payment&optCols=DatePaid.

20

'Facebook, Inc. Second Quarter 2018 Results Conference Call' (Facebook, Inc., 25 July 2018), https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q2/Q218-earnings-calltranscript.pdf.

21

Shoshana Wodinsky, 'Google Drive Is about to Hit 1 Billion Users', The Verge, 25 July 2018, https://www.theverge.com/2018/7/25/17613442/google-drive-one-billion-users.

22

Mathew Ingram, 'Here's How Google and Facebook Have Taken Over the Digital Ad Industry', Fortune, accessed 1 March 2019, http://fortune.com/2017/01/04/google-facebook-ad-industry/.

23

'Acxiom Becomes an Audience Data Provider in Facebook Marketing Partner Program', Acxiom, accessed 1 March 2019, https://www.acxiom.com/news/acxiom-becomes-audiencedata-provider-facebook-marketing-partner-program/.

24

Rennó, 'Brazilian Elections and the Public-Private Data Trade'.

25

'Custom Audiences - Reach Your Customers and Contacts on Facebook', How to reach existing customers with Facebook ads | Facebook Business, accessed March 6, 2019, https://en-gb.facebook.com/business/learn/facebook-ads-reach-existingcustomers.

26

'About the Customer Matching Process', Google Ads Help, accessed March 6, 2019, https://support.google.com/google-ads/answer/7474263?hl=en&ref_topic=6296507.

27

'About Lookalike Audiences for Facebook ads', Facebook Ads Help Center, accessed March 6, 2019, https://www.facebook.com/business/help/164749007013531.

28

'About similar audiences on the Display Network', Google Ads Help, accessed 6 March, 2019, https://support.google.com/google-ads/answer/2676774?hl=en.

29

Mike Allen and Kenneth P. Vogel, 'Inside the Koch Data Mine,' POLITICO, accessed March 7, 2019, https://www.politico.com/story/2014/12/koch-brothers-rnc-113359.html.

30

'The Database - i-360', i360, accessed 1 March 2019, https://www.i-360.com/the-database/.

31

'Data Matching - Advocacy Data', Advocacy Data, 16 September 2015, http://www.advocacydata.com/data-matching/.

32

'Aristotle - Most Comprehensive Voter Data Anywhere', accessed 1 March 2019, http://aristotle.com/data/.

33

Rennó, 'Brazilian Elections and the Public-Private Data Trade'.

34

Varoon Bashyakarla, 'Argentina: Digital Campaigns in the 2015 and 2017 Elections', accessed 1 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-argentina/.

35

Varoon Bashyakarla, 'India: Digital Platforms, Technologies and Data in the 2014 and 2019 Elections', accessed 1 March 2019, https://ourdataourselves.tacticaltech.org/posts/overviewindia/.

36

Linda Poon, 'How Does Your Neighborhood Vote? Find Out From Google Street View', CityLab, accessed 3 May 2018, https://www.citylab.com/transportation/2017/12/google-streetview-data-demographics-cars-research/547436/.

37

Timnit Gebru, Jonathan Krause, Yilun Wang, et al., 'Using Deep Learning and Google Street View to Estimate the Demographic Makeup of Neighborhoods across the United States | PNAS', accessed 4 March 2019, https://www.pnas.org/content/114/50/13108.full.

38

'Home', HaystaqDNA, accessed 5 March 2019, https://haystaqdna.com/.

39

Christl, 'Corporate Surveillance in Everyday Life'.

Voter Files:
Political data about you

"The value of voter files has increased considerably due to advances in methods for collecting, analysing and utilising personal data."

What are voter files?

Voter files are profiles of individual voters that are collected into databases for political campaigning purposes. In its most basic form, a voter file is a list of people who could potentially vote in a given election. This data can also be combined with more detailed information, like party affiliation or registration history. While voter files can vary depending on who produces them—whether electoral administrators, commercial entities or political parties—they often consist of publicly accessible information combined with more detailed data acquired from outside sources and polling.

While governments use voter files for managing voter eligibility, political parties—often in collaboration with digital consultants—use this information in their campaign strategising. Voter files provide a good basis to calculate support for their candidates or causes, as well as to help identify supporters and target undecided voters for conversion, among other uses. Voters' contact information also plays a crucial role in campaign messaging, as it can be used for 'get out the vote' initiatives, to seek volunteers and donations and inform and mobilise supporters.

The value of voter files as an asset to campaigns has increased considerably due to advances in methods for collecting, analysing and utilising vast amounts of personal data. In the last few decades, voter files have benefitted from the market for personal data and have been enhanced by more consequential data sources than the basic information gleaned from electoral rolls. This supplementary data helps campaigns better understand demographic patterns and the voting habits of individuals. Additional data points can be used to create granular, personalised profiles, which are useful in a campaign's predictive analysis. This includes tracking a voter's past turnout and party affiliation to index their sentiment and even utilising relevant financial data such as credit reports, consumer data and other socio-economic indicators.[1] The additional information also helps political campaigns tailor messaging to voters' individual interests.

To illustrate the granularity of data offered by brokers of voter files, the US-based firm HaystaqDNA offers a 'must-have' list of political issues that they claim their data can resolve for individual voters. These include the latest hot-button issues

such as presidential approval and immigration policy, support for activist groups and movements such as Black Lives Matter or Momentum, as well as consumer habits such as being a rideshare user.[2] The scope of voter preferences offered by HaystaqDNA not only shows how voter files now seek to gauge the finer points of voter sentiment, but also exemplifies the shift in the composition of voter files: they are no longer solely developed by political parties, but also by data brokers and digital consultants, many of whom specialise in political data. For example, the data broker NationBuilder offers free voter files for 190 million US voters including their phone numbers, addresses, voter history and sometimes email addresses, acquired from government elections' offices for substantial fees, before being standardised and enhanced by the company. This fine-tuning, they claim, allows them to offer a comprehensive voting history that tracks voter participation in 'any type of election … from football club to parliament'.[3]

Where do they get the data?

Parties can build their voter files from four main sources: electoral registers, polls and surveys, party membership registers, online public data or commercial data brokering companies.

↘ **Voter registration records:** This data can be gathered from an electoral register kept by the local electoral district as a record of who is registered to vote. For example, in the United Kingdom, the local registration officers keep two registers: the electoral register and the open register. Election staff, political parties, candidates and holders of elected office can access this data for 'electoral purposes'.[4] Before elections or referendums the registers are sent to official campaigns for use to send out promotional material.[5] The open register, which citizens can opt out of, can be bought by any person, company or organisation for any reason.[6] Similar data is made available in many countries, varying in accordance with national data protection laws.

↘ **Polls or surveys:** This data is gathered by surveying methods, from simple online polls and political apps to labour-intensive methods such as phone-banking or door-to-door canvassing. Increasingly, contacting voters over the phone relies on technologies such as robocalling. Volunteers will

usually follow a script and ask individuals about their political party preferences or, during referendums, opinions on the ballot question, such as marijuana legalisation. Their responses are then recorded, often using canvassing apps. They may also score other metrics such as 'persuadability' based on their interactions.

↘ **Data brokers:** Data brokers collect voter data and create voter profiles through various means, including the electoral databases mentioned above, surveys and from other commercial data. Data brokers often offer other services for political parties, such as software to manage their databases, referred to as constituent or customer relationship management systems (CRM). Apart from streamlining public data for use in campaigns, NationBuilder can ensure the database has the most up-to-date data and can enhance basic voter information with additional commercial data, such as financial information or hobbies and interests.[7] Another provider, L2, offers basic data as well as occupation, likely primary language and views on hot-button political issues in the US like same-sex marriage and gun control.[8]

↘ **Political party membership**: In many countries, political parties keep registers of the members of their party. Apart from contact information, this history might include an individual's length of membership in the party, their voting records for party leadership, history of volunteering for the party and donations. Parties can use various technological tools to engage with members with the specific aim of collecting further data on them, including through canvassing apps or social media polls. In some countries, such as Kenya, this data must be shared with the government,[9] whereas in others, such as the UK, it is up to the party if they want to publish the data or statistics from the data.[10]

Some examples

In Chile: The electoral register in Chile is freely accessible online as a PDF after the Chilean electoral service declared that it should be made public. The database contains information for all Chileans over 17 years old. In line with standard electoral rolls, this data includes names, unique voting number, gender and address. While regulations prohibit commercial uses of the database, there are few other limitations. Privacy concerns have been raised in response to the publication of this information due to the lack of security around the information and how easy it is to reproduce the database.[11] Further,

Chilean privacy law has not always been enforced in other spheres. Any political campaigning group can use the information as a foundation for their voter files.[12]

In Kenya: There are various sources to help political parties and candidates in Kenya to form their own voter files. In 2017, mass voter registration was carried out by Kenya's Independent Electoral and Boundaries Commission (IEBC).[13] Voters were required to present their national ID card, give fingerprints and have their photo taken at the local polling station. This registration was then made publicly available—usually in printed form, and placed somewhere central to each voting region. If a political candidate wanted the data earlier, they could pay for it. This option was particularly useful as the open publication was delayed for several months, and when it finally appeared was found to be riddled with errors.[14]

In Canada: Political parties in Canada are exempt from privacy laws. Therefore, each political party can keep voter files without needing to adhere to the same laws that regulate businesses' collection of data.[15] By expanding these data sources and developing better analytics, the parties refine their categories of voters according to supporters, non-supporters or undecided. For example, the Conservative Party of Canada use this data to create a scale from -15 to +15 to rate how much an individual supports them, while the Liberal party have a tier system rating from 1 (supporters) to 10 (those who may be hostile).[16] In the deregulated environment there is little transparency about exactly what data the databases contain or what modelling is performed to assess the final ratings of support levels.

In the UK: Each party in the UK maintains its own voter file, therefore they differ greatly depending on the resources and technical expertise of the party itself. The Labour Party has in-house database software called Contact Creator, which contains data on preferences, interests, voting behaviour and socio-economic information.[17] Contact Creator hosts any data collected by phone, email or door-to-door canvassing. The Liberal Democrat's database, Connect, was developed by NGP VAN, the same providers of database software for the Democratic party in the US. Candidates and parties with fewer resources, however, were found to be using much less sophisticated, self-created software and maintained Excel spreadsheets to host supporter information.[18]

- voter_id
- first_name
- middle_name
- last_name
- birth_date
- gender
- turnout2008
- turnout2010
- turnout2012
- turnout2014
- party_affiliation_2008
- party_affiliation_2010
- party_affiliation_2012
- party_affiliation_2014
- party_affiliation (current)
- residential_address
- zipcode
- race, ethnicity (in Florida and North Carolina)

This screenshot from GitHub shows fields belonging to US voter registration data.

Source: https://github.com/ pablobarbera/voter-files/blob/ master/README.md, accessed 11 March 2019.


MODELING ENHANCEMENTS

- Application of Likely Party Modeling from proprietary algorithms developed for L2 to be used in states lacking party registration
- Application of proprietary hot button issue models and L2 private self-reported issue data
- Analysis of family characteristics
- Self-reported views on hot button issues including:
  - Affordable Care Act
  - Election of conservative judges
  - Gay marriage
  - Gun Control
  - Immigration
  - Lawsuit reforms
  - School Choice
  - Social Views
  - Privatizing Social Securiy
  - Abortion
  - and More

A screenshot from the company L2, which offers voter file enhancements including lifestyle data and opinions on political issues.

Source: https://www.l2political.com/products/data/voter-file-enhancements/, accessed 11 March 2019

MUST HAVES

Trump, Views on President	Proud/Embarrassed
Border Wall With Mexico	Support/Oppose
Momentum Voter	Yes
Ban on Muslims Entering U.S.	Support/Oppose
Rideshare User	Yes
Right To Work Laws	Support/Oppose
Black Lives Matter Views	Support/Oppose
Transgender Bathroom Use	Allow/Prohibit
Pathway to Citizenship for Undocumented Immigrants	Support/Oppose

A screenshot from the website of the data firm HaystaqDNA, showing a sample of political data on voters that they offer.

Source: https://haystaqdna.com/politicalhq/, accessed 19 February 2019.

5. What are support levels?

- CIMS follows more than just members or non-members
- Tracks Supporters, Non-Supporters and Undecided
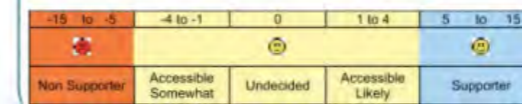
A screenshot of the Canadian Conservative Party's scale of different voter support-levels, ranging from non-supporter (-15) to supporter (+15)

Source: https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-canada.pdf, accessed 7 March 2019.

H Before inputting data, carefully cross reference between the Voter ID sheets and Input data screen the names and polling numbers of the electors you have responses to enter data for.

I Input the responses to the questions answered into the relevant answer boxes alongside the elector's name and polling number. Data must be inputted in the correct format e.g. "L" for Labour, "T" for Conservative, "S" for Liberal Democrat, and in Q3 "Y" for Yes and "N" for no.

A screenshot of the UK Labour Party's voter database Contact Creator shown above has an option to input data generated from campaign contact with individual voters.

Source: The Labour Party. 'Contact Creator, The Essentials', 2017, https://secure.scottishlabour.org.uk/page/-/%282%29%20Images%202018/ Contact%20Creator%20The%20Essentials%202.1.pdf, accessed 11 March 2019

How do I know if I'm part of a voter file?

It is very difficult to determine how you are documented by the various actors and entities that maintain, enhance and distribute voter files. There is rarely any obligation for parties to publish any information regarding their data assets. Nevertheless, there are some sources that could be referenced if you want to check how your personal details are represented. The primary source is the general electoral registers. Each country has different regulations about electoral registers—but those that are public, such as in Chile and Kenya, make it easy to verify what personal data is accessible. The UK and the US similarly make basic information of any registered voter available to the public. A deeper look at communications received from political organisations could additionally provide clues about what personal data has been collected. This includes post and email, as well as visits from canvassers, phone calls or robocalls from political organisations.

Considerations

↘ Voter files allow political parties to understand how to use their limited resources, as voter databases can help decide which messages to deliver to which individuals, depending on their support, opposition or undecided attitude towards the party.

↘ The more detailed databases can help political organisations provide voters with information related to their specific interests such as education, the environment or welfare.

↘ Voter files allow political parties to assess the levels of diversity in their membership and focus outreach efforts on any areas lacking representation.

↘ They can also help political parties better understand their members to develop policy positions based on the interests of local residents.

↘ When national-level voter databases are available to all parties, it helps create an equal playing field; however, political parties with more money, resources and technical expertise are able to enhance this basic information with sophisticated data gathering and analytics, giving them a competitive advantage.

↘ Databases are expensive and time-consuming to keep up-to-date. Therefore, they may contain errors and obsolete information, as in the case of electoral registers in Kenya.[19] In the UK, the Labour Party and Conservative Party have had issues with their databases, from persistent glitches to crashes.[20]

↘ There are several cases of voter files being leaked (or otherwise acquired through illegal methods), with a negative effect on voter privacy.

↘ These databases are assets that can vary greatly between political parties. This may result in an uneven playing field that negatively impacts the power dynamics of democratic systems.

1

'Political HQ', HaystaqDNA, accessed 19 February 2019, https://haystaqdna.com/politicalhq/.

2

'Political HQ', HaystaqDNA.

3

NationBuilder, 'Voter Data and the NationBuilder National Voter File', accessed 8 March 2019, https://nationbuilder.com/voter_data_information.

4

Electoral Commission, 'What Is the Electoral Register?', accessed 8 March 2019, https://www.electoralcommission.org.uk/faq/voting-and-registration/what-is-the-electoral-register.

5

Coventry City Council, 'The Electoral Register and the Open Register | Registering to Vote', accessed 8 March 2019, http://www.coventry.gov.uk/info/8/elections_and_voting/765/registering_to_vote/7.

6

Coventry City Council, 'The Electoral Register and the Open Register | Registering to Vote'.

7

NationBuilder, 'Voter Data and the NationBuilder National Voter File'.

8

L2, 'Data: Voter File Enhancements', accessed 8 March 2019, https://www.l2political.com/products/data/voter-fileenhancements/.

9

Grace Mutung'u, 'Kenya: Data and Digital Election Campaigning', Tactical Tech, 2018, accessed 8 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-kenya/.

10

Noel Dempsey, 'Membership of UK Political Parties', UK Parliament, 2018, Number SN05125, accessed 8 March 2019, https://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN05125.

11

Privacy International, 'State of Privacy Chile', Privacy International, January 2019, accessed 11 March 2019,https://privacyinternational.org/state-privacy/28/state-privacy-chile.

12

Raquel Rennó, 'Chile: Voter Rolls and Geo-Targeting', Tactical Tech, 2018, accessed 8 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-chile/.

13

Grace Mutung'u, 'Kenya: Data and Digital Election Campaigning'.

14

Grace Mutung'u, 'Kenya: Data and Digital Election Campaigning'.

15

Colin Bennett and Robin Bayley, 'Data Analytics in Canadian Elections', Tactical Tech, 2018, accessed 8 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-canada/.

16

Colin Bennett and Robin Bayley, 'Data Analytics in Canadian Elections'.

17

The Labour Party, 'Tools for Activists', accessed 8 March 2019, https://labour.org.uk/members/activist-area/tools-foractivists/.

18

Nick Anstead, 'Data-Driven Campaigning in the 2015 United Kingdom General Election', The International Journal of Press/Politics, vol. 22, no. 3, July 2017, pp. 294–313, doi:10.1177/1940161217706163.

19

Grace Mutung'u, 'Kenya: Data and Digital Election Campaigning'.

20

Mark Pack, 'More Doubts Raised over Conservative Merlin Campaign Database', Mark Pack (blog), 5 April 2010, accessed 11 March 2019, https://www.markpack.org.uk/9471/merlin-database-conservative-party/.
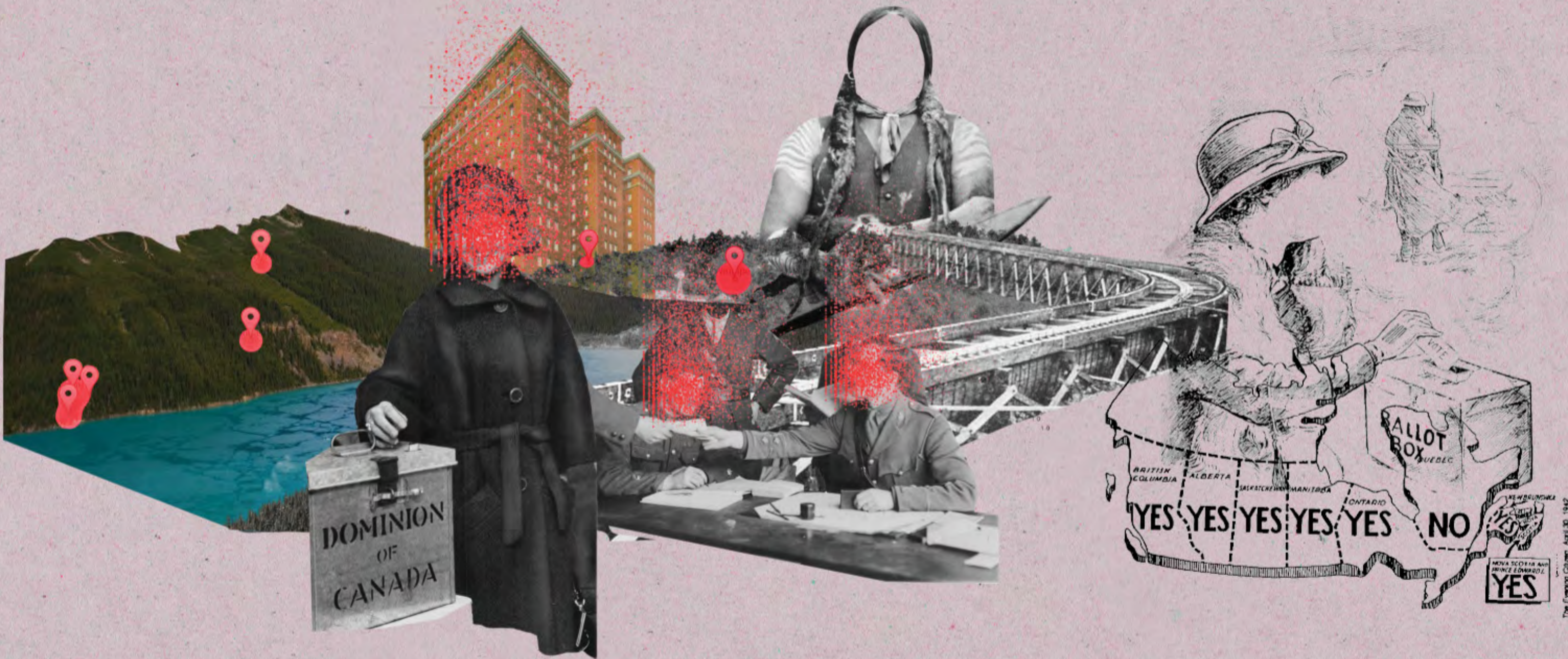
DOMINION
OF
CANADA

BALLOT
BOX

QUEBEC

BRITISH
COLUMBIA
ALBERTA
SASKATCHEWAN MANITOBA
ONTARIO

NEWFOUNDLAND

NOVA SCOTIA AND
PRINCE EDWARD I.
YES

YES YES YES YES YES NO

The Evening Citizen, April 30, 1942

Breaches, Leaks and Hacks: The vulnerable life of voter data

What are breaches, leaks and hacks?

Today, voter data is just as much of a target for malicious hacks and breaches as, say, credit card data, and is equally susceptible to poorly secured digital infrastructure. In fact, the problem has already reached a global scale. While wider international media coverage has largely looked at data hacks and breaches in elections through the lens of leaked emails,[1] nation-state involvement in misinformation campaigns,[2] or insecure infrastructure (such as vulnerabilities in voting booth software[3]), voter data is also at risk. Voter data can be exposed by either a malicious hack, an accidental leak, poorly configured security settings, or the physical theft of hardware. Regardless of the point of exposure, compromised voter data usually includes sensitive and personally identifiable information. As much as data on voters can be a political asset, it can also be a liability.

Over three billion internet credentials and other types of personal data have been stolen by hackers and two-thirds of victims are unaware that their data has been compromised, according to a report by the Center for Strategic and International Studies and McAfee.[4] Some of the most high-profile cases include the data breach at the Equifax credit reporting agency, which exposed the personal financial data of 143 million US consumers; the hacking of Yahoo's customer records, affecting over 1 billion users; and 'a data breach at a leading South African company [that] resulted in the loss of [personally identifiable information] for an estimated 31 million people, including the president, finance minister, and police minister. The data included income, address, and phone numbers'.[5]

What kind of data is involved?

Compromised voter data generally comprises data from two possible sources:

↘ **Official voter registers:** While varieties exist across different countries, most voter registers consist of a combination of voter name, date of birth and current residence, which can either be self-reported or automatically updated by state or governmental bodies. Depending on national structures, official registers may be administered at the state or local level. In the United States, depending on the state, such information is stored on digital spreadsheets and can be emailed to those purchasing the voter files.[6] Voter registers can also be centralised

into national-level registers, as in the United Kingdom, where they can be acquired in various spreadsheet formats as well as a printed document.[7]

↘ **Voter files:** Voter files are created in-house by political parties or by political data consultants for campaigning purposes. Voter files often consist of basic contact details typically sourced from public or governmental records, such as census or voter registration, which can be—and often are—enhanced by third-party datasets. These datasets are composed of a range of sources, from online and offline consumer and behavioural data from data brokers, to credit data from credit bureaus,[8] to canvassing data from campaign volunteers. Frequently, voter files are managed by proprietary software platforms specialising in campaign technology.

Some examples
↘ **Breaches**

In Hong Kong: In March 2017, two laptops belonging to Hong Kong's Registration and Electoral Office were stolen during the AsiaWorld-Expo. The hardware contained information about all of Hong Kong's 3.78 million registered voters, 'including their names, addresses, ID card numbers, mobile phone numbers and the geographical constituencies in which they were registered'.[9] Furthermore, the names of the 1,194 electors on Hong Kong's Election Committee were stored on the laptops. While the data was reportedly encrypted, detectives investigating the theft reportedly did not rule out the possibility that the incident was the result of an inside job.[10]

In the Philippines: In 2016, in what has been described as 'one of the biggest government-related data breaches in history', the website of the Philippine Commission on Elections was subjected to a cyberattack.[11] Simultaneously, a website went live claiming to contain the full 340-gigabyte database of 55 million registered voters.[12] Other reports raise the number of those affected by the leak to 70 million. The breached data included names, dates of birth, addresses, e-mail addresses, parent's full names and in some cases passport details and text markers of fingerprints—all published online. The website attack and data-hack were claimed by Anonymous Philippines and LulzSec Philippines.[13]

↘ **Leaks**

In Lebanon: In April 2018, it was reported that Lebanese embassies made available the personal data of Lebanese citizens living abroad. The Lebanese embassy in the UAE sent an email to Lebanese residing in the country with an attached spreadsheet containing the personal details of more than 5,000 Lebanese citizens who registered to vote in the upcoming elections, asking those contacted to confirm their voter registration information. The Lebanese embassy in the Hague sent a similar email to more than 200 recipients containing an attached spreadsheet with the personal data of Lebanese voters in the Netherlands. Moreover, the person who sent the email entered all the recipient addresses in the Cc: field instead of using the Bcc: field. In both cases the personal information in the spreadsheets included each voter's full name, mother's name, father's name, sex, date of birth, religion, marital status and address.[14]

In Mexico: In 2016, security researcher Chris Vickery located the Mexican voter roll, containing the personal records of 87 million Mexican voters, in a poorly configured database hosted on Amazon Web Services.[15] The leak included names, addresses, birth dates and national ID numbers and was detected through fairly common IT security practices. After an internal investigation, the Instituto Nacional Electoral fined the Mexican political party Movimiento Ciudadano US\$ 1.8 million for negligence in failing to properly secure its copy of the list.[16]

In the US: In 2017, cybersecurity researchers at UpGuard identified a misconfigured database containing the personal details of 198 million US voters. The leaked data included the full name of a given voter, voter's date of birth, home and mailing addresses, phone number, registered party, self-reported racial demographic, voter registration status and even whether they are on the federal 'Do Not Call' list. Also included as data fields were the 'modeled ethnicity' and 'modeled religion' of the potential voter. The leak included data from campaigning firms Deep Root Analytics, TargetPoint Consulting, Inc. and Data Trust—all contracted by the Republican National Committee. The poorly secured 1.1-terabyte database was discovered on an Amazon server and was accessible. In the end, the leak exposed details of nearly all 200 million registered US voters.[17]

↘ **Hacks**

In Turkey: In 2016, an unnamed hacker posted a downloadable 6.6-gigabyte file, titled Turkish Citizenship Database, which appeared to contain personal data of some 50 million citizens, including their names, addresses, parents' first names, places of birth, birth dates and a national identifier number.[18] While the affected data appeared to be from 2008, Isik Mater, a Turkish privacy activist stated to *Wired*: 'I searched my name on the list and reached all my family data. … It doesn't matter if the data is from 2008 because I still have the same name, same last name, same home address and obviously the same national ID number so it means that, the leak data is up-to-date for me and for lots of other people which makes the leak very, very serious'.[19]

In the US: In October 2018, two cybercrime intelligence research firms reported that an estimated 35 million US voter registration details were being offered for sale on a known dark web hacking forum. The data trove consisted of up-to-date 2018 voter registrations for at least 19 states. The researchers further reported that members of the forum banded together to crowdfund the asking price for the individual databases. While the voter files of these states are considered to be 'public' and available for sale, most states limit access to authorised entities, such as campaigns or researchers, and are barred from being republished. Furthermore, the research teams assessed that due to the nature of the available data the illicit vendor 'may have persistent access and/or contact with government officials from each state'.[20]

How do I know if it's affecting me?

Breaches, leaks and hacks of voter data tend to receive less high-profile media coverage, with public attention frequently focusing on state or party-led[21] dis- and mis-information campaigns in national or even small scale elections.[22] Often, compromised voter data is covered by specialist blogs, cybersecurity researchers or niche websites making it more difficult for the non-specialist audiences to know when and where a voter data breach has occurred, let alone if they have been affected. However, in major incidents, such as the 2017 leak of nearly 200 million US voter details, news stories are the most accessible source of information.

A screenshot of a redacted spreadsheet of NGP access credentials as found in the Rice Consulting breach. The exposed data was found by Director of Cyber Risk Research at Hacken, a cyber-security research firm, using an Internet of Things search engine.

Source: Diachenko, Bob. "More than Just a Data Breach: A Democratic Fundraising Firm Exposure." Hacken Blog, accessed 6 March 2019. https://blog.hacken.io/more-than-just-a-data-breach-a-dem-fundraising-firm-exposure

A screenshot of the Philippines' commission on elections' website which was defaced as part of a voter data breach by Anonymous Philippines in 2016.

Source: www.comelecdgov.ph, 27 March 2016

Screenshot of Deep Root Analytics RNC voter data exposure, which was discovered by UpGuard's cyber risk analyst Chris Vickery, showing 'RNC ID' numbers and a modelled score of likelihood of voters supporting certain policies.

Source: Dan O'Sullivan. "The RNC Files: Inside the Largest US Voter Data Leak." UpGuard, accessed 4 September 2018, https://www.upguard.com/breaches/the-rnc-files

In an article, researched and written by Anomali Labs and Intel471, it was found that illegally gained voter lists for 19 US states were advertised on a dark web hacker forum.

Source: Anomali Labs. "Estimated 35 Million Voter Records For Sale on Popular Hacking Forum." Anomali, accessed 7 March 2019, https://www.anomali.com/blog/estimated-35-million-voter-records-for-sale-on-popular-hacking-forum

A redacted screenshot of a Mexican citizen record found in a major data breach provided by MacKeeper security researcher, Chris Vickery, to use in a story run by The Daily Dot.

Source: Dell Cameron. "Private Records of 93.4 Million Mexican Voters Exposed in Data Breach." The Daily Dot, 22 April 2016, https://www.dailydot.com/layer8/amazon-mexican-voting-records/

SMEX obtained this screenshot of an email sent by a Lebanese embassy with an attached spreadsheet of registered voters.

Source: Lebanese Embassies Expose the Personal Data of Registered Voters Living Abroad." SMEX: Channeling Advocacy, 6 April, 2018. https://smex.org/lebanese-embassies-expose-the-personal-data-of-registered-voters-living-abroad/

"In October 2018, two cybercrime intelligence research firms reported that an estimated 35 million US voter registration details were being offered for sale on a known dark web hacking forum."

Considerations

↘ Leaked, hacked or breached voter data has yet to be publicly acknowledged as a source of data for digital campaigning by political campaigns. The nature of how voter data is acquired in these examples means that there is little insight into what role these leaks, hacks and breaches of voter data have in the course of an election. What we do know, however, is that there have been media reports of specifically politically motivated hackers, such as Andrés Sepúlveda in Latin America,[23] and cases where compromised voter data was used to disrupt the election process.[24]

↘ The breadth, depth and country contexts of these breaches, leaks and hacks of voter data vary across each instance, making it difficult to come to a uniform judgment about their full implications. While in some instances it was claimed that the compromised data was outdated and thus arguably lesser value, other examples of breached data have more serious impacts. For example, in October 2018 a security researcher was able to access an unprotected and internet-connected storage device belonging to Rice Consulting, a US fundraising firm hired by the Democratic Party.[25] Along with personal data of fundraisers, from phone numbers, to names, email and postal addresses, the database contained contracts, meeting notes, desktop backups and employee details. Significantly, the instance also contained access details to NGP, the voter database management suite used by the Democratic Party.

↘ Ultimately, the value of voter data is significant, especially if it becomes exposed on the open internet. There is generally a lack of oversight of how this data is stored, secured and handled. Political campaigns, data consultants and service providers have an obligation to handle data in their care with consideration. Changes in data protection laws in the European Union find an entity handling data responsible not only for a data leak or breach, but also for reporting it in a timely manner. According to a survey of the campaigning industry, cybersecurity experts still warn that 'most of the industry isn't taking the threat [of digital interference in elections] seriously enough' and that poor security practices by individual consultants are the 'weak links' in securing voter data and election integrity.[26]

1
Matt Burgess, 'The Emmanuel Macron Email Hack Warns Us Fake News Is an Ever-Evolving Beast', Wired UK, 8 May 2017, accessed 13 March 2019, https://www.wired.co.uk/article/france-election-macron-email-hack.

2
Andy Greenberg, 'Everything We Know About Russia's Election-Hacking Playbook', Wired, 9 June 2017, https://www.wired.com/story/russia-election-hacking-playbook/.

3
Timothy Revell, 'Hacking a US Electronic Voting Booth Takes Less than 90 Minutes', New Scientist, accessed 6 March 2019, https://www.newscientist.com/article/2142428-hacking-a-us-electronic-voting-booth-takes-less-than-90-minutes/.

4
James Lewis, 'Economic Impact of Cybercrime', Center for Strategic & International Studies, accessed 12 March 2019, https://www.csis.org/analysis/economic-impact-cybercrime.

5
Lewis, 'Economic Impact of Cybercrime'.

6
'PA Full Voter Export', Pennsylvania Department of State, accessed 11 March 2019, https://www.pavoterservices.pa.gov/Pages/PurchasePAFULLVoterExport.aspx. 'Statewide Voter File Information', Montana Secretary of State, accessed 11 March 2019, https://sosmt.gov/elections/voter-file/.

7
'Supply of the Electoral Register', The Electoral Commission, accessed 11 March 2019, https://www.electoralcommission.org.uk/__data/assets/pdf_file/0005/162824/List-of-people-entitled-to-be-supplied-with-the-electoral-register.pdf.

8
Drew DeSilver, 'Q&A: The Growing Use of "Voter Files" in Studying the U.S. Electorate', Pew Research Center (blog), 15 February 2018, http://www.pewresearch.org/fact-tank/2018/02/15/voter-files-study-qa/.

9
Ng Kang-chung, 'Privacy Watchdog Blasts Electoral Office for Massive Data Breach', South China Morning Post, 12 June 2017, https://www.scmp.com/news/hong-kong/politics/article/2098002/hong-kong-privacy-watchdog-blasts-electoral-office-massive.

10
Clifford Lo, 'Election Laptop Theft May Have Been "Inside Job"', South China Morning Post, 28 March 2017, https://www.scmp.com/news/hong-kong/law-crime/article/2082894/hong-kong-election-laptop-theft-may-have-been-inside-job.

11
Tina G. Santos, '55M at Risk in "Comeleak"', 23 April 2016, http://technology.inquirer.net/47759/55m-at-risk-in-comeleak.

12
James Temperton, 'Massive Philippines Data Breach Now Searchable Online', Wired UK, 22 April 2016, https://www.wired.co.uk/article/philippines-data-breach-comelec-searchable-website.

13
Leisha Chi Lee Dave, 'Philippines Elections Hack "Leaks Data"', BBC News, 11 April 2016, https://www.bbc.com/news/technology-36013713.

14
'Lebanese Embassies Expose the Personal Data of Registered Voters Living Abroad', SMEX: Channeling Advocacy, 6 April 2018, https://smex.org/lebanese-embassies-expose-the-personal-data-of-registered-voters-living-abroad/.

15
Andrii Degeler, 'Millions of Mexican Voter Records Leaked to Amazon's Cloud, Says Infosec Expert', Ars Technica, 25 April 2016, https://arstechnica.com/information-technology/2016/04/millions-of-mexican-voter-records-leaked-amazon-cloud/.

16
Carina García, 'Aprueban multa de 34 millones para Movimiento Ciudadano por filtrar padrón', El Universal, 23 March 2018, https://www.eluniversal.com.mx/nacion/politica/aprueban-multa-de-34-millones-para-movimiento-ciudadano-por-hackeo-de-padron.

17
Dan O'Sullivan, 'The RNC Files: Inside the Largest US Voter Data Leak', UpGuard (blog), accessed 4 September 2018, https://www.upguard.com/breaches/the-rnc-files.

18
Robert Tait, 'Personal Details of 50 Million Turkish Citizens Leaked Online, Hackers Claim', The Telegraph, 4 April 2016, https://www.telegraph.co.uk/news/2016/04/04/personal-details-of-50-million-turkish-citizens-leaked-online-ha/.

19
Andy Greenberg, 'Hack Brief: Turkey Breach Spills Info on More Than Half Its Citizens', Wired, 5 April 2016, https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/.

20
'Estimated 35 Million Voter Records For Sale on Popular Hacking Forum', Anomali Labs, accessed 7 March 2019, https://www.anomali.com/blog/estimated-35-million-voter-records-for-sale-on-popular-hacking-forum.

21
Craig Timberg and Tony Romm, 'Disinformation Campaign Targeting Roy Moore's Senate Bid May Have Violated Law, Alabama Attorney General Says', The Washington Post, 27 December 2018, https://www.washingtonpost.com/technology/2018/12/27/disinformation-campaign-targeting-roy-moores-senate-bid-may-have-violated-law-alabama-attorney-general-says/.

22
Adam Entous and Ronan Farrow, 'Private Mossad for Hire', New Yorker, 11 February 2019, https://www.newyorker.com/magazine/2019/02/18/private-mossad-for-hire.

23
'Political Cyberhacker Andrés Sepúlveda Reveals How He Digitally Rigged Elections across Latin America', The Independent, accessed 28 August 2018, https://www.independent.co.uk/news/world/americas/political-cyberhacker-andres-sepulveda-reveals-how-he-digitally-rigged-elections-across-latin-a6965161.html.

24
'DA: Hackers Penetrated Voter Registrations in 2016 Through State's Election Site', KQED, 21 July 2017, https://www.kqed.org/news/11579541/hackers-penetrated-voter-registrations-in-2016-through-states-election-site; Latanya Sweeney, Ji Su Yoo, and and Jinyan Zang, 'Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections', Technology Science, 6 September 2017, /a/2017090601/.

25
Bob Diachenko, 'More than Just a Data Breach: A Democratic Fundraising Firm Exposure', accessed 28 February 2019, https://blog.hacken.io/more-than-just-a-data-breach-a-dem-fundraising-firm-exposure.

26
Sean Miller, 'Consultants Mostly Optimistic on Industry's Future, But 2020 Worries Loom', Campaigns & Elections, 6 March 2019, https://www.campaignsandelections.com/campaign-insider/consultants-mostly-optimistic-on-industry-s-future-but-2020-worries-loom.

Data as Intelligence

The digital campaign led by Brad Parscale for the 2016 Trump presidency reportedly tested 40,000 to 50,000 versions of messages per day. This level of testing not only led to messages that demonstrably moved people to action, like donations, but also led to insights into what voters were motivated by and what they wanted to hear, which the campaign adapted per individual or per group.

Emphasis on testing at scale and variance in political campaigning potentially leads not only to forms of 'click-led' politics, but also to new forms of political intelligence gathering. Similarly, the use of methods such as digital listening—collecting openly available information on political discussions—leads to the accumulation of insights into voter opinions, which can then be used to form positions, decide which areas to campaign in, or how to pitch a speech to a certain community.

Knowing what the electorate thinks and wants is an important part of democratic processes. What is new, however, is the scale, pace, dynamism and granularity that big data practices allow. This makes the difference between a technology that can enhance the democratic process by listening to what voters really want and one that becomes a disrupting influence.

A/B Testing: Experiments in campaign messaging

"As long as a campaign has the relevant data and a sufficient number of individuals for a statistically valid experiment, nothing is off-limits for experimentation, pursuant to local laws."

What is A/B testing?

When Barack Obama's 2008 presidential campaign team was having trouble converting web visitors into subscribers, they took a page from commercial marketing's playbook and decided to change the text on their website. They tested three different messages against the site's usual 'Sign Up' prompt: 'Learn More,' 'Join Us Now' and 'Sign Up Now.' They found that 'Learn More' outperformed the default message by a whopping 18.6%.[1] When they tested the prompt alongside six different photo and video options, the winning combination boosted their sign-up rate by more than 3 percentage points. While this number may seem small, the campaign estimated that this single change contributed to nearly three million new email address sign-ups and netted $60 million in new donations.[2, 3, 4] Four years later, the Obama re-election campaign ran over 500 similar A/B tests across web and email in 20 months, increasing their donation conversion by 29% and their sign-up conversions by 161%.[5, 6]

A/B testing, sometimes called split testing, compares two or more variants of an advertisement or message to determine which one performs best. Campaigns commonly experiment on their donation pages to boost contributions. In 2016, Ben Carson's US presidential campaign ran an experiment to find out whether giving away a copy of Carson's book or a campaign hat yielded more donations. By randomly directing website visitors to either the book donation page or the hat donation page, the campaign could measure which offer was more successful. If the cap was found to be more successful, the campaign could have run another experiment pitting the cap against, say, a tote bag; in this way, they could continue optimising the website.[7]

Though digital A/B testing is common in tech and campaign circles today, the method has a long analogue history going back to the 1920s, when the British statistician Ronald Fisher formalised its basic mathematics while testing crop growth by applying fertilizer to one plot of land and withholding it from another.[8] Since then, A/B testing has been integrated into politics and has become part of standard campaign practice for websites, emails (subject lines, bodies), design elements (images, backgrounds, buttons), headlines, direct mail, TV, radio, phone and even texting to 'find the right messaging'.[9, 10, 11, 12, 13] A number of services have made A/B testing easy to run for political campaigns, allowing them to test multiple changes simultaneously.[14, 15]

How is your data used?

Campaigners rely on personal data in both the setup and evaluation of A/B tests. First, they use it to select who qualifies for a given experiment. If a campaign were interested in mobilising working mothers in a swing district or boosting rally attendance in another, for instance, it could launch experiments using address information obtained from voter files, a data exchange or another source. As long as a campaign has the relevant data and a sufficient number of individuals for a statistically valid experiment, nothing is off-limits for experimentation, pursuant to local laws.

A/B testing also relies on personal data to track responses to experiments. If you receive an email from a campaign, for instance, the campaign is likely tracking email open and click-through rates to determine if you engage with it or not. That data can be mined even further: if you unsubscribe from the email list, perhaps you will be considered less likely to vote for the candidate in question. If you consistently open campaign emails promptly, the campaign could deem you a promising volunteer.

Some examples

In the UK: Dominic Cummings, campaign director of Vote Leave during the UK's 2016 EU membership referendum (also known as the Brexit referendum), described how the Leave campaign used personal data and experimentation to help them win. According to Cummings, by surveying voters in the UK, campaign data scientists were able to do things like 'target women between 35 and 45 who live in these particular geographical entities, who don't have a degree or do have a degree […] We essentially ran a whole series of experiments […] out in the digital world and filtered what worked'. The Vote Leave campaign split voters into three groups: those firmly voting remain, those voting leave, and those on the fence. Vote Leave invested 98% of its marketing budget in digital efforts focused on this third group and tested five narratives on them.[16] The winning message was 'take back control'. Research suggested that including the word 'back' triggered voters' anger and dislike of losing things they felt they once had—in particular, control.[17]

In the United States: Some political campaigns in the US are using A/B testing at a staggering scale, even when compared to private companies.[18] Nowhere was this more clear than in Donald Trump's 2016 presidential run. Gary Coby, the director of digital advertising and fundraising for the Trump campaign, called their use of experimentation 'A/B testing on steroids'.[19] The campaign reportedly ran 40,000 to 50,000 variants on a given day,[20] and these experiments proved to be lucrative. As Michael Babyak, former director of marketing technology at the Republican National Convention claimed, 'The RNC Performance, Optimization & Experiments Team […] ran over 300 tests on DonaldJTrump.com from July through November 2016, generating over $30 million in added revenue'.[21] The team found that pro-Trump messages always 'beat out any anti-Hillary or otherwise negative copy'.[22] Well after the election, in May 2018, Coby declared on Twitter that the team still had over 4,000 ads active for 'testing and learning', extending the campaign's intelligence-gathering activities beyond the election.[23]

How do I know if it's being used on me?

You have almost certainly been part of an A/B test. As Christian Rudder, president of OKCupid, wrote in a blog in 2014: 'Guess what, everybody: if you use the Internet, you're the subject of hundreds of experiments at any given time, on every site. That's how websites work'.[24] Another commentator observed, 'every product, brand, politician, charity, and social movement is trying to manipulate your emotions on some level, and they're running A/B tests to find how out'.[25] A/B testing is now standard practice among virtually any entity with an online presence. While you may be able to identify experiments in which you are participating by inspecting hyperlinks or by analysing your third-party cookies, there is no way to comprehensively know in which political campaign experiments you were included.

Considerations

↘ A/B testing allows campaigns to test their assumptions and avoid deferring to HiPPO (the Highest Paid Person's Opinion), a derisive term describing the standard decision-making process. If a political message is tested properly, it has the potential to debunk faulty assumptions.

↘ As one expert observed, 'taken to its logical conclusion, [this trend] could lead to a stream of unique, personalised messages targeted at each voter constantly updated based on A/B testing'.[26] That A/B tests can be selectively targeted and tweaked for personal appeal risks undermining public understanding of political issues and opens the door to more manipulative tactics.

↘ As A/B testing services become more automated, algorithms can create far more variants and combinations of text, media, buttons, etc. based on campaign inputs. This ostensibly means that machines—instead of people—would decide what a potential voter reads and sees, which could set a precedent of creating personalised political content free of human oversight.

↘ If an A/B test demonstrates a desirable and sizeable impact, what of the voters exposed to the 'losing' variant who may, as a result, be marginally less inclined to join a newsletter, to volunteer, to consume political news, or to vote?

↘ Voters are generally unaware of their participation in experiments; moreover, permission is often requested by privacy policies that users tend to accept without reading. As a result of this lack of awareness, there's no way for participants to opt out. Furthermore, many voters are unaware of the impacts that past experiments may have had on them.[27, 28]

↘ Political campaigns often run experiments on people without independent, ethical oversight.[29]
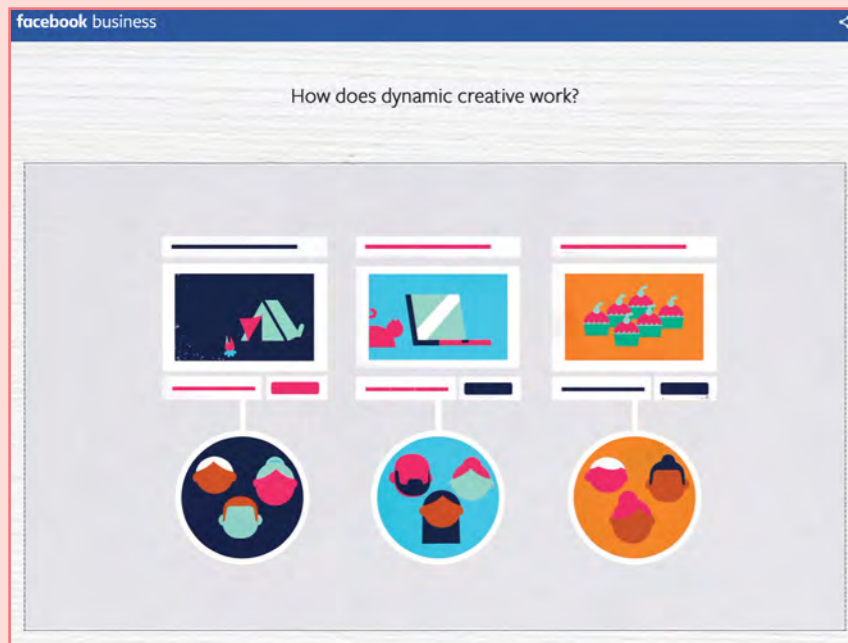
A/B testing is moving towards algorithmic generation of variants. Using data to create the most compelling ad for a given user, algo-rithmically-generated variants allow computers to decide what users see by customizing different ad creatives for different individuals. This screen-shot was taken from promotional 'dynamic creative' product video by Facebook, a popular experimentation platform for political campaigns. The voiceover audio explains that advertisers supply images, video, text, calls to action, budget and target audiences, and the product will decide which combinations work best with any given audience.[30]

Source: https://www.facebook.com/business/m/facebook-dynamic-creative-ads\, accessed 7 January 2019
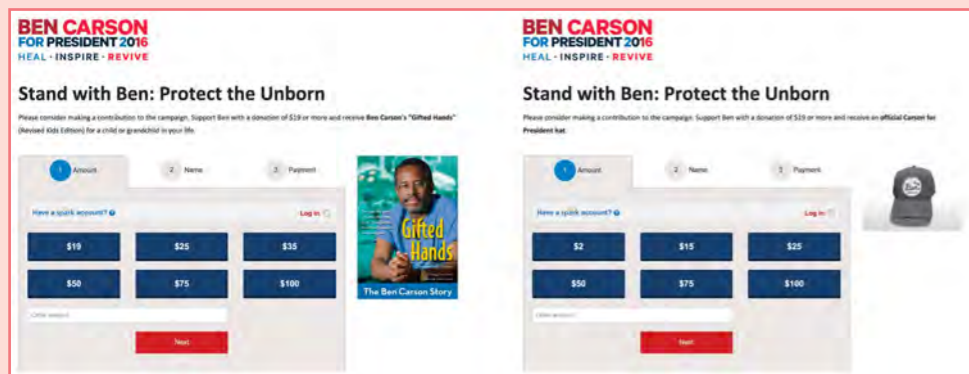

An article published on medium.com explores how Ben Carson's 2016 presidential campaign tested whether a book or a hat was a more effective gift in soliciting donations to his campaign. The test took place on his website, BenCarson.com, which was no longer active at the time of writing.[31]

Source: https://medium.com/soapbox-dc/what-are-jeb-bush-others-a-b-testing-676b231f094f, accessed 11 March 2019


These ads, from Facebook's Ad Archive, encourage Indians to organise a get-together to listen to Prime Minister Narendra Modi's address to the nation. The sign-up messages are identical, but the images differ slightly. All three ads cost less than 15 USD and were seen between 10,000 and 60,000 times.[32]

Source: https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=IN&q=modi, accessed 11 March 2019.
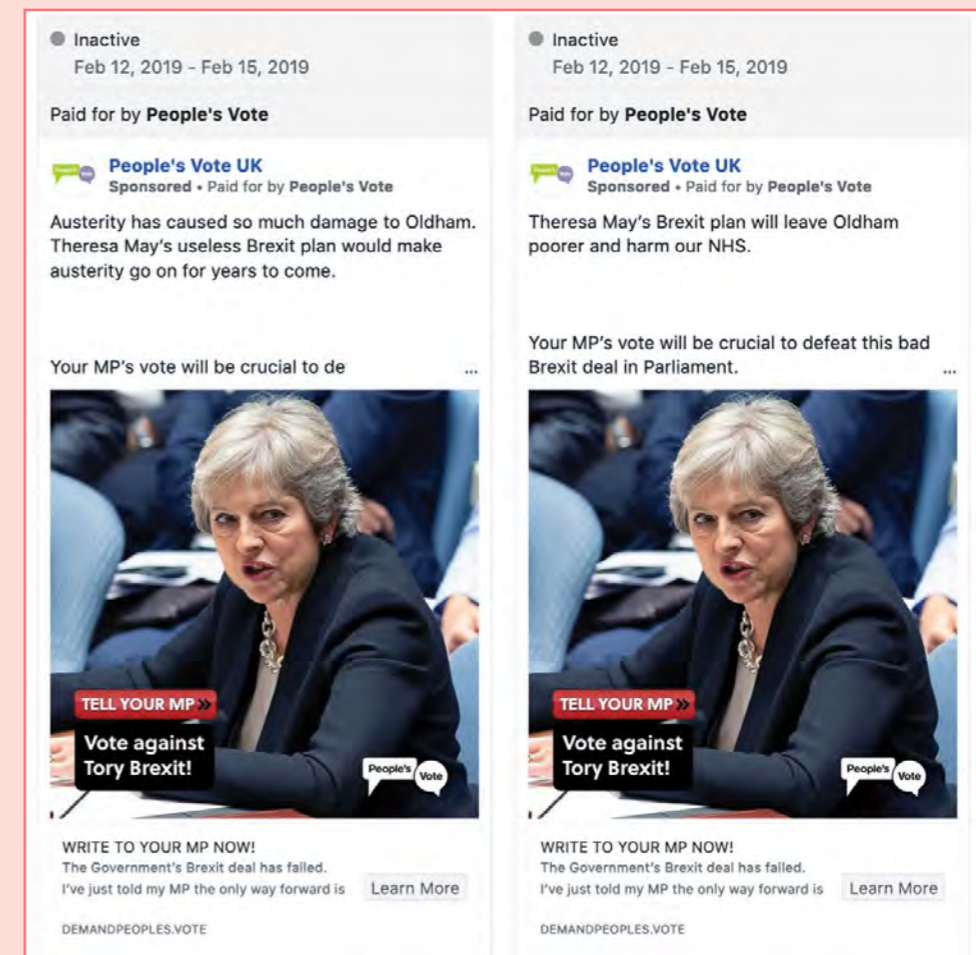
This screenshot from Facebook's ad archive shows two political advertisements against Brexit used the same image but different text. The ad on the left was shown to users less than 1,000 times, while the ad on the right was shown between 5,000 and 10,000 times. No metrics are available whether one garnered more clicks than the other.[33]

Source: https://www.facebook.com/ads/ar-chive/?active_status=all&ad_type=po-litical_and_issue_ads&country=GB&q=brexit%20theresa%20may, accessed 22 February 2019
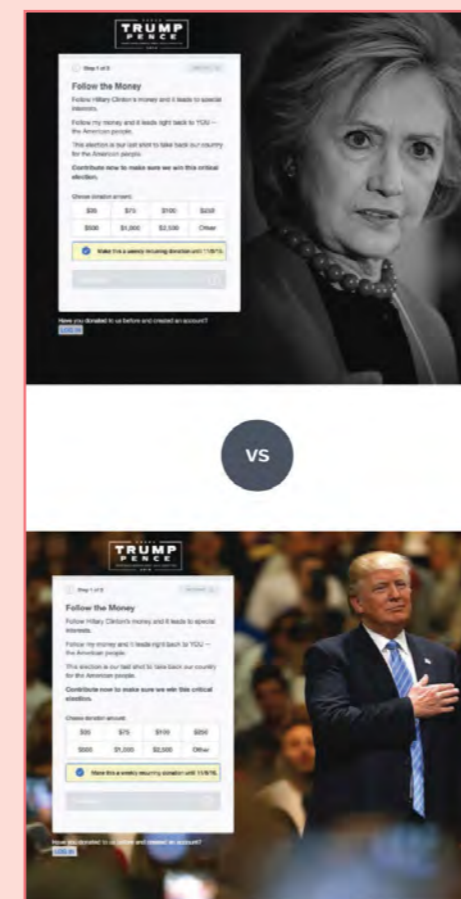
A screenshot from the RNC Testing Booklet posted on www.scribd.com shows how Donald Trump's campaign tested these two background images against each other on its donation page. The image of Trump performed about 80% better than the image of Clinton.[34]

Source: https://www.scribd.com/document/336800205/RNC-Testing-Booklet, accessed 7 January 2019.

Considerations (continued)

↘ A/B testing could be exploited as a testing ground for politicians—a space to trial an idea and conceal it if it fails, or promote it if it works.

↘ A/B testing can save a politician from appearing undecided on an issue by testing different messages and trumpeting the winning variant. One writer observed, 'instead of seeking consensus or taking politically risky decisions, empirical data gained from A/B testing might provide the optimal solution: "Why debate when you can test?"'[35]

↘ A/B testing risks 'circumventing the reasoning process altogether in the search for what works,' redirecting campaigns' attention from issues to button colours.[36, 37]

↘ A/B testing makes campaign monitoring more difficult. Instead of keeping tabs on one website, campaign monitoring groups may have to keep track of multiple variants of the same website.

1
Brian Christian, 'The A/B Test: Inside the Technology That's Changing the Rules of Business', Wired, 26 April 2012, https://www.wired.com/2012/04/ff-abtesting/

2
Tom New, 'Formisimo Blog Digital Marketing and CRO in Political Campaigns', accessed 4 January 2019, https://www.formisimo.com/blog/digital-marketing-and-cro-in-political-campaigns/

3
'How Obama Raised $60 Million by Running a Simple Experiment', Optimizely Blog, 30 November 2010, https://blog.optimizely.com/2010/11/29/how-obama-raised-60-million-by-running-a-simple-experiment/

4
'Which Presidential Candidate Is Winning the Digital Marketing Battle?', accessed 9 January 2019, http://blog.ispionage.com/presidential-candidates-digital-marketing-strategy.html

5
New, 'Formisimo Blog Digital Marketing and CRO in Political Campaigns'.

6
Optimization at the Obama Campaign: A/b Testing', 25 June 2018, https://web.archive.org/web/20180625130050/http://www.kylerush.net/blog/optimization-at-the-obama-campaign-ab-testing/.

7
Alhan Keser, 'What Are Jeb Bush & Others A/B Testing?', Soapbox (blog), 14 February 2016, https://medium.com/soapbox-dc/what-are-jeb-bush-others-a-b-testing-676b231f094f

8
'A Refresher on A/B Testing', accessed 22 February 2019, https://hbr.org/2017/06/a-refresher-on-ab-testing.

9
Erik Kofman-Burns, 'Manually A/B Testing Messaging with Hustle', Hustle Blog, 23 August 2017, https://blog.hustle.com/manually-a-b-testing-messaging-with-hustle-496f32c71408.

10
'Optimization at the Obama Campaign'.

11
The Digital Plan, Digital Political Tips: Peer to Peer SMS A/B Testing, accessed 8 January 2019, https://www.youtube.com/watch?v=JDgY9-422nU.

12
Brexit Sham, Cummings - Why Leave Won the Referendum, accessed 10 January 2019, https://www.youtube.com/watch?v=CDbRxH9Kiy4.

13
Alhan Keser, 'What Is Bernie Sanders A/B Testing?', Soapbox (blog), 7 February 2016, https://medium.com/soapbox-dc/what-s-bernie-a-b-testing-df4437171933.

14
'ActBlue Support', accessed 8 January 2019, https://support.actblue.com/.

15
'What Is an Experiment-Informed Program (EIP) and Do I Want One ?', accessed 8 January 2019, https://www.thecampaignworkshop.com/what-experiment-informed-program-eip-and-do-i-want-one.

16
Brexit Sham, Cummings - Why Leave Won the Referendum.

17
'How Vote Leave Used Data Science and A/B Testing to Achieve Brexit', AB Tasty, 14 June 2017, https://www.abtasty.com/blog/data-science-ab-testing-vote-brexit/.

18
Ron Kohavi and Stefan Thomke, 'The Surprising Power of Online Experiments', Harvard Business Review, 1 September 2017, https://hbr.org/2017/09/the-surprising-power-of-online-experiments.

19
Michael J. Coren, 'Startups Are Co-Opting Donald Trump's Digital Playbook to Push Progressive Politics in 2018', Quartz, accessed 12 December 2018, https://qz.com/1023261/startups-are-co-opting-donald-trumps-digital-playbook-to-push-progressive-politics-in-2018/.

20
Issie Lapowsky, 'This Is How Facebook Actually Won Trump the Presidency', Wired, 15 November 2016, https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/.

21
Michael Babyak, 'Donald J. Trump's $30M Testing Team', Michael Babyak (blog), 9 February 2017, https://medium.com/@babyak/donald-j-trumps-30m-testing-team-e1a9d542039e.

22
Babyak.

23
According to Facebook's new political ad portal, the Trump campaign has bought more than 3,000 ad variants since May 7th of this year. Lots of A/B testing with different text/image/video variants. https://www.facebook.com/politicalcontentads/?Active_status=all&page_ids[0]=153080620724&q=trump …pic.Twitter.Com/DJswUVOvhE', Tweet, @issielapowsky), 24 May 2018, https://twitter.com/issielapowsky/status/999753778709622785?lang=en.

24
Christian Rudder, 'We Experiment On Human Beings!', OkTrends (blog), accessed 8 January 2019, https://web.archive.org/web/20140728200455/http://blog.okcupid.com/index.php/we-experiment-on-human-beings/.

25
'The Morality Of A/B Testing', TechCrunch (blog), accessed 7 January 2019, http://social.techcrunch.com/2014/06/29/ethics-in-a-data-driven-world/.

26
'The Hyper-Personalised Future of Political Campaigning', CapX, 12 July 2018, https://capx.co/the-hyper-personalised-future-of-political-campaigning/.

27
Christian, 'The A/B Test'.

28
'The Morality Of A/B Testing'.

29
'The Morality Of A/B Testing'.

30
https://www.facebook.com/business/m/facebook-dynamic-creative-ads

31
Alhan Keser, 'What Are Jeb Bush & Others A/B Testing?'.

32
'Ad Archive', Facebook, accessed 23 February 2019, https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=IN&q=modi.

33
'Ad Archive', accessed 22 February 2019, https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=GB&q=brexit%20theresa%20may.

34
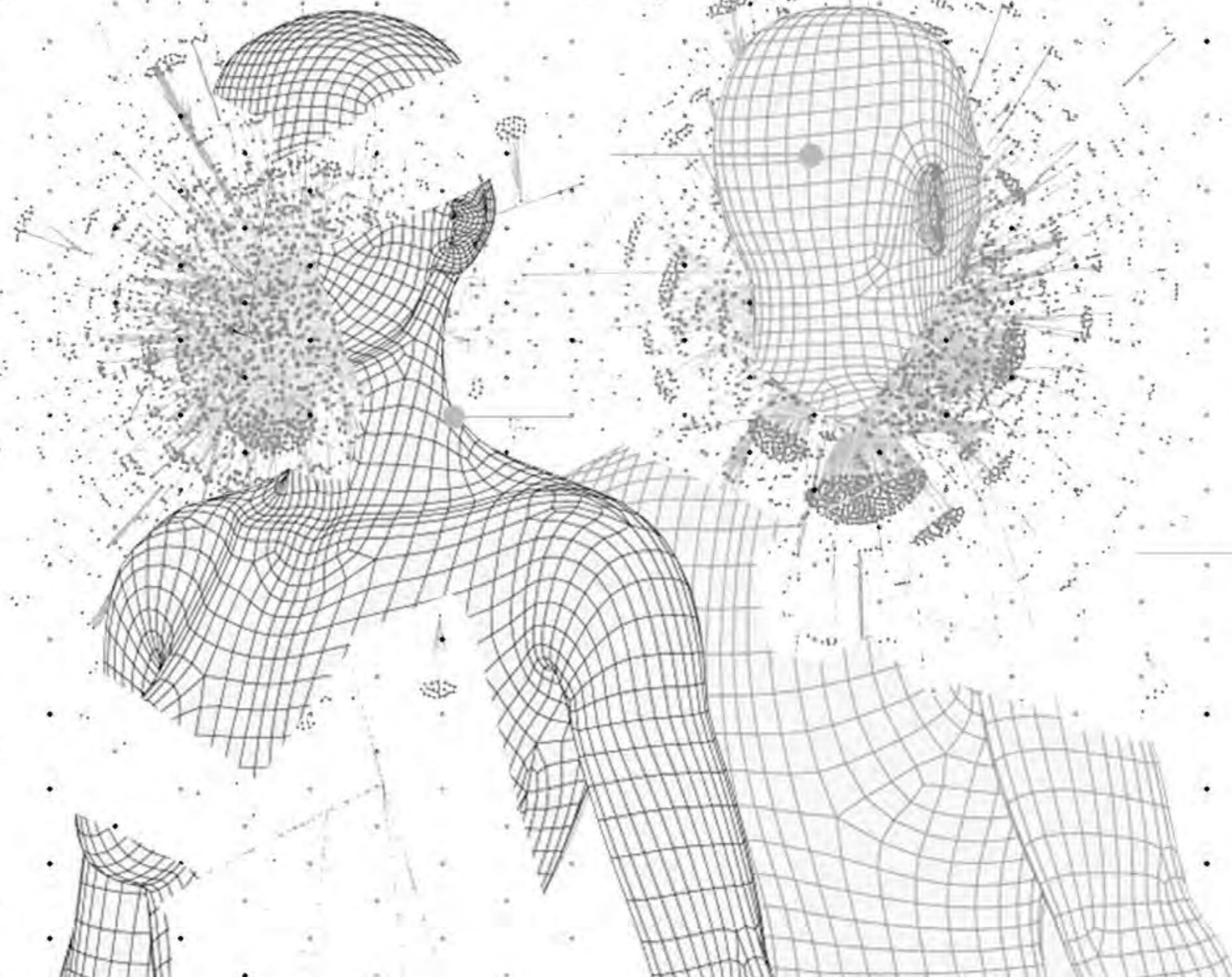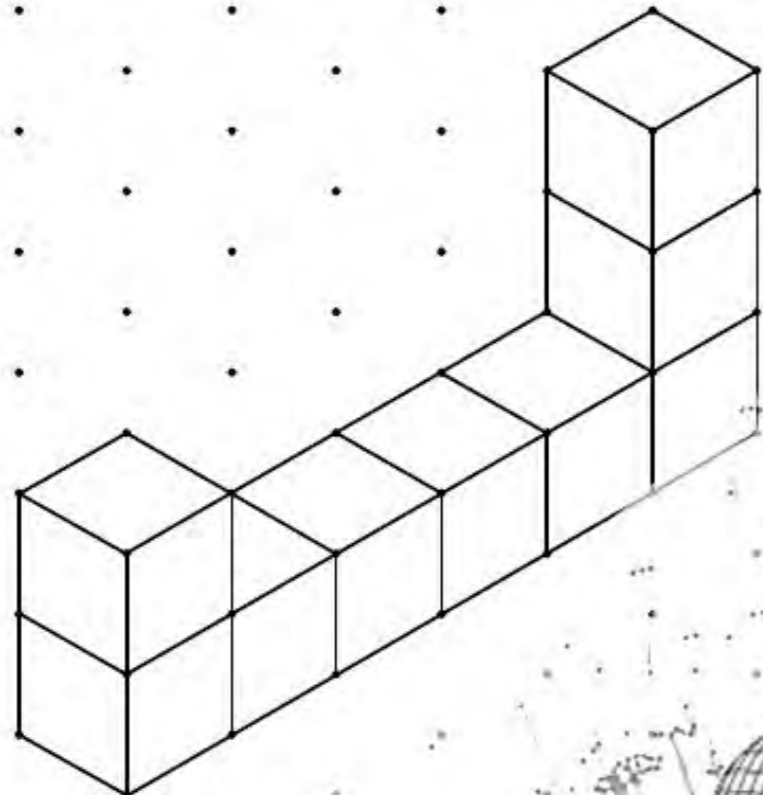*'RNC Testing Booklet | Donald Trump Presidential Campaign, 2016 | 2016 Republican National Convention', Scribd, accessed 7 January 2019, https://www.scribd.com/document/336800205/RNC-Testing-Booklet.*

35
Jeanette Hofmann, 'Microtargeting as a New Form of Political Claim-Making', n.d., 17.

36
Christian, 'The A/B Test'.

37
'Facebook Dynamic Creative', Facebook Business, accessed 11 January 2019, https://www.facebook.com/business/m/facebook-dynamic-creative-ads.

Campaign Apps:
Tap to participate

"We're in a race against time
time to defeat a rigged system…
Together we can win!"

TEXT FROM THE ONLINE POLITICAL GAME CORBYNRUN

What are campaign apps?

Apps aren't just for music, shopping and ride-sharing anymore; increasingly, they are becoming tools for politicians and campaigns to gain support and win votes.

Political campaign apps generally fall into one or more of three categories:

↘ **mobile apps** designed to support specific political candidates or particular causes.

↘ **enhanced canvassing apps** developed to combine information gathered from door-to-door canvassing with data from the campaign, commercial sources and public records.

↘ **games or gamified apps** created to mobilise an existing base of supporters and attract new voters.

How do they work?

↘ **Mobile apps** give politically like-minded people an exclusive space to interact and share ideas outside of larger social media platforms, where views can be more mixed. Some apps encourage participation by gamifying the experience, such as letting users accrue points and unlock badges for completing certain tasks like watching campaign advertisements, tweeting pre-written political messages, sharing their contacts with the campaign or calling their representatives to discuss preset talking points.

↘ **Enhanced canvassing apps** ostensibly allow campaign volunteers to visit homes door-to-door more efficiently. They give canvassers detailed information about the homes in their area, including who lives there, what party they are registered with, when they have voted in the past and what issues they care about. Apps can also supply customised scripts and survey questions for canvassers to ask residents based on their profiles. As canvassers visit homes, they upload the information they collect via the app and it is immediately recorded in the campaign's central database. Behind the scenes these apps gather and match voter registration, bankruptcy, criminal offence and other public-record data. Canvassers using NGP VAN's enhanced canvassing app, for instance, can present a candidate's views on issues affecting former military members if the app indicates that a veteran lives at the home.[1] These apps may also employ elements of gamification, such as leaderboards for the most productive canvassers.

↘ **Games or gamified apps:** Although they do not appear to use personal data and are the least common among these three groups, online political games like CorbynRun (created to support the Labour Party in the UK) and Super Klaver (supporting the centre-left De Groenen party in the Netherlands) are worth mentioning for their novelty.[2] These games, which tend to use 8-bit graphics and lo-fi audio, are easy to understand and can help build communities around political goals. The introduction to CorbynRun, for instance, reads: 'we're in a race against time time to defeat a rigged system … Together we can win!'[3] Fiscal Kombat, built for 2017 French presidential candidate Jean-Luc Mélenchon, shows the candidate fighting political opponents for money to pay for his policies while the rich try to defeat him. Over the course of the game, Mélenchon encounters the chairwoman of the International Monetary Fund, Christine Lagarde; French politician Jérôme Cahuzac, who was prosecuted for tax evasion; and former French president Nicolas Sarkozy.[4] By combining creative elements with topical political matters, games like these introduce new ways of engaging with political ideas while also perhaps blurring the line between reality and fiction.

How is your data used?

Campaign apps capture various types of data that can benefit a campaign as well as the app creator, who can adapt the user experience to solicit even more information from the user. Signing up is often free, and according to makers of such apps, the cost of creating and maintaining an app is 'set off by the data that can be gathered'.[5]

Campaign apps typically collect four types of data:[6]

↘ Data explicitly supplied by the user (such as name, email address, phone number, postal code, gender and age).

↘ Information about the user's social networks. Some apps reward users with points for sharing their address book contacts, which the campaign can cross-reference with its list of target voters. If a potential swing voter is found in the address book of an app user, the user will be prompted to invite the voter to the app with a preset, personalised message. Thomas Peters, CEO of the political app service uCampaign, explained how their Ted Cruz 2016 app reached out to potential swing voters they'd already identified based on voter files: 'if we identify that you have 10 friends in Iowa who are potential Cruz supporters, then we'll ask you to reach out to those people'.[7]

↘ Surveys or quizzes within apps can also supply personal data to campaigns. According to Peters, 'app supporters have completed over 20,000 political ID surveys about themselves, their friends and their neighbours, generating valuable cross-section data on the supporters' political views, activism affinities and personal network, essential information for a modern, data-driven campaign'.[8] While Cambridge Analytica's final product was not an app, the data for its psychometric profiles originated from a Facebook app called 'This is Your Digital Life', which was one of several personality quizzes available on the site.

↘ Behavioural data from interactions on the app. If a user responds to video instead of text, for example, this information may be logged and used to inform future versions of the app.

Some examples

In India: Prime Minister Narendra Modi's official campaign app, NaMo, launched in June 2015, promised to 'bring [users] the latest information' and important updates about Modi's government. In March 2018, it was discovered that the app on Android requested access to 22 different features of users' data, including access to their camera, microphone, contacts, photographs and location. (In contrast, Amazon's app in India requests access to 17 features.)[9] NaMo also seems to have collected personal data from 1.3 million members of the National Cadet Corps, a branch of the Indian military, to facilitate personal interaction between the Prime Minister and cadets.[10]

In the Dominican Republic: In 2012, Danilo Madina of the Dominican Liberation Party was narrowly elected President of the Dominican Republic. Four years later, after investing in both his country's and his campaign's technological base, Madina was reelected by a much wider margin. His app, Danilo 2016, was also built by uCampaign and had been downloaded nearly 14,000 times in the country of 10.65 million. About 65% of the app's users shared their address book contacts with the campaign, and nearly all agreed to receive push notifications. Through the app, users checked into events, shared content on social media, watched videos, posted selfies with President Madina, looked up GPS directions to polling stations, shared their votes on election day and invited friends to join.

In total, uCampaign claims that voters completed over 360,000 actions in support of President Madina's reelection. uCampaign boasts over 600,000 app downloads for political candidates and causes in nine languages across 12 countries.[11]

In France: In the lead-up to the 2017 French Presidential elections, Nicolas Sarkozy's campaign developed an app called Knockin, which mapped the campaign's database of contacts for door-to-door canvassers. The map marked each contact's address with a red dot, along with the resident's name. Canvassers approached the app's contacts at their homes and addressed them by name, leading to a public outcry over its invasiveness and an investigation by the French data protection authority, which ruled the app legal.[12]

How do I know what happens to my data?

Knowing exactly what information you share with apps requires reading their privacy policies, which vary app-by-app and are cumbersome to read. An alternative is to identify all the explicitly political apps on your device and conduct a quick internet search on each of them.

Even official campaign apps are not guaranteed to be secure. Ted Cruz's mobile app, for example, leaked users' IMSI number, a unique number that identifies mobile phone users and can potentially be used to track or eavesdrop on users.[13]

Even secure apps can—and often do—reserve the right to share the data they collect with third parties of their choice, so even if you review a full privacy policy and understand what data you are sharing with a campaign, truly knowing how it is being used downstream is difficult.
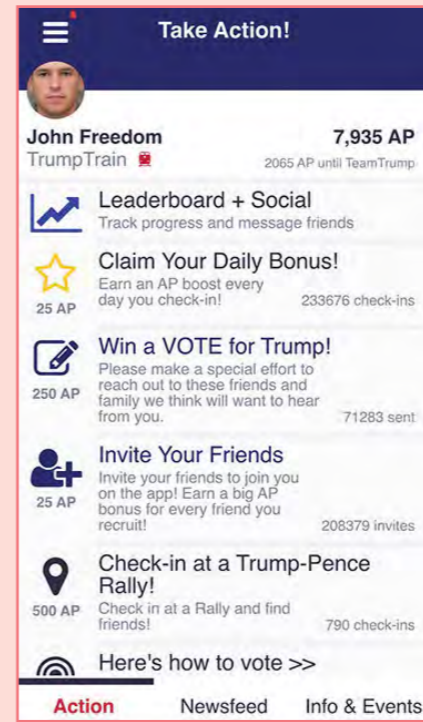
A screenshot from an article on medium.com of a comment posted on Ted Cruz's presidential campaign app, Ted Cruz 2016. The user's mention of being 'hooked' demonstrates how political campaigning apps incorporate elements from traditional gaming apps. The user's post references the 'Leader' badge she unlocked by accumulating points in the app.

Source: Peters, Thomas. 'We Are the Stealth Startup that Helped Ted Cruz Win Iowa' 5 February 2016. https://medium.com/@uCampaignCEO/meet-the-stealth-startup-that-helped-ted-cruz-win-iowa-fea6745b8a6d
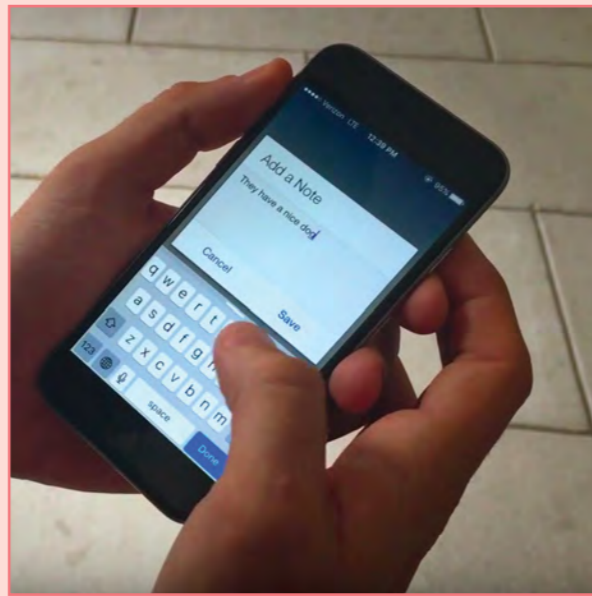

A screenshot from a promotional video, posted on YouTube, for a product by NGP VAN, a company that provides tech services to Democratic candidates in the US. Here, door-to-door canvassers use an enhanced canvassing app that uploads data into a campaign's contact database immediately. In this image, a canvasser populates an open note section of the app after visiting a home. The note reads: 'They have a nice dog'.

Source: 'Mini VAN & Mini Van Manager', https://www.youtube.com/watch?v=0qvF3C-iqCA, accessed 20 February 2019

One of the ways in which political campaign apps collect data is by asking users to share their contacts with the app. Here, a screenshot from the blog of uCampaign, the company that developed the America First app to support Donald Trump's presidential campaign, we see how the app asks users to allow access to their contacts in a GOTV drive. The app gamifies the process by measuring how many personal messages the user has sent to meet their 'Personal Goal.'

Source: https://blog.ucampaign.co/2016/12/20/trump-and-brexit-used-a-new-digital-organizing-tool-to-help-achieve-their-surprise-victories/, accessed 3 December 2018
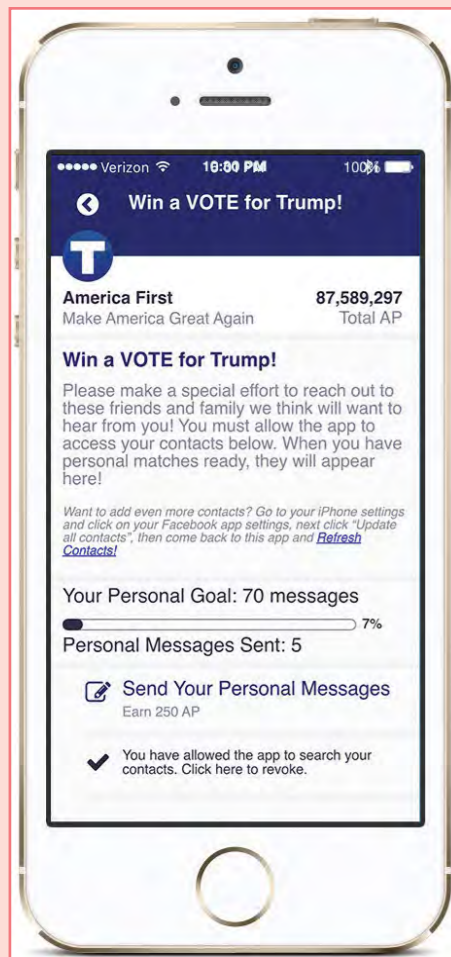

This screenshot from a uCampaign blog article of the official Donald Trump 2016 presidential campaign app, America First, shows some of the actions that can help users earn 'action points', abbreviated to 'AP' in the app.

Source: 'Trump and Brexit used a new digital organizing tool to help achieve their surprise victories', https://blog.ucampaign.co/2016/12/20/trump-and-brexit-used-a-new-digital-organizing-tool-to-help-achieve-their-surprise-victories/, accessed 3 December 2018
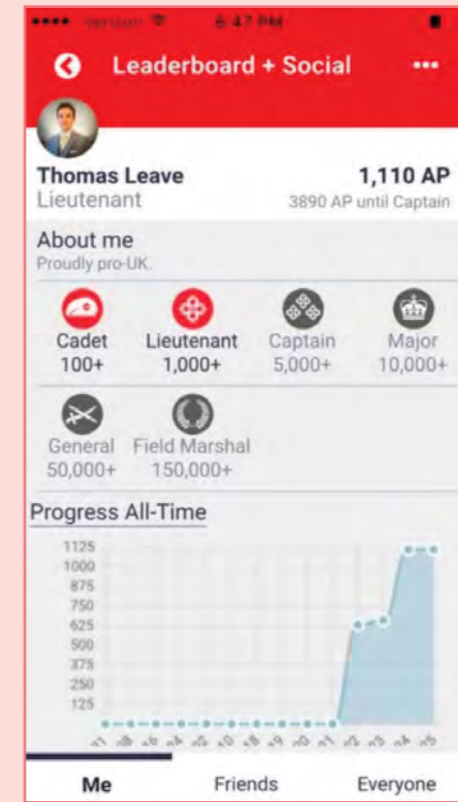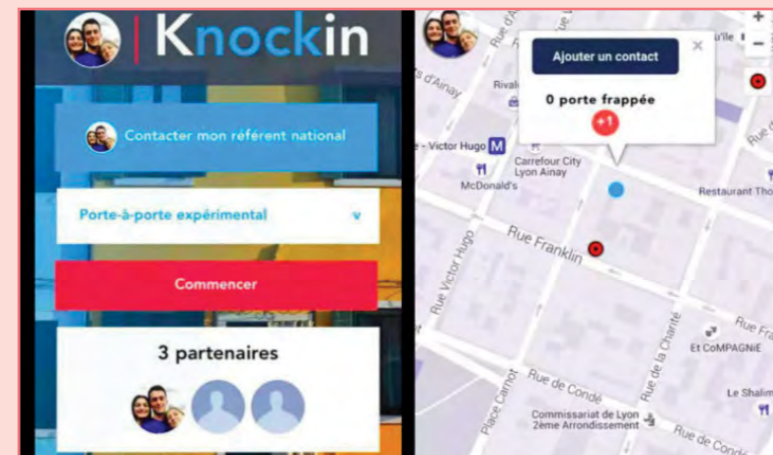

A screenshot from a uCampaign blog article of Vote Leave's app showing the different badges users can unlock by accumulating 'action points' ('AP'). Users can also compare their point total against their in-app friends and all other app users.

Source: 'Trump and Brexit used a new digital organizing tool to help achieve their surprise victories', https://blog.ucampaign.co/2016/12/20/trump-and-brexit-used-a-new-digital-organizing-tool-to-help-achieve-their-surprise-victories/, accessed 3 December 2018

A screenshot of Knockin, an app developed and used by French presidential candidate Nicolas Sarkozy's team. The mobile app shows a map with red spots that identifies a supporter of the right-wing candidate at their address. The app prompted public debate and was generally considered invasive.

Source: 'France: Data Violations in Recent Elections', 7 December 2018, https://ourdataourselves.tacticaltech.org/posts/overview-france/

A screenshot of the game Fiscal Kombat, created to support French presidential candidate, Jean-Luc Mélenchon. The protagonist Mélenchon shakes money from Christine Lagarde, chairwoman of the IMF, to collect money for his policies.

Source: 'Fiscal Kombat', http://fiscalkombat.fr/, accessed 20 February 2019

"App supporters have completed over 20,000 political ID surveys about themselves, their friends and their neighbors, generating valuable cross-section data on the supporters' political views, activism affinities and personal network, essential information for a modern, data-driven campaign."

THOMAS PETERS, CEO OF uCAMPAIGN

Considerations

↘ Overall, campaigns claim that apps help them operate more efficiently.

↘ Apps can enhance the efficiency of canvassing efforts, which may increase participation in elections.

↘ Campaign apps collect a lot of data, much of it without the user's clear consent or awareness.

↘ Voters who may not want to receive messages from a certain campaign may have their names, email addresses, places of work, websites and other contact data shared without their permission or knowledge via an address book contact.

↘ By profiling voters' homes and tailoring canvassers' talking points, enhanced canvassing apps can make interactions more personalised, but they can also feel like an invasion of privacy.

↘ To the extent that canvassing can encourage voters to vote, selectively knocking on doors believed to support one candidate and skipping those thought to support the opposition is problematic. Companies that focus on knocking on the 'right doors' and making the 'right calls' implicitly attempt to avoid spending resources on those assumed to be politically misaligned or unengaged.[14]

↘ While gamified campaign apps can help high scorers accrue social capital, they also risk publicly shaming or pressuring some voters to be more politically engaged as measured by the app's scoring system.[15]

↘ Because apps attract people who think similarly and circumvent the ideological diversity of larger social networks, they risk creating filter bubbles and perpetuating confirmation biases.

↘ Because these digital products often survive in some form post-election, they set a precedent for a never-ending campaign season.

1

Haley Thompson, 'How NPG VAN's Software Fixed Canvassing', Chronicle of the Week, 16 April 2018, https://chronicleweek.com/2018/04/ngp-van-canvass-solution/, accessed 3 December 2018.

2

'Episode 41: Online Political Games', Simplecast (podcast), 1 January 2018, https://simplecast.com/s/7a499a50, accessed 3 December 2018.

3

https://corbynrun.com/, accessed 3 December 2018.

4

'Fiscal Kombat: French presidential candidate Jean-Luc Melenchon stars in video game', 11 April 2017, https://www.bbc.com/news/world-europe-39569301, accessed 20 February 2019.

5

Sean J. Miller, 'Should down-ballot campaigns invest in an app?', Campaigns & Elections, 12 April 2017, https://www.campaignsandelections.com/campaign-insider/should-down-ballot-campaigns-invest-in-an-app, accessed 20 February 2019.

6

Thomas Peters, 'We Are the Stealth Start-up that Helped Ted Cruz Win Iowa', Medium (blog), 5 February 2016, https://medium.com/@uCampaignCEO/meet-the-stealth-startup-that-helped-ted-cruz-win-iowa-fea6745b8a6d, accessed 3 December 2018.

7

Scott Detrow, 'Cruz's Crew: You Play the Game but It's the Campaign that Scores', NPR's Morning Edition, 9 November 2015, https://www.npr.org/2015/11/09/455225893/cruzs-crew-you-play-the-game-but-its-the-cruz-campaign-that-scores, accessed 5 July 2018.

8

Peters, 'We Are the Stealth Start-up that Helped Ted Cruz win Iowa'.

9

The day after these findings were published, the app's privacy policy was updated to allow sharing of data with third parties. Krishn Kaushik, 'Narendra Modi App asks for sweeping access', The Indian Express, 26 March 2018, https://indianexpress.com/article/india/namo-app-asks-for-sweeping-access-camera-audio-among-22-inputs-facebook-data-leak-5111353/, accessed 4 December 2018.

10

Aman Sharma, 'Modi's digital cabinet: NaMo mobile app to tap ministers and MPs', The Economic Times, 1 August 2016 https://economictimes.indiatimes.com/news/politics-and-nation/modis-digital-cabinet-namo-mobile-app-to-tap-ministers-mps/articleshow/53482384.cms, accessed 4 December 2018

11

Thomas Peters, 'We built the app that helped reelect the president of the Dominican Republic by a landslide', Medium (blog), 22 May 2016, https://medium.com/@uCampaignCEO/we-built-the-app-that-helped-reelect-the-president-of-the-dominican-republic-by-a-landslide-28cf3666c050, accessed 20 February 2019.

12

Judith Duportail, 'The 2017 Presidential Election: The arrival targeted political speech in French Poliitics', Tactical Tech, https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-france.pdf, accessed 20 February 2019.

13

Tim Starks, 'Report: Presidential campaign apps failing to safeguard data', Politico, 25 April 2016, https://www.politico.com/story/2016/04/2016-campaign-apps-fail-222394, accessed 3 December 2018.

14

NGP VAN promotional video, https://www.youtube.com/watch?v=xY0ZaIONwjI, accessed 20 February 2019.

15

Aarti Shahani, 'Mobile Apps: a digital take on political canvassing', NPR, 1 November 2012, https://www.npr.org/2012/11/01/164129881/mobile-apps-a-digital-take-on-political-canvassing, accessed 3 December 2018.

No. 10

Cronia

Dey

Third-Party Tracking: Cookies, beacons, fingerprints and more

"A recent assessment identified 70 different tracking technologies used to capture actions like email opens."

What is third-party tracking?

If a political campaign wanted to target their advertisements to women interested in the Bible, conservative politics and the environment, it could turn to one of the scores of marketers and data brokers who have amassed large troves of personal data. This is precisely what Jim Bender's New Hampshire Senate campaign did in 2010 with the help of a marketing firm called RapLeaf.[1] But how did RapLeaf know who was interested in the Bible and also concerned about the environment? And how do campaign ad tech companies ascertain this sort of information across the millions of voters on whom they boast having data?[2] The answer is tracking services.

A wide range of tools are used to track users as they surf the internet or access services on a mobile phone.[3] These are used across digital services and the marketing industry and include cookies, tracking pixels, browser fingerprinting, web beacons, IP targeting, HTML storage, GPS data and more. In recent years, there has been substantial growth in political and commercial tracking services.[4] Virtually all political campaigns use them.[5] In fact, many specifically promote a 'political cookie', a piece of data that can be used to match a person's online identity with their offline details, like 'party registration, voting history, charitable donations, address, age, and even hobbies'.[6] When voter files are supplemented with data purchased from data brokers, as the CEO of one targeting firm explained, 'working with about 100 high-traffic websites that register their users, they can match the offline data to the online identities of individuals'.[7]

This matching is possible because many campaign websites reserve the right to share their visitors' information with unaffiliated third parties in the legal jargon of their privacy policies.[8] In recent congressional elections in the US, third-party trackers were found on 87% of websites affiliated with candidates.[9] Data protection regulation, where it exists, can be ineffective: none of the eleven candidates' websites in the 2017 French presidential elections fully obeyed the country's legal requirements regarding consent and the use of cookies.[10]

How is your data used?

Cookies: Not all cookies are bad; in fact, cookies are legitimately used by a wide range of websites to remember useful things like your login details, preferences and items in your shopping cart.[11] These first-party cookies improve your user experience, while third-party cookies can track your browsing.

Third-party cookies are a greater concern for privacy because cookies from the same tracking company can monitor various sites. To illustrate: in the run-up to an election, a voter may want to research candidates by visiting their affiliated websites. Even when the candidates and parties are different, these sites could be showing ads using the same service. This ad serving company could monitor activities like donations, signing up for a newsletter, or even what is clicked on. A tracking company could then cross-reference the user's browsing activity and combine it with external data sources that profile the voter. Then, further browsing—even on seemingly unrelated sites— could contain ads that promote candidates or views based on the information gleaned by the tracking cookies during the voter's initial research.[12, 13]

Tracking Pixels: Tracking pixels are single-pixel transparent images that exist within some websites but come from a third-party. While they are invisible to the user, this seemingly discrete connection allows third parties to glean useful information about your device such as your system hardware, browser configuration and IP address. Apart from your browsing history, tracking pixels can be used to determine whether emails are opened or not. Campaigns also use them to track how many people start the donation process but don't finish it, so they can streamline their donation forms.[14] NationBuilder, a popular campaigning software, has a prepared set of instructions online for 'How do I add a tracking pixel to my site?'[15]

Browser Fingerprinting: Browser fingerprinting is a technique that combines a browser's characteristics (such as time zone, language, screen resolution or installed fonts) to uniquely identify it. While cookies can be cleared and other tracking technologies can be blocked, browser fingerprinting is more sophisticated and harder to circumvent.[16]

Beacons: Beacons are physical devices that wirelessly register the presence of nearby mobile devices.[17] Beaconstac, a manufacturer of portable beacons, has proposed deploying volunteers with beacons to political campaign rallies to collect data on nearby devices, which could be used to identify attendees.[18, 19] Attendance could then be combined with other data points obtained, for instance, from third-party data brokers.[20, 21]

IP Targeting, Geofencing, and Other Technologies: Campaigns are expanding beyond tracking cookies into more sophisticated techniques such as IP targeting and geofencing. IP addresses not only identify a specific connection to the internet, but they also reveal the connection's approximate geographical location. Political campaigns are targeting devices 'anchored' in home's IP address'.[22]

Mobile devices can be tracked through geofencing, which tracks users' locations based on their GPS data or connections that can be registered by other technologies such as Bluetooth, Wi-Fi and radio frequencies. Many other techniques are proliferating: a recent assessment identified 70 different tracking technologies used to capture actions like email opens.[23]

Some examples

In Colombia: During Colombia's 2018 national election, an analysis of websites belonging to leading candidates revealed extensive use of third-party tracking tools. Of the leading 21 candidates' websites, eight had third-party Facebook trackers, 12 had Twitter trackers and 11 had some form of tracking on the donation page. Among 10 political party websites, five had Facebook trackers, seven from Twitter, and five had other trackers on the donation page. As one anonymous interviewee who managed the campaign of a Liberal party candidate explained, 'if you enter the website of [name of political candidate] and return to Facebook, images of them begin to appear. This is done using software' (namely third-party Facebook tracking software). Another digital strategist remarked, 'at a marketing level, what people do is [...] start "sticking" cookies to you from when you turn on the computer to when you turn it off'.[24]

Across the European Union: A 2018 investigation found that a number of European political party websites had Facebook tracking pixels embedded on them. The parties spanned the European continent and the political spectrum. Facebook's tracking pixel was also detected on the sites of two EU agencies.[25] The Nordic Council's digital editor explained, 'we have installed the Facebook pixel in order to expose more relevant content on Facebook for website visitors. This is mainly career opportunities or free publications and news about specific subjects that the user has showed interest in on our website'.[26]

How can I avoid being tracked?

Recently, browsers have implemented a 'Do Not Track' request; however, it is not binding, as a tracker can simply ignore the request. Browser extensions and ad blocking firewalls offer more robust defences. While cookies are currently too useful for non-tracking purposes to block outright, recent browser designs and privacy legislation is starting to limit their privacy vulnerabilities. Since 2017, Safari took measures to limit cookies and Firefox has added a 'Facebook Container', which prevents the social network from tracking you around the web.[27, 28]

In the EU, because of the General Data Protection Regulation (GDPR), websites must request consent for cookies to access the website, though many claim this form of consent is simply a barrier to access content and not a meaningful decision regarding privacy.[29] Notions of voter privacy are changing how some political campaigns deal with voter information; some offer a degree of transparency regarding their collection of data, even permitting voters to submit corrections.[30]

Some services are becoming more transparent: Google allows users to review what information the company has amassed on them for advertising purposes.[31] Despite this progress, much of the responsibility still falls on the user to avoid tracking. The Electronic Frontier Foundation, a non-profit defending digital privacy, has a free tool called Panopticlick that shows users if their browser blocks third-parties and if their browser fingerprint is unique.[32]
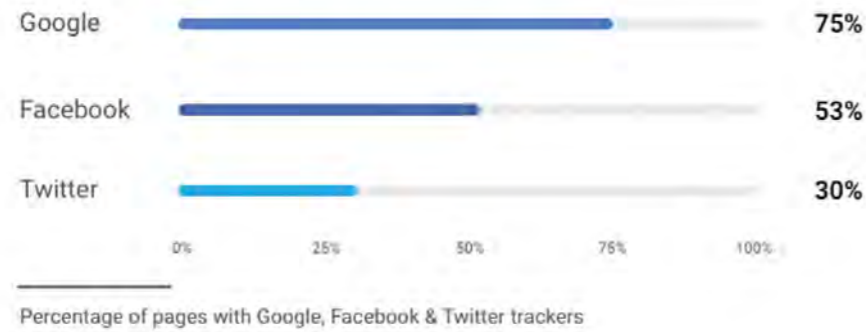
In a study by Ghostery, third-party trackers from Google, Facebook and Twitter were found on 75%, 53% and 30%, respectively, of the 981 websites affiliated with 2018 US congressional candidates.

Source: '2018 Midterm Election Study', Ghostery, 30 October 2018, https://www.ghostery.com/blog/ghostery-news/2018-midterm-elections-ghostery-study/, accessed 11 March 2019


This screenshot shows that third-party tracking services like cookies are anonymous, but companies like LiveRamp have a history of working with political campaigns and offer identity-cookie matching services.[33]

Source: 'Data Matching with Identity Graph', LiveRamp, accessed 26 February 2019, https://liveramp.com/discover-identitylink/identitylink-features/identity-graph/
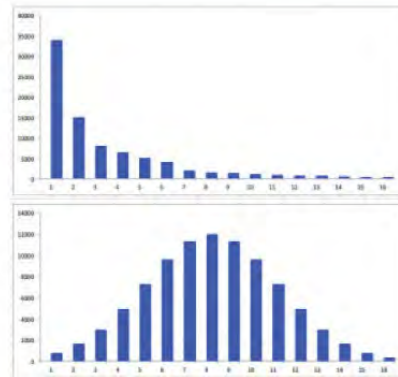
A slide deck leaked to US News & World Report from Jeb Bush's 2016 presidential campaign shows how it was 'constantly targeting the person, not the site, not the device'.

Source: 'Jeb Bush's Campaign Blueprint' 29 October 2015, https://www.usnews.com/news/blogs/run-2016/2015/10/29/jeb-bushs-campaign-blueprint

A chart showing active data collection on Colombian candidate and party websites. Notably, 38% of the 21 candidates' website contained a third-party Facebook tracker, compared to 57% from Twitter.

Source: Varoon Bashyakarla, 'Colombia: Personal Data in the 2018 Legislative and Presidential Elections', accessed 26 February 2019, https://ourdataourselves.tacticaltech.org/posts/overview-colombia/

These are stills from a video published by DSPolitical on its website. The film's voice-over confirms the link between tracking cookies and voter information: 'we take cookies and match them with the voter file'.

Source: 'DSPolitical Brings Technology It Pioneered in U.S. to UK', DSPolitical, 17 February 2015, https://www.dspolitical.com/press-releases/dspolitical-brings-technology-pioneered-u-s-uk/
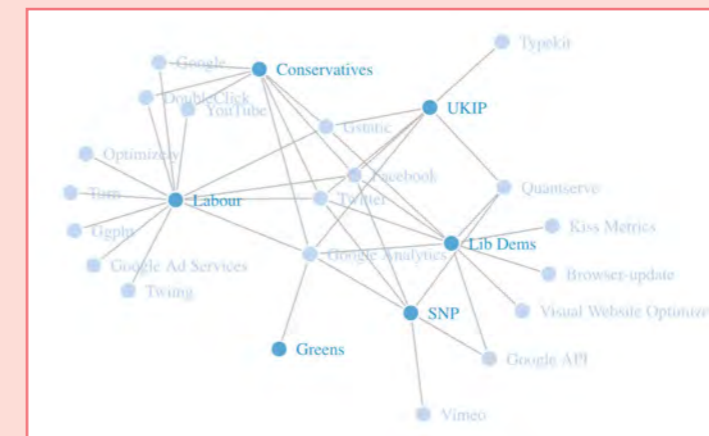
A visualisation of potential trackers on UK political party websites from June 2017, based on an investigation at Tactical Tech. Labour's website exceeded the tracker count on the Conservatives' website.

Source: Tactical Tech, 2017

Considerations

↘ Tracking can prevent users from seeing the same ad repeatedly.[34]

↘ Cookie matching can enable political campaigns to exclude voters who are not politically engaged from seeing political ads.[35, 36]

↘ Tracking helps identify click fraud, a practice in which a person or automated script repeatedly clicks on a paid ad without any real interest in it, thereby generating revenue for the website or draining revenue from the advertiser.[37]

↘ When used in a transparent and privacy-respecting way, third-party tracking can strengthen democratic foundations by, for example, promoting Get Out The Vote messages.

↘ The amount of personalisation in advertising and communication today risks skewing voters' understanding of candidates' priorities and agendas.

↘ The chain of consent is opaque and extends without end. When consenting to receiving cookies from a third-party on a given site, users have no control over whether and how that information is subsequently used and can not find out later where their information has gone. This extension of consent is particularly sensitive when consent is granted to sharing data in an apolitical context and when any captured data is later shared with a political actor. Additionally, simply soliciting users for access (e.g., click 'Accept all cookies to access this website') is not meaningful consent. Consent is only meaningful if it is an actual choice, not simply granted to a gate for the purpose of access.[38]

↘ Personalised advertising allows campaigns to show relevant ads to voters, but surveys show that voters don't want their political ads tailored to their personal interests.[39]

1

Emily Steel, 'A Web Pioneer Profiles Users by Name', Wall Street Journal, 25 October 2010, sec. Tech, https://www.wsj.com/articles/SB1000142405270 2304410504575560243259416072.

2

Sasha Issenberg, 'This Could Have Been the Election When Web-Based Ads Changed Everything. What Happened?', Slate Magazine, 26 April 2012.

3

'IAB Digital Simplified Mobile Cookies', accessed 22 January 2019, https://www.iab.com/wp-content/uploads/2015/08/IABDigitalSimplified-MobileCookies.pdf.

4

'Tracking the Trackers: Early Results', accessed 17 January 2019, http://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results.

5

Charles Duhigg, 'Campaigns Mine Personal Lives to Get Out the Vote', New York Times, 14 October 2012, https://www.nytimes.com/2012/10/14/politics/campaigns-mine-personal-lives-to-get-out-vote.html, accessed 12 March 2019

6

Jessica Leber, 'Campaigns to Track Voters with "Political Cookies"', MIT Technology Review, accessed 16 January 2019, https://www.technolo-gyreview.com/s/428347/campaigns-to-track-voters-with-political-cookies/.

7

Leber, 'Campaign to Track Voters with "Political Cookies"'.

8

'Online Trust Alliance Audit Finds 74% of U.S. Presidential Candidates' Websites Fail to Respect Americans' Privacy | Online Trust Alliance', accessed 22 January 2019, https://otalliance.org/news-events/press-re-leases/online-trust-alliance-audit-finds-74-us-presidential-candi-dates%E2%80%99-websites.

9

'Google Ad Trackers Found On 57% Of Political Campaign Sites', accessed 17 January 2019, https://www.mediapost.com/publications/article/327297/google-ad-trackers-found-on-57-of-political-campa.html.

10

Varoon Bashyakarla, 'France: Data Violations in Recent Elections', accessed 26 February 2019, https://ourdataourselves.tacticaltech.org/posts/overview-france/.

11

Simon Hill, 'The History of Cookies and Their Effect on Privacy', Digital Trends, 29 March 2015, https://www.digitaltrends.com/computing/history-of-cook-ies-and-effect-on-privacy/.

12

John Wilander, 'Intelligent Tracking Prevention', WebKit (blog), 5 June 2017, https://webkit.org/blog/7675/intelligent-tracking-prevention/.

13

'Cookie Central—What Went Wrong?', accessed 21 January 2019, http://www.cookiecentral.com/cookie5.htm.

14

'New Feature Conversion Tracking for Online Ads', ActBlue Blog, 1 July 2013, https://blog.actblue.com/2013/07/01/new-feature-conversion-tracking-for-online-ads/.

15

'How do I add a tracking pixel to my site?', NationBuilder, accessed 5 March 2019, https://nationbuilder.com/abrahamhuie/how_do_i_add_a_tracking_pixel_to_my_site.

16

Rebecca Greenfield, 'How Google Will Be Able to Track You without Cookies', Quartz, accessed 23 January 2019, https://qz.com/125470/google-can-track-you-without-cookies/.

17

'What Beacon Technology Can Do for the Election Campaign Marketing?', accessed 22 January 2019, https://www.techware.co.in/what-beacons-can-do-for-your-election-campaign-or-public-political-party-meetings.php.

18

'Beacon-Hardware-Datasheet', accessed 26 February 2019, https://resources.beaconstac.com/pdf/beacon-hardware-datasheet.pdf.

19

'How Beacon Technology Is Reshaping Election Campaign Marketing', accessed 22 January 2019, https://blog.beaconstac.com/2018/04/how-bea-con-technology-is-reshaping-election-campaign-marketing/.

20

'What Data Can a Beacon Actually Collect? - Multichannel Merchant', accessed 26 February 2019, https://multichannelmerchant.com/marketing/data-can-beacon-actually-collect/.

21

Graham Kates, Trump Campaign Changes Web Privacy Policy after Questions from CBS News', accessed 27 February 2019, https://www.cbsnews.com/news/trump-campaign-changes-privacy-policy-after-cbs-news-questions/.

22

'Political Targeting In A Post-Cookie World', AdExchanger, 2 March 2018, https://adexchanger.com/politics/political-targeting-post-cookie-world/.

23

Brian Merchant, 'How Email Open Tracking Quietly Took Over the Web', Wired, 11 December 2017, https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/.

24

Fundacion Karisma, '¿Cómo se usaron los datos personales de los colombianos en la pasada campaña legislativa?', Fundación Karisma (blog), translated from Spanish, 21 August 2018, https://karisma.org.co/como-se-usaron-los-da-tos-personales-de-los-colombianos-en-la-pasada-campana-legislativa/.

25

Peter Treffer, '[Investigation] Tory and National Front Websites Hid Facebook Tracking Pixel', accessed 17 January 2019, https://euobserver.com/jus-tice/141589.

26

Treffer, '[Investigation] Tory and National Front Websites Hid Facebook Tracking Pixel'.

27

Liam Tung, 'IOS 11 Rolls out Today with Safari Anti-Tracking: Here's Why Advertisers Hate It', ZDNet, accessed 21 January 2019, https://www.zdnet.com/article/ios-11-rolls-out-today-with-safari-anti-tracking-heres-why-ad-vertisers-hate-it/.

28

'Facebook Container Extension: Take control of how you're being tracked—The Firefox Frontier', accessed 26 February 2019, https://blog.mozilla.org/firefox/facebook-container-extension/.

29

'Cookie Consent | How to Get Valid Consent for Your Website | Cookiebot', accessed 26 February 2019, https://www.cookiebot.com/en/cookie-consent/.

30

Dave Maass, 'Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election', Electronic Frontier Foundation, 29 February 2016, https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election, accessed 11 March 2019

31

'Ad Settings', accessed 6 March 2019, https://adssettings.google.com/anonymous

32

'Panopticlick', accessed 27 February 2019, https://panopticlick.eff.org/.

33

'Revolution Messaging Case Study', accessed 26 February 2019, https://lp.liveramp.com/rs/320-CHP-056/images/Revolution%20Messaging%20%20Case%20Study.pdf.

34

'Advertising—Privacy & Terms—Google', accessed 21 January 2019, https://policies.google.com/technologies/ads.

35

Matt Petronzio, 'Can Targeted Ads Save Millions of Campaign Dollars?', Mashable, accessed 22 January 2019, https://mashable.com/2012/10/02/online-ads-politics/.

36

Leber, 'Campaigns to Track Voters with "Political Cookies"'.

37

'Advertising—Privacy & Terms—Google'.

38

Lois Beckett, 'How Microsoft and Yahoo Are Selling Politicians Access To You', ProPublica, accessed 27 February 2019, https://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you.

39

Joseph Turow, et al., 'Americans Roundly Reject Tailored Political Advertising', accessed 22 January 2019, http://web.asc.upenn.edu/news/Turow_Tailored_Political_Advertising.pdf.

JU LAH
KERUSI   PARLIMEN 144

19 0 0 0 0 0 0 0 0 1
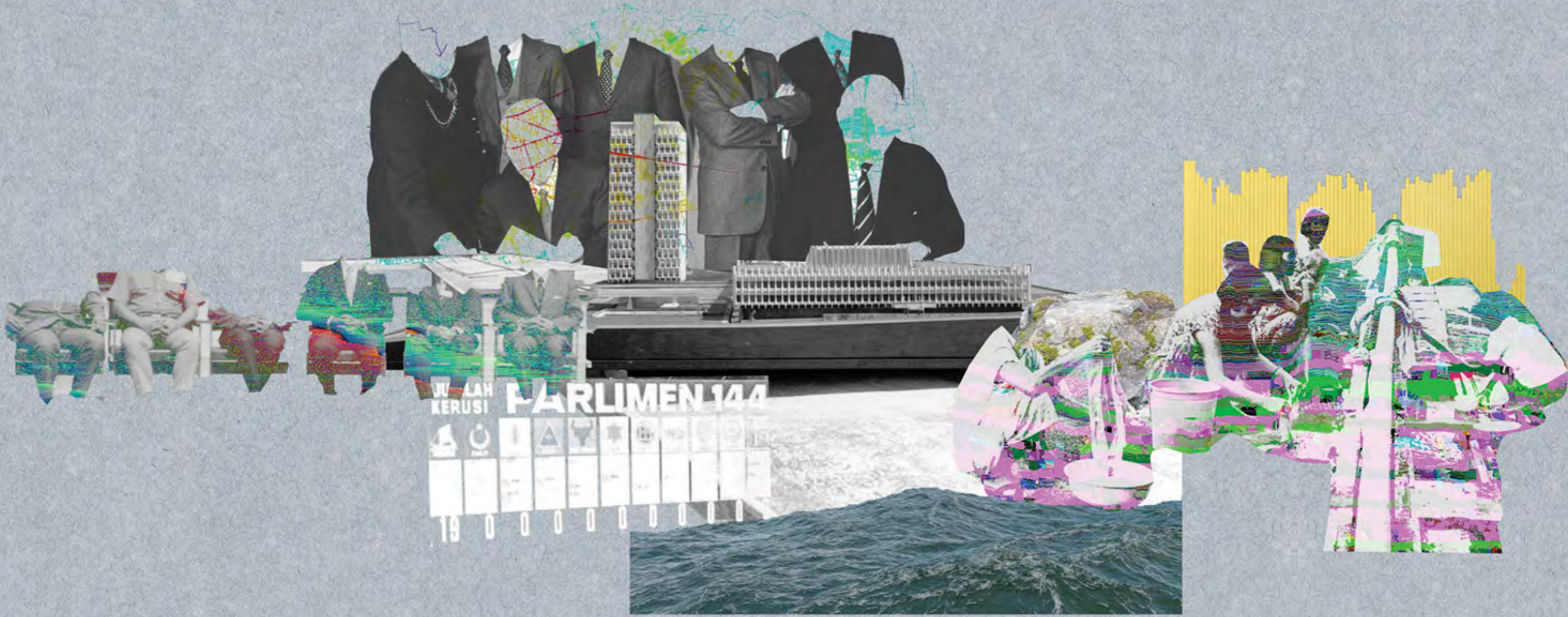
Digital Listening:
Insights from social media

"Traditionally, political strategists and campaigns use polls, calls and canvassing to ascertain voters' opinions and to take the political temperature. Digital listening technology allows them to do the same kind of analysis as these conventional tools, but far more quickly, with fewer resources, and to study larger groups of people."

What is digital listening?

When you tweet your opinion about Brexit or Trump, you probably don't expect the content of your tweet to become part of an analysis of public opinion on the topic. But the emerging field of digital listening draws from your individual interactions on social media—along with that of others—and analyses their content to assess the feeling of individual potential voters and the overall public mood. Although the majority of conclusions from digital listening studies about public political opinions are published by academic researchers or NGOs, the method is also sold as a service as a way of gathering intelligence for political campaigns.[1,2]

Digital listening is an umbrella term for monitoring and analysing what someone does or says on social media platforms such as Facebook and Twitter. Both the behaviour (retweeting, liking, sharing an image or commenting on a post) and the content (hashtags, tweets, posts and comments) are analysed.[3] Companies who offer these services are able to measure which topics are being discussed among users at a given time or to monitor the sentiment of the content, such as whether people feel positively or negatively towards a candidate. One such company, Bakamo.Social, which works with governments, NGOs and political parties, explains the services it offers through digital listening on their website:

'Bakamo go way beyond keywords and sentiment. From the gritty detail we derive broad themes that attract and motivate people to join the conversation. We understand the full social discourse, chart consumer journeys, define segments based on needs, identify factors that catalyze product choice, and more. Through their authentic voices, you get real, nuanced, and unexpected insight into consumer behavior.'[4]

How does it work?

Traditionally, political strategists and campaigns use polls, calls and canvassing to ascertain voters' opinions and to take the political temperature. Digital listening technology allows them to do the same kind of analysis as these conventional tools, but far more quickly, with fewer resources, and to study larger groups of people.

When that analysis is combined with other datasets, such as lists of the users' followers or their location, digital listening can measure the public opinion of a targeted group of people, making it a valuable tool for political candidates and campaigns.

Digital listening involves two components that automation has accelerated and scaled up: data acquisition and data analysis. First, data is gathered through software called scrapers, from social media posts, tweets connected to a hashtag, or from certain sets of people on Twitter or content from comments on Facebook posts. Data about behaviours is also gathered which help show 'engagements' on the platform such as retweets on Twitter or likes on Facebook. These interactions can be ranked as positive or negative engagements with a topic.

Next, this data is analysed using algorithms to infer different pieces of information, such as whether a tweet demonstrates a positive or a negative sentiment, by analysing the words and context in which they appear. Much of this analysis builds on recent advances in natural language processing (NLP), a kind of artificial intelligence that specialises in looking at large bodies of text. NLP is programmed not only to recognise positive and negative sentiments of certain words, or the linguistic context for the sentiment of a message, but also to develop new rules as it performs more and more analysis, making it 'smarter' over time.

Digital listening technologies, rather than replacing older tools, are usually used in conjunction with them. For example, one traditional polling organisation, YouGov, has been gathering public opinion through emails or other online methods for political parties, governments and private companies. In 2018, YouGov purchased an AI company called Portent.IO for its digital listening capabilities to complement their work.[5] Portent.IO, rebranded as YouGov Signal, carries out text and behaviour analysis on Twitter to 'distil key insights around overall engagement, opinion and market efficacy'. This is used to help understand how well any company, campaign or individual is viewed by the public, which can be helpful for politicians to understand how they can improve their status in the eyes of potential voters.[6]

How is your data used?

Data collected from social media by political campaigns can achieve a number of outcomes:

↘ The data can help campaigns understand if a candidate or issue is perceived positively or negatively, what sort of language they are associated with, and how much they are talked about.

↘ The data can show what issues people care about by analysing the most talked about topics or trending hashtags throughout an election cycle.

↘ The software can also help identify political influencers by looking at who has the furthest reach on social media and who has positive sentiment towards a political campaign.

NUVI, a social listening tool developed by Brickfish, offers services devoted to politics. The headline of their politics page reads: 'Understand what is important to your voters at any given moment. Monitor the trends and concepts that your voters are sharing and stay on top of emerging ideas'.[7] Among their services they offer to help political actors to 'stay on top of what voters are thinking', 'create lists of your influencers and detractors, and be alerted when they are talking about certain topics', '[measure] sentiment on specific issues' and '[visualise] real-time conversation data in dashboards you can access on your mobile device'.[8]

The company Crimson Hexagon, which also specialises in digital listening, offers details on how they gather insights about current political discussions from social media. For example, they recently analysed which candidates have been talked about most when announcing their run for US President in 2020. According to their information, in late 2018, 'when Kamala Harris announced she was running on Jan. 21, there were 191k tweets about her candidacy. Bernie Sanders also generated 191k tweets when he announced he was entering the race on Feb. 19'.[9] They also measured public sentiment about the elections and found that many voters were 'sad' about critical issues such as climate change and immigration; some people had 'fear' and some had 'joy' surrounding the new candidate announcements.[10]

Another company, Ossalabs, markets their Election Impact tool specifically for political campaigns.[11] Ossalabs advertise that through their tools they can help politicians 'prepare for public questions by keeping your fingers on the pulse of constituents' top of mind issues', 'discover and respond to small crises that impact electorate decisions before they become too large', 'anticipate impending attacks from your opponents' and 'understand which talking points and topics are resonating'.[12]

These three companies show the variety of types of opinions that can be measured to inform candidates about whether their talking points are working or if they should adjust them according to public sentiment.
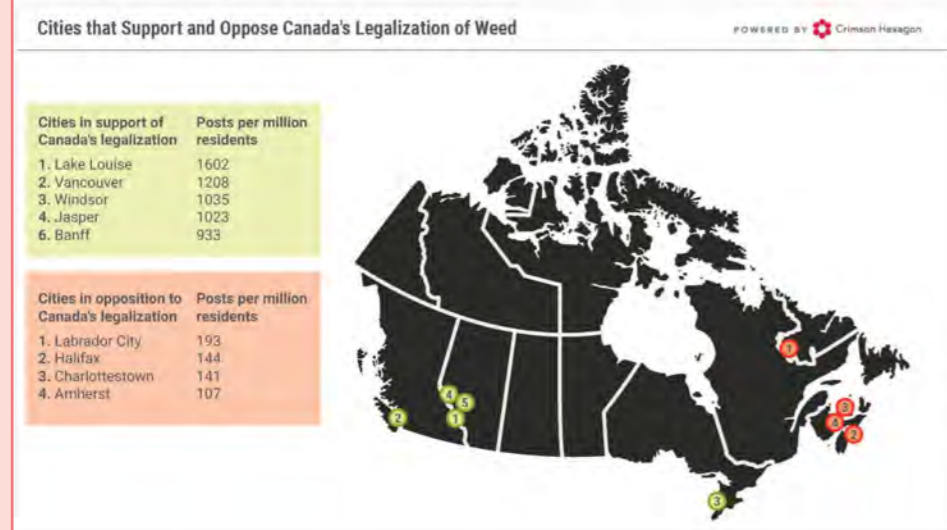
Some examples

In Taiwan: The firm AutoPolitic worked on the mayoral campaign for Taipei in 2014. AutoPolitic, in their words, 'crawls and transforms social media data into actionable intelligence'.[13] A first-time candidate running for Mayor of Taipei, Ko Wen-je worked with AutoPolitic. For Dr. Ko's campaign, the company measured public sentiment to understand 'what topics the public cared about (and why), who the influencers are (so they can engage them) and what topics the influencers are most interested in'.[14] The firm generated a list of activities and ranked them based on their predictions about how much engagement they would get based on past actions online. They concluded that Dr. Ko should engage with young people through activities including tattoos, street dancing, basketball and riding bicycles. Dr. Ko followed this advice and his visit to a tattoo parlour was considered successful, as it was shared widely on social media platforms.[15]

In India: Germin8 Social Intelligence is an Indian company that has provided digital listening research in politics. Germin8's 'social command centre' is online software that monitors 'social conversations' such as debates on Twitter or public Facebook pages.[16] They published analysis of these conversations in the run-up to the 2014 elections and published the results online, available for anyone to use. The results showed that the Bharatiya Janata Party (BJP) had a more positive message focusing on hope, whereas the Aam Aadmi Party had a critical approach that focused on issues such as corruption. A Germin8 spokesperson said how this probably impacted the success of the campaign, as a positive message is more appealing to first-time voters. This shows how digital listening can provide information that can be integrated into strategies for future campaigns.[17]

## Canada Has Legalized Weed and Banff National Park is Loving It

10.17.2018 | Culture, Politics

Cities that Support and Oppose Canada's Legalization of Weed

POWERED BY ⬡ Crimson Hexagon

Cities in support of Canada's legalization	Posts per million residents
1. Lake Louise	1602
2. Vancouver	1208
3. Windsor	1035
4. Jasper	1023
6. Banff	933

Cities in opposition to Canada's legalization	Posts per million residents
1. Labrador City	193
2. Halifax	144
3. Charlottetown	141
4. Amherst	107

In October 2018, Canada became the first major globalised economy to legalise the use of marijuana for recreational purposes. Crimson Hexagon, a Boston-based insights company, monitored the country's reaction online. According to this screenshot from their website, the day of legalisation saw 40,000 posts on social media, 56% of which were labelled 'joyful'. Sentiments were split geographically; cities in western Canada favoured the change, while those in the east opposed it.

Source: 'Canada Has Legalized Weed and Banff National Park Is Loving It', accessed 12 March 2019, https://www.crimsonhexagon.com/the-crimson-post/canada-weed-legalization-2018-10-17/
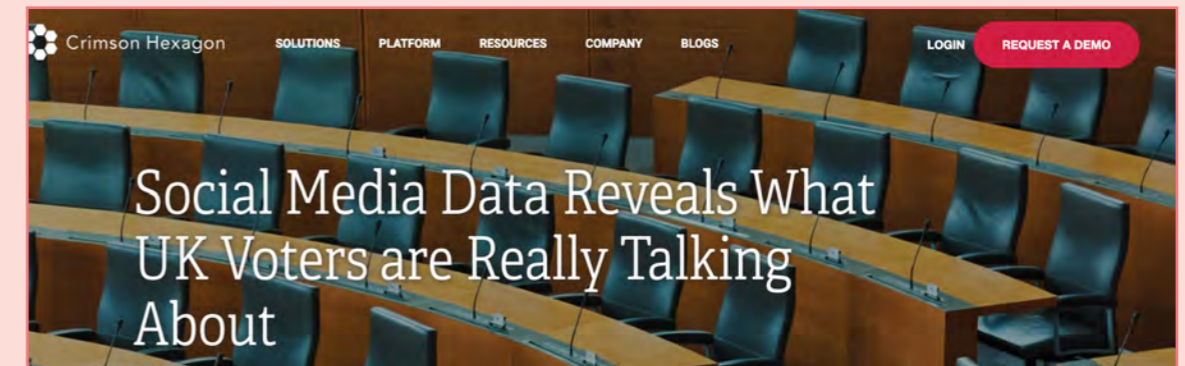
The OssaLabs social media monitoring tool helps you:
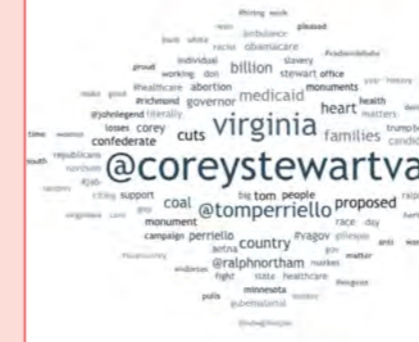
- Determine when political messages delivered online or on the campaign trail are getting lift and inspiring voters or falling flat
- Discover voter perception in real-time as a support system for the typical polling process and to monitor your brand
- Make sense of the vast collection of politically-charged messages coming from supporters and opponents on social media
- Prepare for public questions by keeping your fingers on the pulse of constituents' top-of-mind issues

Digital listening can be used to accomplish a variety of goals. OssaLabs, based in Virginia, explains how campaigns can use their services in this screenshot taken from the website. The company's name comes from Ossa, the Greek goddess of both rumour and fame.

Source: 'Political Campaigns', OssaLabs, accessed 12 March 2019, http://www.ossalabs.com/political
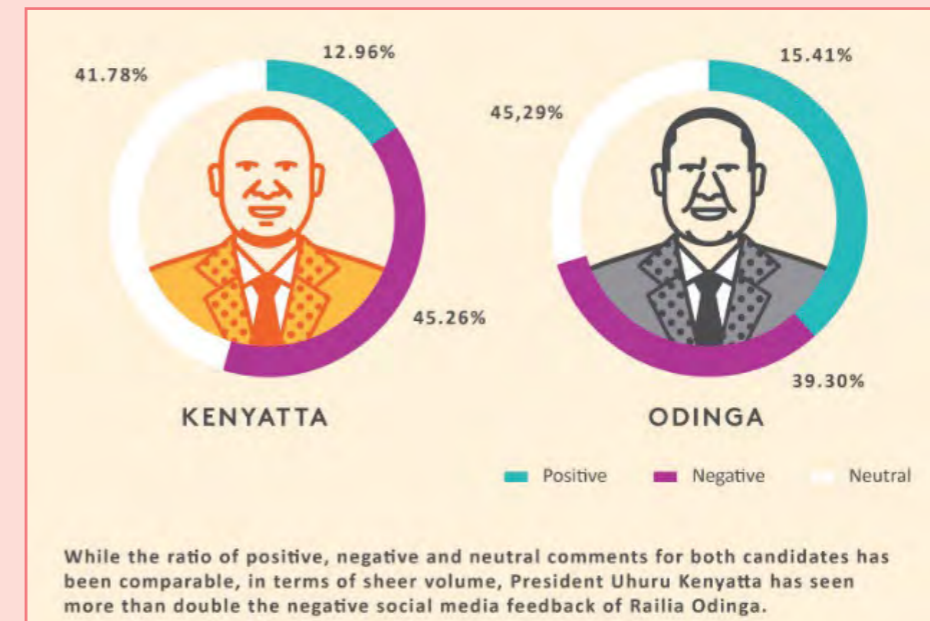
In Politics, reputation matters above all

Millions of politically-charged conversations are taking place on social media every day, so how do you keep on top of it all? Do you know what the public really think about the important topics? About you and your political track record? NUVI allows you to gauge at any moment how the public perceives you.

REQUEST A DEMO

NUVI, a social media mining company based in Utah, markets to political campaigns. This screenshot from its website previews information about the gender of a client's followers, where they are based, how engaged they are, and how these vary over time. Intelligence of this sort can be used to craft future political messages.

Source: 'Politics - NUVI - Real-Time Social Intelligence', accessed 12 March 2019, http://marketing-stage.nuvi.com/politics/

Social Media Data Reveals What UK Voters are Really Talking About

In this blog post from 2015, Crimson Hexagon explains some of its findings on voters in the UK. The blog post states that UK Independence Party voters on social media are '40x more likely to be interested in Jihad' than other users and that Labour supporters are '26x more likely to be interested in wildlife' than others.

Source: Crimson Hexagon, 'Voter Interests UK Election | Affinity Analysis Politics', accessed 12 March 2019, https://www.crimsonhexagon.com/blog/social-media-data-reveals-what-uk-voters-are-really-talking-about/

KENYATTA 41.78% / 12.96% / 45.26%

ODINGA 15.41% / 45,29% / 39.30%

■ Positive ■ Negative ☐ Neutral

While the ratio of positive, negative and neutral comments for both candidates has been comparable, in terms of sheer volume, President Uhuru Kenyatta has seen more than double the negative social media feedback of Railia Odinga.

A screenshot from a blog post belonging to the company Meltwater shows their measurements of sentiments towards Kenyan presidential candidates Uhuru Kenyatta and Raila Odinga.

Source: Philippa Dods, 'Kenya-Elections-Online-Media-Analysis', South Africa — Meltwater (blog), accessed 12 March 2019, https://www.meltwater.com/za/kenya-elections-online-media-analysis/

"Some organisations are explicit that they are on Twitter to monitor Twitter behaviour; others are not. This makes it difficult to know definitively whether you are being 'listened' to."

How do I know if it's being used on me?

Digital listening companies frame their methods as measuring what is said in 'public'. There is little transparency as to the full extent of this monitoring of 'public' space. Some organisations are explicit that they are on Twitter to monitor Twitter behaviour; others are not. This makes it difficult to know definitively whether you are being 'listened' to. You can, however, assume that by talking in a public online space, such as Twitter, or if you have a public Facebook account or talk in public Facebook groups about politics, your data could be collected and used in ways outlined above.

Considerations

↘ Digital listening can circumvent some of the problems associated with conventional opinion-gathering, such as self-censorship and the Hawthorne effect (the effect by which subjects may behave differently when they are aware that they are being observed).

↘ Digital listening allows campaigns to assess and measure the opinions and sentiments of much broader and larger groups of people than traditional methods of polling and surveys.

↘ Digital listening focuses on behaviour instead of aspiration or attitude—it provides 'unfiltered' opinions.

↘ Users rarely provide or are asked for explicit consent to be part of digital listening analyses, but companies justify it by the collection of data from 'public' spaces. Bakamo.Social's slogan, 'Insights without asking' suggests that this lack of consent can be seen as an advantage.

↘ Though digital listening service providers suggest that 'sentiment is pretty simple to understand. It's just a feeling or emotion, an attitude or opinion',[18] opinion is not 'simple' to gather. Rather, digital listening focuses on present tense as a way of predicting what people want or will want in the future —which is not necessarily a reliable method.

↘ Further, though digital listening might help reach or measure different sets of groups to those who are surveyed through traditional techniques, it is limited only to those people engaging in political discussions through social media online and therefore gives a limited perspective.

1

Dave Nyczepir, 'The Next Step in Online Persuasion', Campaign and Elections, accessed 12 March 2019, https://www.campaignsandelections.com/campaign-insider/the-next-step-in-online-persuasion.

2

'2017 French Election Study Microsite', Bakamo Social, accessed 12 March 2019, https://www.bakamosocial.com/frenchelection.

3

Kristof Varga, 'Why European Campaigns Should Invest in Social Media Listening', Campaigns and Elections, accessed 12 March 2019, https://www.campaignsandelections.com/europe/why-europeancampaigns-should-invest-in-social-media-listening.

4

'Bakamo.Social | Strategic Social Listening | Insights without Asking', accessed 12 March 2019, https://www.bakamosocial.com/.

5

Steve O'Hear, 'YouGov Acquires Portent.IO, accessed 12 March 2019, https://techcrunch.com/2018/12/18/yougov-acquires-portent-io/.

6

'How We Work', YouGov Signal, accessed 12 March 2019, https://yougov-signal.com/how-we-work/.

7

'Politics - NUVI - Real-Time Social Intelligence', accessed 11 March 2019, http://marketingstage.nuvi.com/politics/.

8

'Politics - NUVI - Real-Time Social Intelligence'.

9

'Bernie Sanders and Kamala Harris Most Discussed Democratic Party Candidates', accessed 12 March 2019, https://www.crimsonhexagon.com/the-crimson-post/bernie-sanders-kamala-harris-most-discusseddemocratic-party-candidates/.

10

'Bernie Sanders and Kamala Harris Most Discussed Democratic Party Candidates'.

11

'Election Impact', OssaLabs, accessed 12 March 2019, http://www.ossalabs.com/election-impact.

12

'Political Campaigns', OssaLabs, accessed 12 March 2019, http://www.ossalabs.com/political.

13

'Case Study', AutoPolitic, received on 5 August 2018

14

AutoPolitic.

15

AutoPolitic.

16

Elonnai Hickok, 'Digital Platforms, Technologies, and Data in the General Elections in India', 2018, accessed 11 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-india/.

17

Rohan Swamy, 'Did Social Media Really Impact the Indian Elections?', Gadgets 360, 20 May 2014, accessed 11 March 2019, https://gadgets.ndtv.com/social-networking/features/did-social-media-reallyimpact-the-indian-elections-527425.

18

Brittany Berger, 'How to Use Social Media Sentiment Analysis for Listening', The Mention Blog, 2017, accessed 12 March 2019, https://mention.com/blog/social-media-sentiment-analysis.

Data as Influence

Whether bought from data brokers, accessed through large-scale platforms or gathered through volunteers, widespread access to personal data on millions of citizens allows for micro-targeting with the aim of creating influence. The personalisation of messaging is, at present, largely delivered through digital advertising. While debates exist about its effectiveness, it is rapidly becoming an essential tool in persuading people not just what to vote for, but also what not to vote for.

Many voters feel too steadfast in their political alliances to be swayed by ads, but micro-targeting is honed to convince the undecided or those who are less inclined to vote. It can also be used for other ends: raising money, increasing solidarity or garnering the support of political influencers and their social circle. It can also be a form of alternative messaging from the media and a way to influence wider opinion, spread confusion, or in some cases, a method for attempting to suppress votes within certain targeted populations.

Several different techniques are used for micro-targeting individually or in combination. Micro-targeted ads can be delivered to individuals based on information about daily habits and routines, personality traits or assumptions about what kind of person you are, where you are physically at a given moment, or what you are searching for online or watching on television.
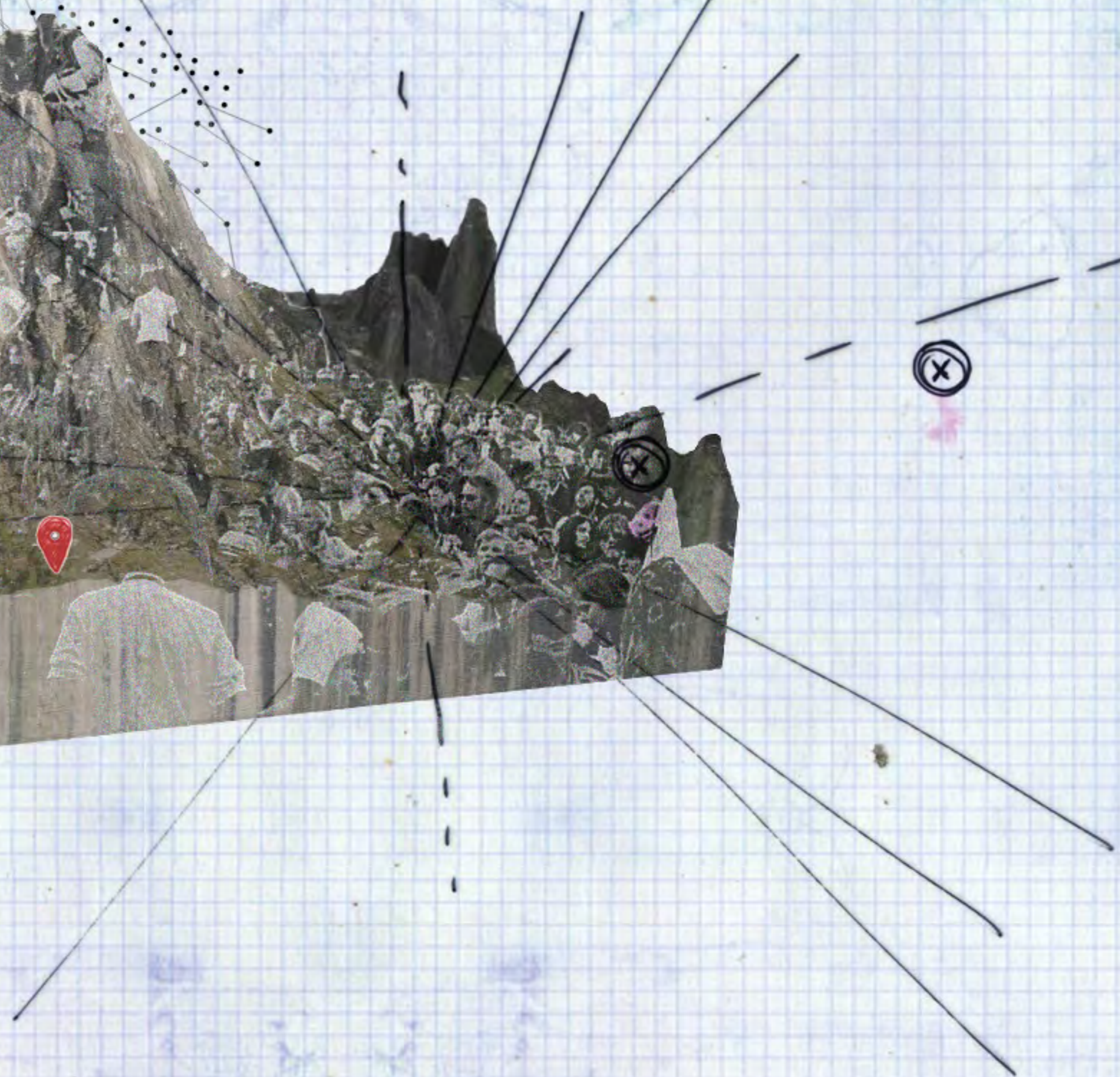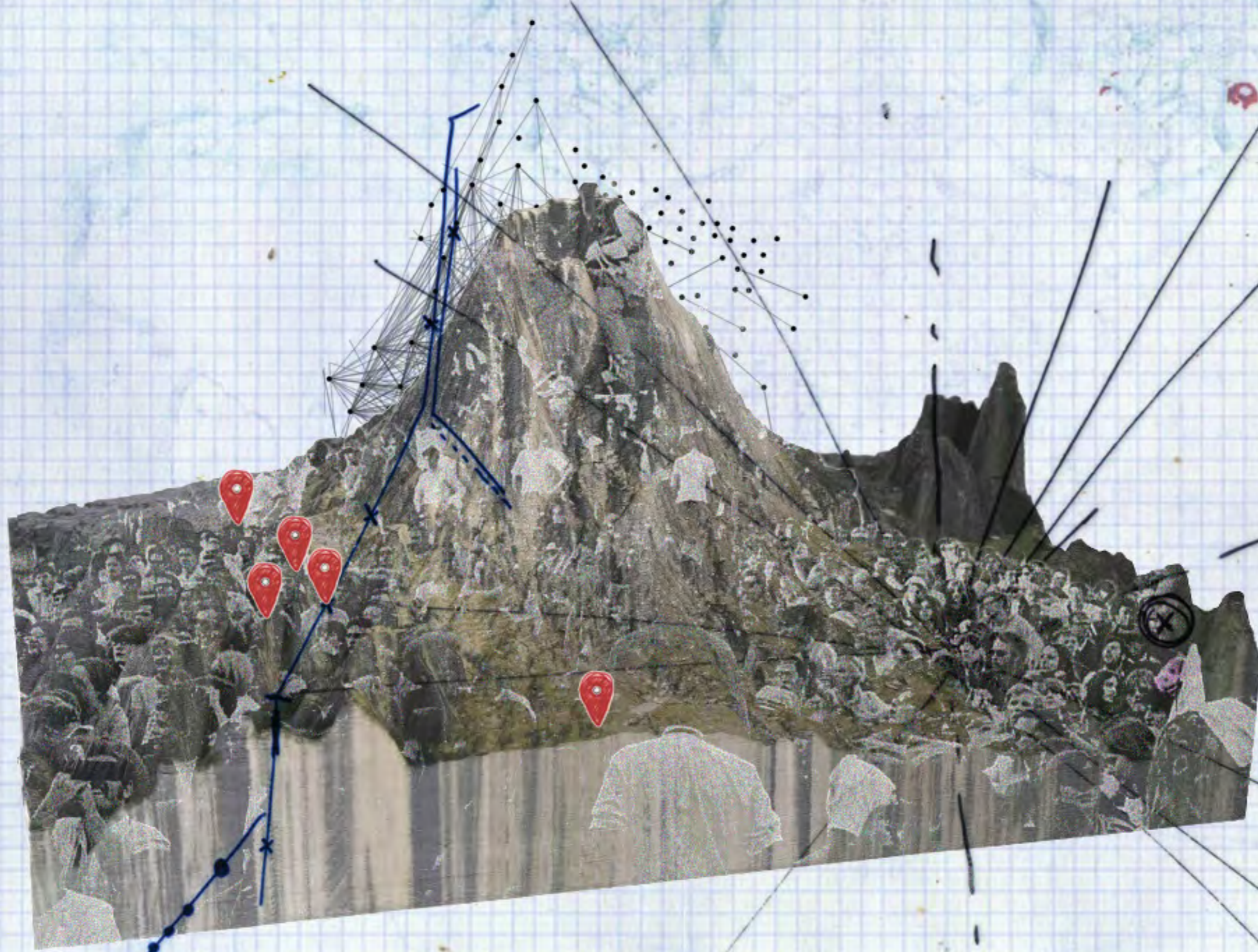
Geotargeting:
The political value
of your whereabouts

What is geotargeting?

Geotargeting is the practice of using your location information —anything from the city you live in to your exact GPS coordinates—to target you with particular ads or messages. Your geolocation can reveal where you live, where you work and what you do on the weekends. It can give clues about your fitness routines, your trips to the supermarket and your outings to the local cinema. Because your location data has so much potential to reveal what you're interested in and what you value, it is a valuable asset for political campaigns.

Campaigns have long practised basic geotargeting by treating swing districts and stronghold districts differently. Today, with the rich behavioural information extracted from location data, they can target voters much more precisely. Political parties can harness your location information from a variety of sources, including self-reported forms, publicly available voter rolls, private companies and data brokers, location-enabled services, APIs connected to location-based apps, data licensed from third-party providers and more.[1] As the number of sensors around the world increases, location data will become even more accessible.[2] Using this data, political campaigns will continue to be able to target their messages to certain districts, political rallies or events—or even to single households—with increasing granularity and precision.

Geotargeting can take many forms, but the three most established types are:

↘ **Geofencing:** creating a virtual perimeter around a point of interest to promote a message only to individuals inside that area. Geofences can be cast around individl buildings or around areas with a radius of several miles.

↘ **IP targeting:** gleaning location-based information from IP (Internet Protocol) addresses and targeting messages based on IP location information.

↘ **Mobile and property geotargeting:** targeting political messages to less granular geographic segments or aggregations, such as postal codes via the post or mobile phones via digital ads.

Some form of geo-specific micro-targeting is taking place in virtually every election campaign with basic resources around the world; nearly all campaigns use popular technology platforms to geotarget ads, whether on the city, district, neighbourhood or individual household level. More sophisticated forms of geotargeting will inevitably become more prevalent as companies expand their offerings and lower their costs in the process.

How is your data used?

In principle, you can imagine geolocation data as troves of dots representing different people moving around on a map between home, work, public transport, a concert, the park and home again. On its own, this information is more or less meaningless. It only becomes valuable when assumptions and interpretations are applied to it, perhaps informed by other sources of information. A location trace that frequents the gym is not interesting to a campaign until it is assumed or corroborated to belong to a health enthusiast, for instance. While your postal code might suggest your political persuasion, when combined with your location data, like a supermarket you regularly visit, it could suggest your attitude toward certain environmental issues. You can assume that some form of your location data—whether it's where you live or the coordinates of your mobile phone—will be an asset for a political campaign that wants to target you.

Increasingly, companies outside of politics—like The Weather Channel App (owned by IBM) and Snapchat—have started making the location data they collect about their users available to political campaigns. In 2012, The Weather Channel announced a partnership with Jumptap, a mobile ad company, for election ads. Location data that was ostensibly used to provide weather forecasts to app users was made available to political campaigns, as noted on a Weather Company website that has since been taken down.[3]

Snapchat's location data has also been used by political campaigns. In the UK's 2017 snap election, the Labour party used Snapchat to encourage young people to vote via a tool for looking up their voting location. The message was viewed 7.3 million times and 780,000 people used the tool to look up their polling place.[4] In the US, Snapchat deployed a voter registration campaign before the 2018 midterm Congressional elections.[5]

Political campaigns have also started IP targeting. DSPolitical, a political consultancy based in Washington DC, used IP and cookie targeting to serve eight million digital video impressions to 450,000 voters in the 2015 Canadian Federal elections. The company claims that its campaigns were so successful that it has since been involved with two provincial Canadian elections.[6] The Liberal Democrats in the UK used the company Digital Element, branded as 'the global IP geolocation leader', in the 2015 general election.[7]

Some examples

In the United States: In April 2016, when US Senator Lisa Murkowski was seeking reelection in Alaska, her campaign created an ad geotargeted to a single building. The ad declared Murkowski's support for building an 11-mile road through a wildlife refuge in her state, a project that the Department of the Interior (the federal agency that oversees national parks) opposed at the time. Her campaign appears to have deployed a geofence around the headquarters of the Interior Department, mere blocks away from the White House. Officials who worked in the building, browsing their newsfeeds at lunch, saw Murkoswski's ad appear 7,000 times. In January 2018, the head of the Interior Department formally approved construction of the road.[8]

In Guyana: The US-based ad tech company El Toro helped lead the opposition presidential candidate, David Granger, to victory in 2015 with the use of their IP targeting service. El Toro evidently mapped users' IP addresses to their home addresses, enabling Granger's campaign to send personalised ads to single households and devices, even when they left their homes or offices. The victory was particularly notable because the Guyanese government controlled TV and radio, rendering them unusable for the opposition candidate.[9] El Toro claims to have used their IP targeting technology in over 2,000 elections worldwide and to be able to target voters based on their physical location at any point in the previous six months.[10]

In France: The firm Liegey Muller Pons (LMP) has provided election services to over 1,000 campaigns across six European countries.[11] Because French law generally prohibits individual-level targeting, LMP helps campaigns decide which geographic districts and polling stations to prioritise, based on which ones are thought to be more amenable to a candidate's ideas.[12] LMP partnered with Cloud Factory, a 'distributed workforce company' based in Nepal, for data processing of geospatial images to help Emmanuel Macron's 2017 presidential campaign prioritise polling stations. In a blog post entitled 'French Presidential Campaign Rolls to Victory Using Geospatial AI', Cloud Factory describes how it helped LMP 'visualize electoral results, voter demographics, voting trends and other information that help candidates understand their constituencies on a deeper level'. It also states, 'Geospatial mapping can allow candidates to identify target areas and potential opportunities to connect with voters. It can help staff in the field coordinate with their colleagues in the office to identify the best spots for rallies and other election events'.[13]

National Republican Senatorial Committee

Sponsored State Geofilter Campaign

The NRSC and Snapchat partnered to let Snapchatters all over Ohio put Rob Portman on their Snaps!

Source: Snapchat Internal Data; Millward Brown Digital and Brand Lift Insights

The Story

This election season, the National Republican Senatorial Committee (NRSC) partnered with Snapchat to reach Ohio voters and drive support for Senator Rob Portman's re-election campaign. Using Snapchat's geofencing technology, the NRSC launched a series of Geofilters across Ohio to raise Senator Portman's profile among Snapchatters.

Objective

- Increase Senator Portman's name identification among Ohio voters.
- Reach potential voters who are unlikely to be on other platforms, like television.
- Develop a creative execution that Snapchatters can engage with and send to their friends.

A screenshot from Snapchat showing that Rob Portman's 2016 reelection campaign enlisted Snapchat's geofencing and geofiltering capabilities to boost Senator Portman's name identification among voters in Ohio. Snapchat estimates that the campaign resulted in a 10.8% increase in candidate awareness.

Source: 'National Republican Senatorial Committee Sponsored State Geofilter Campaign', accessed 27 February 2019, https://storage.googleapis.com/snapchat-web/success-stories/pdf/pdf_nrsc_en.pdf

With today's geospatial technologies we can take huge amounts of complex information, such as family size, socio-economic indicators, political affiliations, and other public data, and visualize it in an interactive map.

Similar to how data was used in the French election, geospatial AI collects information and maps it within the designated area. Data is then used to visualize electoral results, voter demographics, voting trends and other information that help candidates understand their constituencies on a deeper level. Geospatial mapping can allow candidates to identify target areas and potential opportunities to connect with voters. It can help staff in the field coordinate with their colleagues in the office to identify the best spots for rallies and other election events.

A screenshot from Cloud Factory's blog shows the company's geospatial technology can assist political campaigns.

Source: Wilson, Courtney. 'French Presidential Campaign Rolls to Victory Using Geospatial AI'. 23 May 2017, https://blog.cloudfactory.com/french-presidential-campaign-geospatial-ai

el toro

THE #1 POLITICAL ADTECH

Are you interested in running a political digital advertising campaign? We can help with that. El Toro's Political IP Targeting has been used in over 2,000 political campaigns to date. By leveraging your voter file, you can turn a physical address into an IP address, creating an entry point for serving digital banner and video ads directly to the home. Think of us as the digital direct mail provider of the internet! We are the only digital targeting tool that has been proven to increase voter turnout.

Additionally, via our mobile targeting product Venue Replay, you can target voters based on where their mobile devices have been seen at any point in the past six months (e.g. specific polling places, churches, community events, protests, etc.)

With our political digital advertising, you can ensure you're reaching the appropriate voters who support your campaign. So what are you waiting for? Fill out the contact form and let's discuss your next political campaign.

A screenshot from El Toro's website shows that the company claims it can target voters based on their devices' location data over a period of six months, matching it to the voters' physical addresses.

Source: 'Political Digital Advertising: Digitally Advertise with Political IP Targeting', El Toro, accessed 27 February 2019, https://www.eltoro.com/political-digital-advertising/

"Because our location histories reflect where we spend our time, and, by extension, what sorts of activities we value, they can be windows into intimate and sensitive parts of our lives."

Considerations

↘ Because our location histories reflect where we spend our time, and, by extension, what sorts of activities we value, they can be windows into intimate and sensitive parts of our lives.

↘ Geolocation data is readily accessible to entities simply willing to pay the price for access.

↘ Since geolocation data derives meaning from assumptions and interpretations drawn from it, it can be subject to bias. While part of this bias concerns the accuracy of the inferences made, the bigger concern is the way these biases can undermine democratic principles, such as by excluding people from the political process.

↘ Most people are unaware of geolocation-based practices, even if they benefit from their commercial applications.

↘ Geotargeting requires that campaigns select areas to include and areas to exclude from their political outreach efforts, exacerbating the risk of excluding certain groups from the democratic process altogether. Some services define 'high-value areas', leading some to wonder how these same services treat 'low-value' areas.[14] Others have underscored the importance that 'organizations have the ability to create hold out groups to ensure their message doesn't reach a certain population', raising questions of how geotargeting could be used for voter suppression or exclusion.[15]

↘ Geolocation-based techniques have already been used in controversial ways. Women visiting abortion clinics in several American cities (including New York City, St. Louis and Pittsburgh) have been targeted with geofenced advertisements from anti-abortion activists.[16] Reports of law firms sending ads to patients in emergency rooms have also been documented.[17] Geotargeting tactics like these can be used towards ethically dubious ends and are subject to very little oversight.

1

Allison Schiff, '2017 Marketer's Guide To Location Data', AdExchanger, 8 May 2017, https://adexchanger.com/mobile/2017-marketers-guide

2

"Location Tracking and the Trouble With "Opting In"', Ad Age, accessed 6 June 2018, https://adage.com/article/digital/mobile-location-trouble-opting/306121/.

3

Andrew Blankstein, 'The Weather Company app sued over claims it sold location data', 4 January 2019, https://www.nbcnews.com/tech/tech-news/weather-channel-sued-over-claims-it-sold-location-data-its-n954706. Original source, www.theweathercompany.com/newsroom/2014/08/19/weather-channel-partners-jumptap-national-election-advertising

4

Andrew Gwynne, 'Theresa May Called a Snap Election, but We in Labour Had Snapchat. No Contest | Andrew Gwynne', The Guardian, 15 June 2017, sec. Opinion, https://www.theguardian.com/commentisfree/2017/jun/15/theresa-may-snap-election-labour-snapchat-campaigning.

5

'2018 Midterms: Facebook, Snapchat, Lyft Turn out with Vote Initiatives', usatoday, accessed 27 February 2019, http://www.usatoday.com/story/news/politics/elections/2018/10/20/tech-companies-social-media-voter-initiatives/1592854002/.

6

'DSPolitical International', DSPolitical, accessed 27 February 2019, https://www.dspolitical.com/worldwide/.

7

'Liberal Democrats Are the First Party to Use IP Geolocation', Digital Element (blog), 28 April 2015, https://www.digitalelement.com/liberal-democrats-are-the-first-party-to-use-ip-geolocation-to-engage-voters-ahead-of-general-election-2/.

8

Kashmir Hill, 'How a Senator Used Facebook Ads to Influence Employees in a Single D.C. Building', Splinter, accessed 27 February 2019, https://splinternews.com/how-a-senator-used-facebook-ads-to-influence-employees-1793856310.

9

'El Toro LLC Contracted in David Granger's Campaign for Guyana Presidency', Louisville Business First, accessed 27 February 2019, https://www.bizjournals.com/louisville/blog/2015/06/louisville-start-up-helps-client-win-guyana.html.

10

'Political Digital Advertising: Digitally Advertise with Political IP Targeting', El Toro (blog), accessed 27 February 2019, https://www.eltoro.com/political-digital-advertising/

11

'Liegey Muller Pons', Liegey Muller Pons, accessed 27 February 2019, https://www.liegeymullerpons.fr/en

12

'The 2017 Presidential Election: The Arrival of Targeted Political Speech in French Politics', accessed 27 February 2019, https://ourdataourselves. tacticaltech.org/media/ttc-influence-industry-france.pdf

13

Courtney Wilson, 'French Presidential Campaign Rolls to Victory Using Geospatial AI', accessed 27 February 2019, https://blog.cloudfactory.com/french-presidential-campaign-geospatial-ai

14

RickRedding, 'Louisville's El Toro Helps Opposition Win in Guyana Election', Louisville KY, 16 June 2015, http://louisvilleky.com/louisvilles-el-toro-helps-opposition-win-in-guyana-election/

15

'Partner Spotlight: Q&A with Factual', The Trade Desk, 16 June 2016, https://www.thetradedesk.com/blog/partner-spotlight-q-a-with-factual.

16

'Anti-Choice Groups Use Smartphone Surveillance to Target "Abortion-Minded Women" During Clinic Visits', Rewire.News, accessed 27 February 2019, https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/

17

'Digital Ambulance Chasers? Law Firms Send Ads To Patients' Phones Inside ERs', NPR.org, 25 May 2018, https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers

Search Result Influence:
Reaching voters
seeking answers

"Google Search and YouTube's ability to serve you ads and sponsored content that are related to what you are searching for makes them particularly powerful methods for campaigns and politicians."

What is search result influence?

Searching online is one of the key ways that we discover, learn and verify information, and for that reason, the ability to influence search results is a key tool for political campaigns looking to influence or target you before and during referendums, elections and other political debates. From placing ads within your search results to seeking to influence the results themselves, political campaigns consider search to be a priority in their advertising budgets.

Google Search and YouTube are the main sources of information online for many users and are heavily relied upon for way-finding, learning and fact-checking. Google Search is the most widely used search engine in the world, dominating over 90% of the search market on desktop computers.[1] Google also owns YouTube, which is quickly becoming the second most popular search tool in the world, as increasing numbers of people use it not only for watching videos but also for searching for information and knowledge online.[2]

Google Search and YouTube's ability to serve you ads and sponsored content that are related to what you are searching for makes them particularly powerful methods for campaigns and politicians who want to get their messages across more efficiently and target them more precisely.[3] The apparent neutrality of Google Search in particular—with users seeing it as mainly a reference and discovery tool—makes it extremely attractive to political campaigners who want to spread information.

How does it work?

When you search for something in a search engine, you get two kinds of search results: 'organic' search results are controlled by the algorithm of the search engine, while 'paid' search results are normally placed through paid advertisements. These organic and paid search results appear together, with a small 'ad' sign to indicate which ones have been paid for.

Despite their apparent neutrality, search results can influence what people see and what they believe, particularly when it comes to political views. A study published in 2015 attempted to assess the impact of search rankings on undecided voters —testing what the authors call the Search Engine Manipulation Effect (SEME).[4] Their research concluded that 'Google's search algorithm can easily shift the voting preferences of undecided

voters by 20 percent or more—up to 80 percent in some demographic groups—with virtually no one knowing they are being manipulated'.[5]

Political campaigns can invest in data-driven techniques to influence two kinds of search results:

↘ **Organic search results**: Organic search results, or 'natural' search results, are served based on a search engine's algorithms. While organic search results cannot be influenced by paid ads, both advertisers and political campaigns alike often try to influence the results of organic searches—what is usually referred to as Search Engine Optimisation (SEO)—with varying degrees of success. SEO involves a series of measures to raise a site in search rankings based on assumptions about the logic of the search engine's algorithm. SEO is common practice amongst most website developers, including political sites, and there are a wide range of services available to help parties maximise results.[6] What are known as Black Hat Search Engine Optimisation methods, on the other hand, are essentially underhanded techniques outside the guidelines of search engines, which can be taken by those willing to risk being blocked by the search engine company.[7] Political campaigns have been known to use both of these techniques, though standard SEO techniques are more commonplace.

↘ **Paid search results**: In contrast to organic search results, paid search results—such as Google Ads (formerly known as AdWords)—are personalised results based on the data that the platform collects about you, including your past search history, recent locations you've visited, and in the case of Google Search, your activities within other Google products, for example YouTube videos you've watched.

Political campaigns buy Google Ads through an auction-based system, placing bids that respond to words you use in your search. These are then displayed and ranked based on how much the advertiser is willing to pay and an estimate of how relevant the ad is to the search.[8] These ads can just show key terms or display additional images and graphics or AdWord extensions, like a phone number. Additionally, Responsive Search Ads allow advertisers to make ads that have multiple variables—such as different headings and captions—and generate many different versions depending on what works.[9]

The array of services offered by Google facilitates not only political ads that respond to what you are searching for, but also a variety of strategies used by political parties to get into your search line-of-sight to deliver a particular message. As such, paid search results served to you based on your personal data can be utilised for a variety of things—not just to drive you to click or vote a certain way, but also to discredit the opposition or spread counter-information on a topical issue that may be trending in the news. In the frenzy of an election period, this can lead to a cumulative effect, with political campaigns buying ads to counter each others' claims. For example, one political campaign strategist gives advice online about how to counter ads that discredit your political campaign as follows: 'savvy voters will use the web to try and fact check ads on their own, by buying terms relevant to those negative ads, you can combat their message and refer voters to a page on your website that specifically addresses the ads' claims. With these ads, you can quickly disseminate time sensitive information and often set the record straight'.[10]

There has been much speculation about whether paid search-based political ads can influence elections. However, since May 2018, Google has made significant changes to how they handle political advertisements, in conjunction with political events and elections in several countries:

↘ In the period before the Irish abortion referendum in May 2018, Google decided to ban all advertising related to the referendum on its platform.[11]

↘ Political ads on Google Search in the US[12] are now disclosed by the company in their Transparency Report so that interested parties can see an archive of ads purchased since 31 May 2018 and get additional information, such as how many people have seen an ad and how much was spent on them.[13]

↘ The platform has put some restrictions on political ads in place, such as a requirement that political ads should carry information about who paid for them, as well as new advertiser verification requirements in connection to some elections periods, such as in India and in the EU in 2019.[14]

↘ In March 2019, Google announced they would ban political ads on their platform in the run-up to the Canadian federal elections.[15]
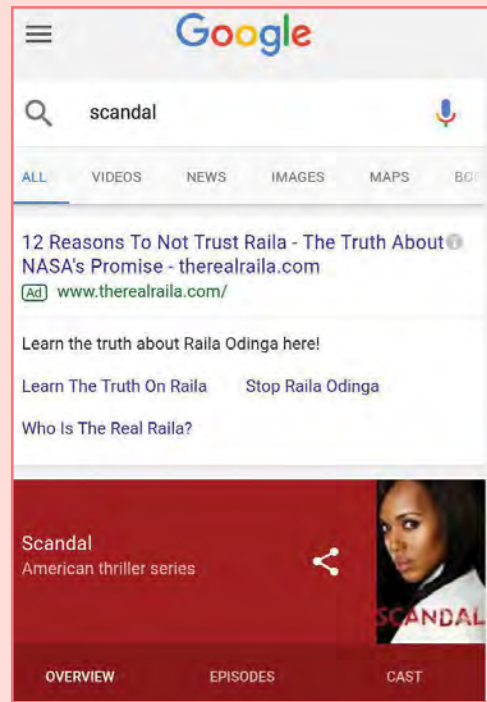
Some examples

In Kenya: In research commissioned by Tactical Tech about data-driven campaigning in Kenya, the author reports that in the run-up to the 2017 campaign between Uhuru Kenyatta, the then-president and leader of the Jubilee party, and Raila Odinga of the National Super Alliance (NASA), Kenyans reportedly saw ads on Google's Search page that cast the opposition candidate Raila Odinga in a negative light. The adverts returned results such as '12 reasons never to trust NASA' when visitors searched the word 'scandal', and screenshots were extensively shared on private messaging apps that showed that when the search term 'Unga' (maize flour) was used, the first result promoted a news-type article claiming that Kenyatta had pushed down the prices, which at the time was a hotly debated issue'.[16] This shows how influencing search results was one method both parties used to disseminate negative information about the opposition.

How do I know if it's affecting me?

Since Google has changed its policies on the declaration of political advertisements, you should be able to find a notification on an ad to check who paid for it, depending on which country you are in. However, you will not be able to find out why you are receiving that ad or based on what data or variables.

You can use Google's political ad library to check political ads that you may have seen, filtered by a specific date range, the amount spent on the ad's campaign, and media type (image, video, text). However, at the time of writing, this feature only functions in the US. Search results can also be sorted by 'most recently launched', 'spend—high to low' or 'views—high to low'. Nevertheless, political ad data that doesn't mention a specific candidate or elected federal office holder is not available on the platform as of March 2019.

Lastly, you can look at some of your account profile details that are used for both Google and YouTube searches by looking at your account information and settings.[17]
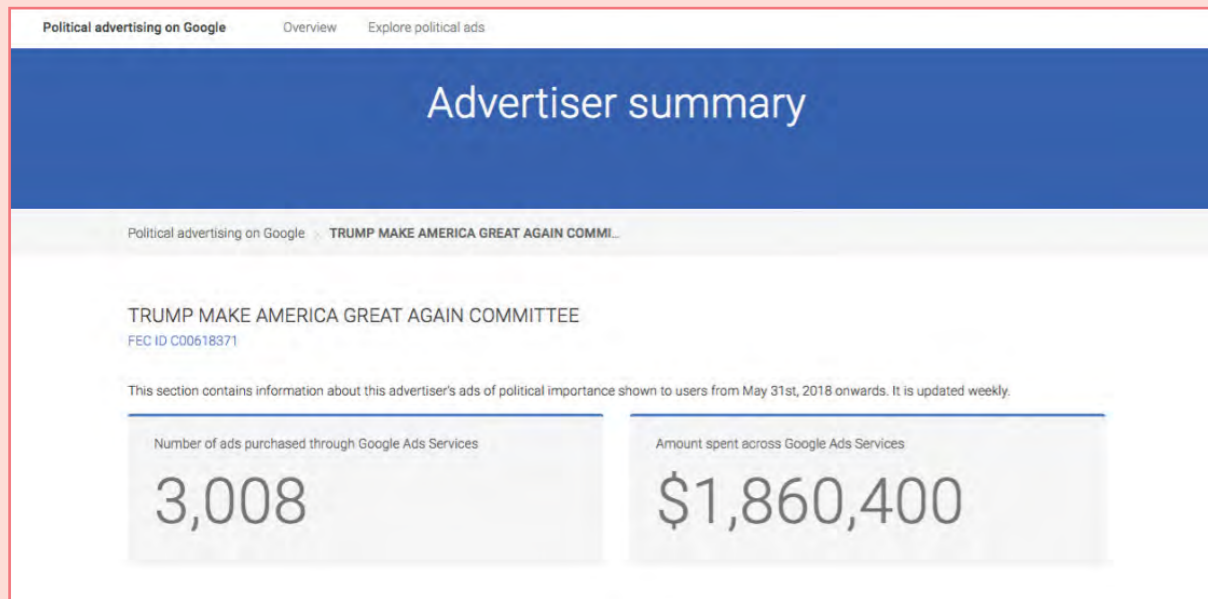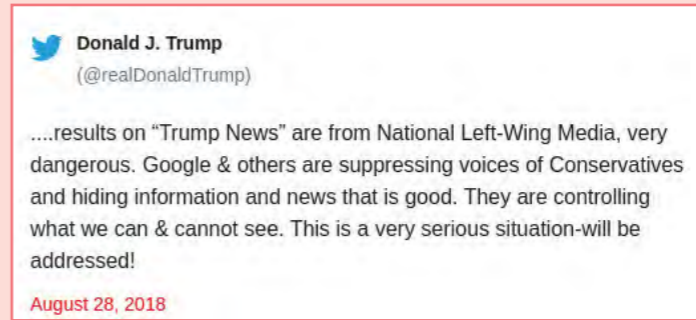
"Paid search results served to you based on your personal data can be utilised for a variety of things—not just to drive you to click or vote a certain way, but also to discredit the opposition or spread counter-information on a topical issue that may be trending in the news."

Considerations

↘ The affordability and straightforward interface of paid search results, such as Google Ads, means that political campaigns without large budgets can join debates and access audiences that may otherwise be inaccessible to them. As one campaign consultant states on their website: 'One of the really nice parts of Google Ads is that they're relatively inexpensive and can get a campaign good coverage for a tiny percentage of their media budget'.[18]

↘ Affordable search-based advertising can serve to equalise the playing field for parties who do not have the money to spend on billboard or television advertising and targeting and can facilitate highly focused campaigns.

↘ On the flip side, political parties with large advertising budgets can significantly drown out smaller parties and dominate the political narrative.

↘ It is well documented that large political parties with significant budgets have received support from Google staff services, specifically Google Search. An academic study by Daniel Kreiss and Shannon McGregor documented the work of Microsoft, Facebook, Twitter and Google's sales teams during the 2016 US presidential cycle.[19] This research was extended by a report from the Campaign for Accountability, which found: 'Google employees work inside political campaigns where they are sometimes indistinguishable from campaign hands. These embeds, offered to every presidential campaign in 2016, helped politicians target voters, craft their messages, design their ads, and even respond to opponents during and after political debates'.[20]

↘ Google's Transparency Report is an important step forward and an invaluable resource, but it does not provide the context of where, why and when these political ads were inserted, which is the most important aspect of the search engine. In addition, as digital ads become more algorithmic, with hundreds and sometimes thousands of variations being generated and served based on response, the archive will hold less value and produce fewer insights.

↘ The fact that Google dominates the search market through Google Search and YouTube means that a large amount of political faith is being entrusted to one company, which on the issue of digital political advertising is currently largely self-regulated.

↘ There has been widespread debate about the extent to which Google's algorithms themselves 'personalise' search results based on data they use to customise results so that they are more relevant, such as location, previous search requests or device type, and in turn how much this could skew the results of a search, result in 'filter bubbles',[21] or ultimately impact the political landscape. In several tweets in August 2018, Donald Trump accused Google Search of being biased against conservative media, claiming that Google Search results for 'Trump News' were 'rigged' against him because they showed only coverage from outlets like CNN and not conservative publications.[22] Despite the fact that Trump's accusations were not backed by any evidence, Google invited journalists into their meeting to find out how the search engine actually works.[23]

↘ Although Google maintains that they do not personalise organic search results, there have been significant ongoing debates about to what extent search results are optimised based on the unique characteristics of a specific search that can impact the way search results are stacked and served.[24] The amount that search is 'personalised' changes over time.[25] All of this is particularly relevant to electoral campaigns because studies have shown that filter bubbles, based on data about the search inquiry and the searcher, tend to arise more when searches are about political issues or candidates.[26] All of these examples focus on the United States, but since Google Search and YouTube are widely used globally it has implications for different contexts.

1
'Worldwide market share of search engines', https://www.statista.com/statistics/216573/worldwide-market-shareof-search-engines/, accessed 8 March 2019

2
David Mogensen, 'YouTube Content for I-Want-to-Do Moments', accessed 7 March 2019, https://www.thinkwithgoogle.com/marketing-resources/micro-moments/i-want-to-do-micro-moments/.

3
Michelle Castillo, 'Google is trying to earn more money from YouTube by capitalizing on people using it for searches', accessed 7 March 2019, https://www.cnbc.com/2018/10/01/youtube-will-now-show-you-more-adsbased-on-your-search-habits.html.

4
Robert Epstein and Ronald E. Robertson. "The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections." Proceedings of the National Academy of Sciences, Aug. 2015, p. 201419828. www.pnas.org, doi:10.1073/pnas.1419828112.

5
Robert Epstein, 'How Google Could Rig the 2016 Election', POLITICO Magazine, accessed 7 March 2019, https://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548.html.

6
Harnoor Kaur, 'SEO for Political Campaigns: Strategies for Election Season SEO Mechanic', SEO Mechanic, March 13, 2016, accessed 7 March 2019, https://www.seomechanic.com/seo-political-campaigns/.

7
John Rampton, '25 Black Hat Techniques That Are Killing Your SEO', Forbes, accessed 7 March 2019, https://www.forbes.com/sites/johnrampton/2015/07/29/25-black-hat-techniques-that-are-killing-your-seo/.

8
Google Ads, AdWords Tutorial from Google - Step 4: How AdWords Works, accessed 7 March 2019, https://www.youtube.com/watch?v=xH4Tlnes3ew.

9
'Putting Machine Learning into the Hands of Every Advertiser', accessed 7 March 2019, https://www.blog.google/technology/ads/machine-learning-hands-advertisers/.

10
'Political Online Advertising Strategies with Google AdWords', accessed 7 March 2019, http://www.newmediacampaigns.com/page/political-online-advertising-strategies-near-election-day.

11
'Transparent Referendum Initiative – For an Open, Truthful and Honest Debate', accessed 7 March 2019, http://tref.ie/.

12
At the time of writing this service was only available for US political advertisements.

13
'Google Transparency Report', accessed 7 March 2019, https://transparencyreport.google.com/political-ads/library?hl=en.

14
'Political Content - Advertising Policies Help', accessed 7 March 2019, https://support.google.com/adspolicy/answer/6014595?hl=en.

15
'Google to Ban Political Ads Ahead of Federal Election, Citing New Transparency Rules', accessed 7 March 2019, https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citingnew/.

16
Influence Industry case study on Kenya by Grace Mutung'u, 'Kenya: Data and Digital Election Campaigning', accessed 7 March 2019, https://ourdataourselves.tacticaltech.org/posts/overview-kenya/.

17
'Google Account', accessed 7 March 2019, https://myaccount.google.com/intro/data-and-personalization.

18
'Political Online Advertising Strategies with Google AdWords', accessed 7 March 2019, http://www.newmediacampaigns.com/page/political-online-advertising-strategies-near-election-day.

19
Daniel Kreiss & Shannon C. McGregor (2018)Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle, DOI:10.1080/10584609.2017.1364814

20
'Partisan Programming: How Facebook and Google's Campaign Embeds Benefit Their Bottom Lines', Campaign for Accountability, accessed 7 March 2019, https://campaignforaccountability.org/work/partisan-programminghow-facebook-and-googles-campaign-embeds-benefit-their-bottom-lines/.

21
'Measuring the Filter Bubble: How Google Is Influencing What You Click', DuckDuckGo Blog, accessed 7 March 2019, https://spreadprivacy.com/google-filter-bubble-study/.

22
Ginger Gibson and Susan Heavey, 'White House Probes Google after Trump Accuses It of Bias', Reuters, accessed 7 March 2019, https://www.reuters.com/article/us-usa-trump-tech-idUSKCN1LD1I1.

23
Jillian D' Onfro, CNBC, accessed 7 March 2019, https://www.cnbc.com/2018/09/17/google-tests-changes-to-its-search-algorithm-how-search-works.html
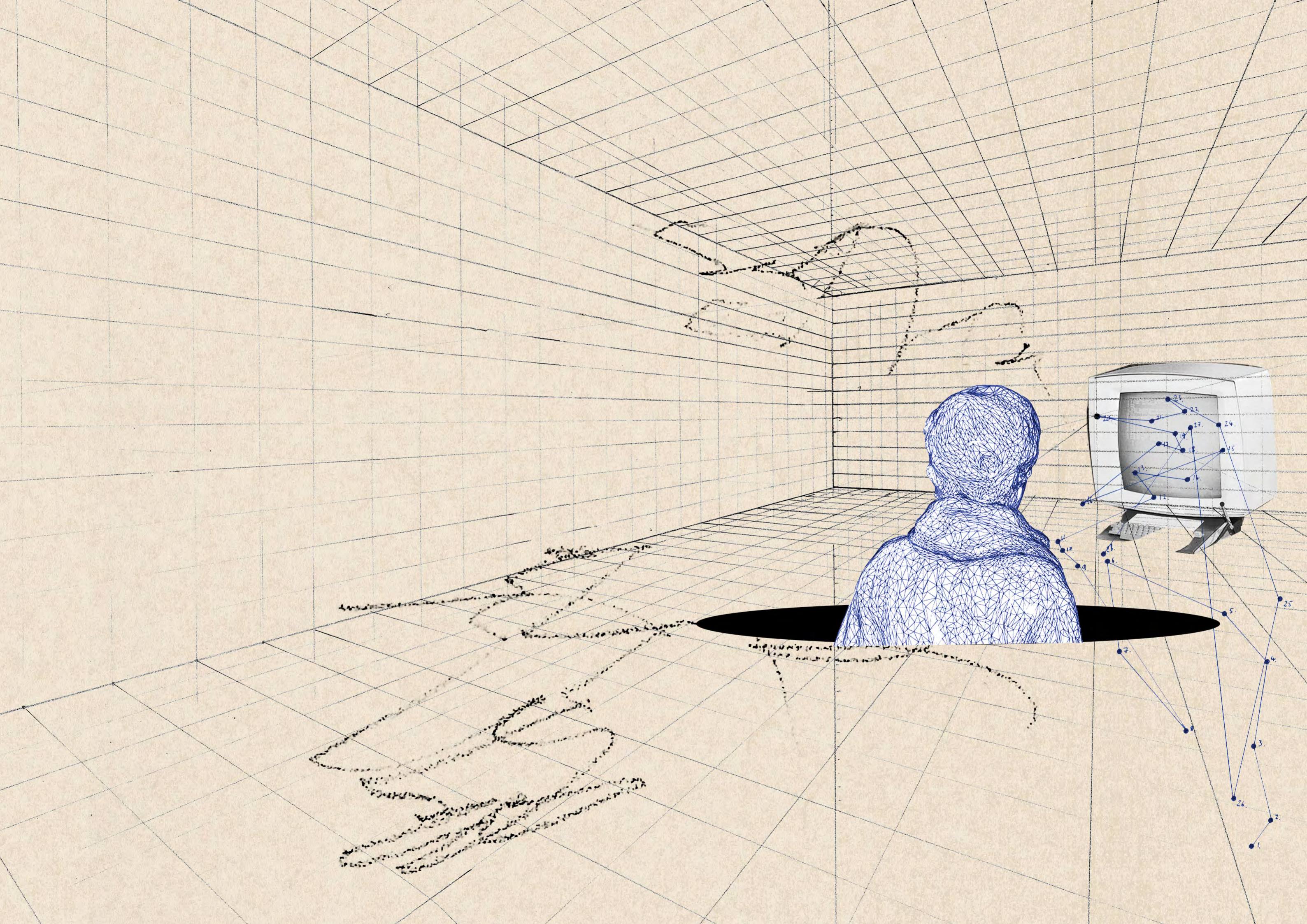
24
Nick Statt, 'Google Personalizes Search Results Even When You're Logged out, New Study Claims', The Verge, accessed 7 March 2019, https://www.theverge.com/2018/12/4/18124718/google-search-results-personalizedunique-duckduckgo-filter-bubble.

25
'Google Admits It's Using Very Limited Personalization in Search Results', Search Engine Land, accessed 7 March 2019, https://searchengineland.com/google-admits-its-using-very-limited-personalization-in-search-results-305469.

26
Julia Angwin, 'On Google, a Political Mystery That's All Numbers', Wall Street Journal, November 4, 2012, sec. Tech, accessed 7 March 2019, https://www.wsj.com/articles/SB10001424052970203347104578099122530080836.

Addressable TV: Who's watching what you're watching?

"In essence, Addressable TV enables campaigners to target advertisements to TVs with the same precision as those delivered over the internet, displayed on mobile phones, and sent via the post."

What is Addressable TV?

Data about your television-viewing habits reveals a wealth of information about your preferences, interests, lifestyle and beliefs, all of which political strategists can leverage in campaigns. Advertising on television has always been an important vehicle for political campaigning, but the rise of Advanced TV—streaming and on-demand television delivered through the internet—gives campaigners new possibilities for political advertising and micro-targeting, customisable down to the individual viewer.

Advertising via Advanced TV, commonly called 'Addressable TV' in industry lingo, allows ads to be delivered directly to specific households instead of across wide demographics like whole cities or regions, as with traditional TV advertising. In essence, Addressable TV enables campaigners to target advertisements to TVs with the same precision as those delivered over the internet, displayed on mobile phones, and sent via the post. Doing so is still relatively expensive, but some claim that traditional TV advertising costs are underestimated because of their lack of precision.[1, 2] In its white paper on Addressable TV, the consumer reporting agency Experian claims, 'Addressable TV is about the person and not the program. You and your next door neighbour may be watching the same show, but through the power of Addressable TV, end up viewing different ads'.[3]

How does it work and how is your data used?

Advanced TV delivers content over the internet from a provider to a connected device, rather than through cable networks. These connected devices include smart and connected TVs, set-top boxes like Roku or Apple TV, and gaming consoles such as PlayStation or Xbox.

The next generation of TV advertisements are called 'addressable' because advertisers can now address the needs and wants of individual users; in politics, these inferences are informed by data. Addressable TV advertising achieves individual, household-level precision using granular data. In the words of former Dish Media Sales VP Adam Gaynor, 'Addressable television doesn't work without data'.[4]

That data comes from three sources:[5]

↘ **First-party data:** in-house data that the advertiser collects on you, such as your viewing, payment and subscription histories.

↘ **Second-party data:** shared information from partnerships and affiliates. In the context of political ads, second-party data could be data from a political action committee or an issue group exchanged with a candidate's campaign to advance a political goal.

↘ **Third-party data:** data purchased from a separate source (including data brokers like Acxiom, Experian, LiveRamp, Neustar or others that specialise in political data) or supplied by a consultancy assisting with the purchase of the ads. This information ranges widely, but for political purposes it usually includes information about how persuadable you are and how likely you are to vote. The digital advertising company Altice Media Solutions gives campaigns the ability to target voters via Addressable TV using basic demographics like their ethnicity, as well as more intimate details like their stances on controversial issues.[6]

All of this personal, demographic, geographic and behavioural data is aggregated and analysed to evaluate whether you are a suitable target for a particular political advertisement.[7, 8] Ben Tatta, former president of Cablevision Media Sales, a leading provider of Addressable TV, remarked, 'it's fascinating that of all the categories we work with, political probably is the most sophisticated in terms of the use of the data'. He likened Addressable TV to canvassing efforts in which campaigns 'are knocking on doors and they kind of know the voting history of someone's house before they even knock on the door; they can apply those same principles in television'.[9]

Some examples

mitú: The multi-channel network mitú launched a campaign to focused on driving bilingual, millennial Latinos in the US to tune in to Major League Baseball games. It observed such great success that, in May 2016, it launched a political initiative called 'Take Action, Commit Others' to boost voter turnout among the same target audience. As part of this political mobilisation effort, the network organised a meet-up between Barack Obama and Gina Rodriguez, a Puerto Rican-American actress. In the end, it attracted 75 million media impressions. Multichannel networks like mitú are increasingly positioned between advertisers and platforms (e.g., Facebook, YouTube, Pinterest, Snapchat), which situates them perfectly for political influence, especially among younger voters who consume media through means other than traditional TV.[10]

D2: In 2014, D2 Media Sales became the 'largest household addressable TV advertising platform' in the US as a result of a merger between American satellite networks DISH and DirecTV.[11] D2 Media's advertising platform delivers addressable ads to nearly 22 million households.[12] The company forged partnerships with data providers for both major American political parties including i360 and Deep Root Analytics, both of which service Republican campaigns, and TargetSmart, which caters to centre-left candidates.[13, 14, 15] In 2016, D2 Media provided Addressable TV ads to over 100 political campaigns.[16]

How do I know if it's being used on me?

Most TV watchers do not consider the fact that their viewing habits and preferences can be—and sometimes are—used to shape how political campaigns communicate with and persuade them. This is partly because this development, as described here, is quite new. Though the term 'Advanced TV Targeting' was first introduced in 1990 at the MIT Media Lab, it didn't gain momentum until recently.[17] Three factors came together to facilitate the adoption of Addressable TV advertising: the 2016 American election cycle and the search for a competitive advantage, the technological infrastructure and advancement of advertising agency capabilities, and—perhaps a longer-term trend—the 'consolidation of the media industry'.[18] As the amount of content sent over IP, over-the-top and on-demand platforms reached a critical mass, Addressable TV became a viable option for political strategists. In fact, according to D2

Media Sales, the '2016 presidential election cycle [was] the first [presidential] one in which campaigns have been able to target voters with addressable television advertising'.[19] Between the 2014 and 2016 American election cycles, the use of Addressable TV increased about 60%.[20] Addressable TV is expanding to Latin America and Europe, but its adoption in political campaigning outside the United States appears to be slower.[21, 22, 23]

Considerations

↘ When implemented under certain constraints, Addressable TV can deliver ads that cater to viewers' interests.

↘ Companies offering Addressable TV services claim that it can strengthen the democratic process by improving the efficiency of political campaigns and by fostering political participation.

↘ However, advertisements served to individual households reflect a campaign's understanding of individuals living in those homes – knowledge that can be acquired through invasive or privacy-compromising means. When voters are included in an advertising campaign, addressable advertising is symbolic of 'a shift from identifying groups to identifying people', as president and CEO of digital media agency Bully Pulpit Interactive remarked.[24] The wide gap between media practices and data protections presents a host of concerns. Both Germany and the Netherlands have recognised the sensitivity of personal information processed by Advanced TV and have adopted enforcements in response.[25]

↘ Household-level targeting of political ads can easily contribute to the 'filter bubble' effect, as individual voters may understand candidates and their campaigns differently based on the information they've been served.

↘ Advertisers' data on individual households—whether directly observed or predicted—may be inaccurate or outdated, leading to political profiles and advertising campaigns unfit at best or damaging at worst. This is particularly an issue for Addressable TV: because it's relatively new, it lacks industry standards with respect to basic metrics.

↘ An awareness of logging and using data on media consumption to inform political messaging can lead to a chilling effect among voters.
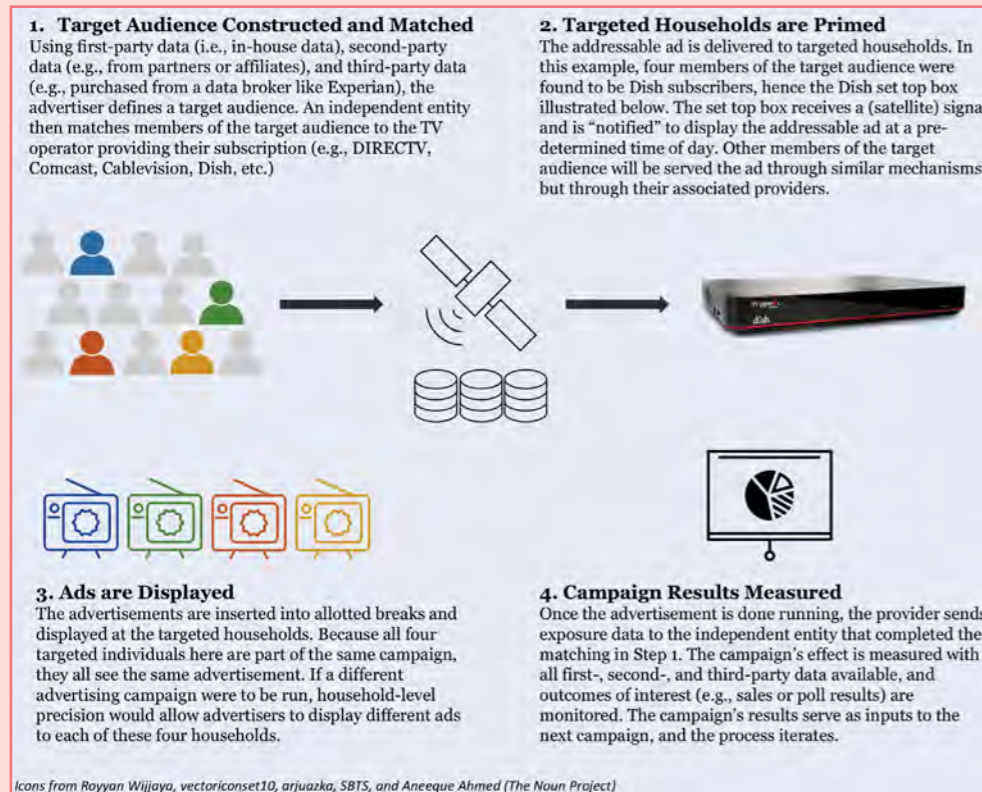
ADVANCED TV

The TV industry is undergoing an evolution. Viewers are changing the way they access content, causing viewership patterns to become extremely fragmented. Don't miss the mark with a wide audience TV ad, reach the voters who matter with precision by delivering ads to over-the-top (OTT) devices, Smart TV apps and gaming consoles.

Using rich digital data sets in combination with TV data, advertisers can determine whether their ads are driving consumers to visit their website, and what actions they are taking once there. In turn, campaign managers can efficiently use their TV budget towards likely voters, while viewers have a better user experience with ads customized to their political opinions.

A screenshot from The Trade Desk, a cross-device digital advertising company, published this short introduction to Advanced TV in the context of political campaigning.

Source: https://www.thetradedesk.com/ white-papers/making-history-programmatic-in-politics, accessed 5 March 2019

1. Target Audience Constructed and Matched
Using first-party data (i.e., in-house data), second-party data (e.g., from partners or affiliates), and third-party data (e.g., purchased from a data broker like Experian), the advertiser defines a target audience. An independent entity then matches members of the target audience to the TV operator providing their subscription (e.g., DIRECTV, Comcast, Cablevision, Dish, etc.)

2. Targeted Households are Primed
The addressable ad is delivered to targeted households. In this example, four members of the target audience were found to be Dish subscribers, hence the Dish set top box illustrated below. The set top box receives a (satellite) signal and is "notified" to display the addressable ad at a pre-determined time of day. Other members of the target audience will be served the ad through similar mechanisms but through their associated providers.

3. Ads are Displayed
The advertisements are inserted into allotted breaks and displayed at the targeted households. Because all four targeted individuals here are part of the same campaign, they all see the same advertisement. If a different advertising campaign were to be run, household-level precision would allow advertisers to display different ads to each of these four households.

4. Campaign Results Measured
Once the advertisement is done running, the provider sends exposure data to the independent entity that completed the matching in Step 1. The campaign's effect is measured with all first-, second-, and third-party data available, and outcomes of interest (e.g., sales or poll results) are monitored. The campaign's results serve as inputs to the next campaign, and the process iterates.

Icons from Royyan Wijjaya, vectoriconset10, arjuazka, SBTS, and Aneeque Ahmed (The Noun Project)

The schematic above shows one example of how addressable advertisements are delivered to individual households. D2 Media Sales' website states: "The set top box receivers in DIRECTV and DISH subscriber homes are like mini-computers. Demographic and voter file attributes specific to that subscriber are loaded on the box. Once an advertiser selects a target audience, we are then able to deliver a specific television commercial to that household during a commercial break when they are watching TV. The reporting that we are able to provide on the back end is more complete than anything ever seen in TV post campaign reporting." In practice, TV advertising is used to complement direct mail campaigns and interventions on mobile, desktop, digital radio and other media.

Source: Varoon Bashyakarla, 'Psychometric Profiling: Persuasion by Personality in Elections', 18 May 2018, https://ourdataourselves.tacticaltech. org/posts/psychometric-profiling/

POLITICAL ADVERTISING

Altice Media Solutions connects you with the voters you want to reach on over 100 of the most-watched networks on television.

CONTACT US

Altice Media Solutions offers the ability to target voters via Addressable TV using not only basic demographics but also ethnicity and political persuasion, among others.

Source: http://www. alticemediasolutions. com/amslocal/ political-advertising-0, accessed 5 March 2019

The proprietary segments created by Deep Root Analytics and made available for addressable advertising via D2 Media Sales include:

Reluctant Republicans	Disaffected Democrats
Swing Voters	Senior Swing Voters
Young Swing Voters	Women Swing Voters
Blue Collar	Hispanic Persuasion
Influentials	GOP GOTV
GOP Primary	2nd Amendment Voters
Jobs Voters	Free Trade
Energy Voters	Anti-Terrorism
Immigration	Social Conservatives
Libertarian Voters	Fiscal Conservatives
Education Voters	Health Care Voters
High Disposable Income	Minimum Wage Ballot Initiative
Pro-Marijuana Ballot Initiative	Anti-Marijuana Ballot Initiative

This screenshot was taken from a promotional video uploaded to YouTube with actress Gina Rodriguez and President Barack Obama to boost voter turnout among young Latinos living in the US. It was made possible by mitú, a multi-channel network. Positioned between platforms, their influencers and advertisers, multi-channel networks like mitú are in a prime position for influence, especially among younger audiences who consume content outside of traditional TV.

Source: 'Gina Rodriguez interviews President Obama - mitú', https://www.youtube.com/watch?v=oLLt-a6dI_0, accessed 5 March 2019

"You and your next door neighbour may be watching the same show, but through the power of Addressable TV, end up viewing different ads."

EXPERIAN WHITE PAPER ON ADDRESSABLE TV

1

Brett Hurwitz, 'Three Big Misconceptions About Addressable TV Advertising', Broadcasting & Cable, accessed 5 March 2019. https://www. broadcastingcable.com/blog/three-big-misconceptions-about-addressable-tv-advertising.

2

Jamie Power, 'Don't Believe Everything You've Heard about Addressable TV Advertising', accessed 5 March 2019. https://adage.com/article/media/perception-reality-addressable-tv today/315351/.

3

'Addressable TV: Harness the power of audience data for one-to-one targeting', accessed 5 March 2019. https://www.experian.com/assets/marketing-services/white-papers/audience-iq-addressable-tv-wp.pdf.

4

Andy Plesser, '(VIDEO) Election Sweet Spot Making Addressable Hum, DISH's Gaynor', Huffington Post (blog), 31 October 2016. https://www.huffingtonpost.com/andy-plesser/video-election-sweet-spot_b_12735720.html.

5

'Audience-Iq-Addressable-Tv-Wp.Pdf'.

6

'Political Advertising', accessed 5 March 2019, http://www.alticemediasolutions.com/amslocal/political-advertising-0.

7

Samantha Bookman, 'Cablevision Dives Deeper into Addressable TV Ads and DAI with Google Partnership | FierceVideo', accessed 5 March 2019, https://www.fiercevideo.com/cable/cablevision-dives-deeper-into-addressable-tv-ads-and-dai-google-partnership.

8

Anthony Crupi, 'Cablevision "TAPPs" Into the Power of Addressable Advertising', accessed 5 March 2019, https://adage.com/article/media/cablevision-tapps-power-addressable-advertising/298339/.

9

BeetTV, Cablevision Sees Political Campaigns Embracing Linear, Addressable TV Together, accessed 5 March 2019, https://www.youtube.com/watch?v=FtGGHuPnbjY.

10

RTL AdConnect, 'Total Video Key Facts 2017', accessed 5 March 2019, http://files.chinagoabroad.com/Public/uploads/content/files/201804/TVKF%202017.pdf.

11

Meg James, 'DirecTV, Dish Network to Vie for Political Cash with Customized Ads', latimes.com, accessed 5 March 2019, https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-political-ads-satellite-directv-dish-network-20140819-story.html.

12

Deep Root Analytics, 'Deep Root Analytics Teams Up With D2 Media Sales to Offer 26 Proprietary Political & Advocacy Audience Segments to Target TV Ads to Dish & DirecTV Households', accessed 5 March 2019, https://www.prnewswire.com/news-releases/deep-root-analytics-teams-up-with-d2-media-sales-to-offer-26-proprietary-political--advocacy-audience-segments-to-target-tv-ads-to-dish--directv-households-300330085.html.

13

'Data Dictionary DISH/DirecTV', accessed 5 March 2019, http://www.i-360.com/wp-content/uploads/2017/10/Data-Dictionary-D2.pdf.

14

Deep Root Analytics, 'Deep Root Analytics Teams Up With D2 Media Sales to Offer 26 Proprietary Political & Advocacy Audience Segments to Target TV Ads to Dish & DirecTV Households'.

15

'Democratic Candidates Step into the Future of Political Advertising with D2Media Sales', Clarity Campaign Labs, accessed 5 March 2019, http://www.claritycampaigns.com/news/2014/8/11/d2media-sales.

16

Steve Ellwanger, 'DISH & DirecTV Venture (D2 Media) Provides Addressable TV Ads For More Than 100 Political Campaigns In 2016 – Beet.TV', accessed 5 March 2019, https://www.beet.tv/2016/09/mark-failla.html.

17

Adam Lowy and Doug Fleming, 'A Guide to Advanced TV Targeting', IAB - Empowering the Marketing and Media Industries to Thrive in the Digital Economy, 20 February 2018, https://www.iab.com/news/advanced-tv-targeting-guide.

18

'AOL: We'll Reach the Tipping Point for Addressable TV This Year | MediaVillage', accessed 5 March 2019, https://www.mediavillage.com/article/aol-well-reach-the-tipping-point-for-addressable-tv-this-year/.

19

'DISH & DirecTV Venture (D2 Media) Provides Addressable TV Ads For More Than 100 Political Campaigns In 2016 – Beet.TV'.

20

Ross Benes, 'Targeted TV Ads Find Niche in Political Campaigns', Digiday (blog), 2 December 2016, https://digiday.com/media/targeted-politics-ads/.

21

'Sky and Virgin Media to Accelerate Brand-Safe Advertising', Virgin Media, accessed 5 March 2019, https://www.virginmedia.com/corporate/media-centre/press-releases/sky-and-virgin-media-announce-strategic-partnership-to-accelerate-brand-safe-targeted-tv-advertising.html.

22

Addressable TV', accessed 5 March 2019, http://www.smartcliptv.com/wp-content/uploads/2016/04/Infographic-Addressable-TV.pdf.

23

Agustin Bertran, 'Movistar Will Bring Addressable TV Advertising to Latin America', NexTV News, 8 February 2019, http://nextvnews.com/movistar-will-bring-addressable-tv-advertising-to-latin-america/.

24

Philip Elliot, 'New Political TV Ads Can Target Individual Homes | PBS NewsHour', accessed 5 March 2019, https://www.pbs.org/newshour/nation/new-political-tv-ads-can-target-individual-homes.

25

Kristina Irion and Natali Helberger, 'Smart TV and the Online Media Sector: User Privacy in View of Changing Market Realities', Telecommunications Policy 41, no. 3 (1 April 2017): 170–84, https://doi.org/10.1016/j.telpol.2016.12.013.

Robocalls and Mobile Texting: Automated campaign outreach

"It felt like a real invasion...My first reaction was, who is this? How do they know my name? And how did they get my cellphone number?"

COMMENT FROM A ROBOCALL RECIPIENT,

AS REPEATED IN THE NEW YORK TIMES [1]

What are robocalls and mobile texting? [2]

The longstanding campaigning method of phone banking has evolved: advances in technology has allowed this established technique to be used at a far wider scope and scale than ever before. The growing accessibility of voter data now provides robocalling and mobile texting[3] services with more ways to engage and analyse voters. These tools can also be used to gather additional data from voters, such as their likelihood to attend a campaign event or their stance on a particular issue or candidate.

↘ **Robocalling:** A robocalling service automatically dials a list of phone numbers in order to deliver a prerecorded message or, in more technically advanced scenarios, even conduct a live call. Additionally, these advanced functions enable increased voter segmentation by conducting surveys and polls.[4] Along with volunteer phone banking, robocalls are an essential tool for campaigns seeking to promote a candidate or party.

↘ **Texting:** Like robocalling, mobile texting is used to directly broadcast a political message or a call-to-action to voters' mobile phones or devices. Campaigns can also use messaging platforms such as WhatsApp[5] or peer-to-peer SMS (as opposed to bulk texting) to initiate conversations between campaign volunteers and voters, as well as to administer surveys and polls.[6]

How is your data used?

Calling and texting both aim to reach you as directly as possible by using one of your most binding piece of personal data: your phone number. To build direct relationships quickly and cost-effectively, political campaigns can feed their in-house voter files or purchased data to a data-driven service provider, who helps them automatically dial phone numbers and deliver messages. Many of these companies also sell curated datasets of voter phone numbers. Campaigns in many countries rely on these services (as well as phone numbers contributed by party members) in their outreach campaigns, especially those using large-scale messaging platforms such as WhatsApp.

Data-driven services are becoming the technological backbone of the modern campaign phone bank. As such, they are often integrated into the offerings of robocalling providers. For

example, the company RoboCent[7] advertises 'reliable voter data [at] just 3¢/record',[8] including data points such as full names, full addresses, political affiliation (deduced from party membership or other indicators), age, gender, voting jurisdiction, email addresses, landline and mobile phone number, and demographic information such as ethnicity, language spoken and education.[9]

Texting services are similar in that they also obtain and utilise mobile phone numbers from existing voter lists or self-sourced voter files. Services such as uCampaign,[10] RumbleUp[11] and Relay[12] advertise being able to use their customers' lists of contacts in a texting campaign and even contact 'individuals that have been modeled to be likely donors/supporters of your cause'.[13] These services can also source and provide phone numbers to political parties. Relay, for instance, allows for data to be imported from third-party vendors of voter files and voter databases, such as NGP VAN[14] and Political Data Inc.[15]

Robocalling and texting services establish a two-way conversation that helps candidates gather more information from the people they're reaching out to. Both approaches seek to collect voter data and segment and quantify voters for the benefit of the campaign. The purpose of these techniques is to engage the voter in conversation and learn more about their views through pre-set questions, which can be posed by a human, by a machine, or by a combination of the two. Robocalls can implement polls and surveys by asking call recipients to use their keypad or voice to answer questions. This data can be quickly processed to enhance the data assets of campaigns and voter data platforms like NGP VAN.[16]

In the field of texting, Upland Software's Mobile Messaging[17] product, for example, has a 'Tell-a-Friend' feature, which was used in at least one political campaign, where 'students could text in their friends' phone numbers to invite them to join the mobile list'.[18] Callhub.io's SMS Marketing Software[19] advertises an 'expansive' SMS-based data collection solution where the software will 'automatically gather [voter] information through a sequence of interactive text messages and build detailed contact profiles for each supporter',[20] as well as several other methods to automatically gather and analyse data for campaigning purposes.

Some examples

In Canada: While the use of personal data in political robocalling and texting campaigns is a common practice, it seldom receives media attention until voter information is misused or the content of the calls sparks outrage. Voter data was misused in Canada's 2011 federal election, when residents in several electoral districts [21] were subject to a voter suppression campaign[22] driven by robocalls spreading misinformation about polling stations and polling locations on election day. The courts eventually ruled that 'the most likely source of the information used to make the misleading calls was the CIMS database[23] maintained and controlled by the [Conservative Party of Canada], accessed for that purpose by a person or persons currently unknown'.[24] In 2014, a former Conservative Party staffer was found guilty of violating Canada's Elections Act for his involvement in the robocalling misinformation scandal. The staffer had made several thousand robocalls to voters in Guelph, Ontario with a disposable mobile phone.[25, 26]

In India: In an effort to bridge the digital divide in India, the state of Chhattisgarh launched a large-scale plan to connect its population in part by providing free low-end smartphones to students and women. In the run-up to the 2019 elections, it was reported that these government-issued phones were being targeted with calls from the political campaign of the state's Chief Minister and the The Bharatiya Janata Party (BJP). The report suggests that this robocall targeting of voters, which included surveys and get-out-the-vote messaging, was originating from a call-centre which had previously been hired by the state government and was now being used for political activity on behalf of a single client.[27] Additionally, data gathered by the robocalling campaign was analysed in order to 'steer party activists to visit voters' with political leanings toward the opposition Indian National Congress Party. In response, the Congress Party filed complaints with the country's election commission arguing that the BJP was utilising government data on voters for the benefit of their own campaign.

In Malaysia: Reports on the prolific use of voter data in the run-up to the 2018 elections in Malaysia included references to political robocalling. A report for Tactical Tech details several instances of voters being contacted via phone by the 'National Census Department'.[28] However, there is no such department

in Malaysia. Nevertheless, the caller was able to identify the voter by name and regional language and asked surveying questions regarding the current government and attitudes towards the opposition. In another case, an interviewee stated that she had been contacted by one of Malaysia's leading call centres by an unknown caller asking for her voting preferences, polling station and reasons for voting. It remains unclear which political party or entity commissioned these robocall surveys, how the voter contact data was obtained or how the results of the calls would be processed.[29]

In the UK: During the 2016 UK European Union membership referendum, the Leave.EU campaign's affiliate, Better for the Country Ltd, sent text messages to over 500,000 mobile phone numbers of UK voters. *The Guardian* has reported these mobile phone numbers were sourced from voters who had consented to receiving text messages regarding leisure, home improvements and insurance. In 2016, the UK's Information Commissioner's Office fined the Leave.EU campaign £50,000 for this mass texting campaign for not obtaining clear consent from those voters.[30]

How do I know if it's being used on me?

It's usually not hard to tell if you are being targeted by a data-driven robocalling or texting campaign: voters will notice their inboxes and phones bombarded by political messages from candidates or causes.

Mass and direct voter contact through robocalling and texting is often regulated by local consumer protection laws to allow contact only when consent has been given. However, these regulations can vary in terms of what definitions are applied to these methods of voter outreach. Election campaign messaging, for example, is often less strictly regulated than sales initiatives.[31]

Despite these restrictions, US-based robocall and texting services have found ways to exploit loopholes in legislation. For example, automated, 'blast' text messages are not permissible without prior express consent: 'a human being must be present to "send" on every unsolicited text', according to the Federal Communications Commission.[32] Peer-to-peer texting services circumvent these rules by relying on the fact that there is an actual campaigner engaged in a direct conversation with the targeted voter. Thus, it is not considered to be a 'robotext', even when it involves sending mass, canned responses to thousands of voters' mobile phones.[33]

The use of WhatsApp in elections

WhatsApp is increasingly becoming a tool for political parties and candidates to establish and maintain direct voter contact in campaigns around the world. Its ability to connect groups of people in peer-to-peer or group conversations at low or virtually no cost[i] is not unique, and it is not the only platform to offer end-to-end encryption of messages. It, however, does dominate the messaging ecosystem in its sheer volume of users. As of 2018, WhatsApp had over 1.5 billion users[ii] and is the most popular messaging app in large parts of Africa, Asia, Europe and Latin America, where it is not just used for friends and families to communicate directly, but also by large groups of people who share common interests – from fans of a particular football team to those who share similar political views. It has also been used as an effective tool for political and social organising.

WhatsApp allows users to create groups of up to 256 people. While usually all the members of the group are able to comment on the conversation, a 2018 update now enables groups to act more like broadcast channels, in which only the administrator(s) can send messages to the group.[iii] Furthermore, messages—which can range from texts, to voice, video or web links—within a particular peer-to-peer or group chat can be forwarded to other chats on the platform, enabling a rapid spread of information throughout a user's social groups. Political campaigns can use WhatsApp to quickly spread their communications by banking on the 'viral' quality of their messaging or by implementing strategies of establishing as many groups as possible with as many users as permissible, or by 'injecting' themselves into groups in order to spread information.[iv]

In terms of the uses of personal data, the techniques applied in WhatsApp outreach are practically the same as those of texting and robocalling. WhatsApp numbers (phone numbers linked to WhatsApp accounts) are the key pieces of data, which campaigns segment into various lists for targeted outreach. There are also numerous online vendors that sell WhatsApp numbers, often with little information on their source.[v] Furthermore, there are 'unofficial' techniques that claim to expand the functionality of the platform, such as bulk-sourcing of phone numbers from existing WhatsApp groups,[vi] bulk-messaging to large number of users[vii] and analysis of group chats such as sentiment analysis.[viii] In addition, our partners' country studies found that party members in some countries are recruited, requiring them to provide hundreds of phone numbers for contacts in order to build networks for messaging.

The use of WhatsApp in political campaigning has been widespread in those parts of the globe where the platform is dominant. In India, Kenya and Malaysia, for example, the platform is used by politicians, party IT officers and supporters in coordinated strategies to customise messages and target them to specific groups based on geographic areas—sometimes up to 30 times per day in close to 1,000 groups simultaneously—and to coordinate communications and logistics.[ix]

The power of WhatsApp for political purposes is in the 'personal' feeling and sense of immediacy and urgency that direct voter contact produces, be it via direct outreach from a campaign or the spread of messaging via known contacts, such as friends and family. However, the prominence of the platform in connecting users brings some considerations with it. In Brazil, for example, WhatsApp is one of the main sources of information for its 120 million users. The design of the platform and the 'viral' nature of how stories, links, images and videos are shared is not conducive to fact-checking or efficient controls of misinformation. In the final weeks prior to Kenya's 2017 election, political and non-political WhatsApp groups were flooded with fake news and misinformation,[x] so much so that the country's Communications Authority threatened to hold group administrators responsible for the contents spread in their groups.[xi] Similarly, fake news was prevalent on WhatsApp in the run up to the 2018 election in Brazil, and it was reported that supporters of Jair Bolsonaro 'paid digital marketing firms … to spread tens of thousands of attack ads [on WhatsApp].'[xii] In order to combat fake news in the 2019 Indian election, WhatsApp itself announced it would reduce the number of times that users would be able to forward messages to contacts and groups from 20 to 5. This move came in response to Indian political parties creating 'hundreds of thousands of WhatsApp group chats to spread political messages and memes' in what has been dubbed as the 'WhatsApp Election.'[xiii]

i
'WhatsApp: The Widespread Use of WhatsApp in Political Campaigning in the Global South', accessed 19 February 2019, https://ourdataourselves.tacticaltech.org/posts/whatsapp/.

ii
Larry Kim, 'The Top 7 Messenger Apps in the World', Inc.com, 20 September 2018, https://www.inc.com/larry-kim/the-top-7-messenger-apps-in-world.html.

iii
Rachel Kraus, 'WhatsApp Adds Group Chat Option for Only Admins to Send Messages', Mashable, accessed 4 March 2019, https://mashable.com/article/whatsapp-group-chat-admin-only-messages/.

iv
Grace Mutung'u, 'Data and Digital Election Campaigning in Kenya', The Influence Industry (Tactical Technology Collective, 2018), https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-kenya.pdf.

v
A basic online search for 'WhatsApp channels for sale', for example, returns numerous web pages offering the sale of or access to WhatsApp numbers for bulk messaging.

vi
Chandan Baba, 'How to Extract Contact List from WhatsApp Group?', Mashtips, 6 June 2018, https://mashtips.com/whatsapp-group-extract-contact/.

vii
'Bulk WhatsApp Sender Suite - WhatsApp Marketing Panel', 30 March 2018, https://web.archive.org/web/20180330031815/http://bulkwhatsappsender.com/bulk-whatsapp-sender-suite/.

viii
Gaurav Bidasaria, '8 WhatsApp Analytics Tool to Analyze Chat History', TechWiser (blog), 25 February 2019, https://techwiser.com/whatsapp-analytics-tool/; Dr Nitin Paranjape, 'WhatsApp Group Chat Analytics Using Excel and Power Query', Efficiency 365 (blog), 17 April 2014, https://efficiency365.com/2014/04/17/whatsapp-group-chat-analytics-using-excel-and-power-query/; Sudharsan Ravichandiran, Whatsapp Chat Sentiment Analysis in R | Sudharsan, accessed 28 February 2019, https://www.youtube.com/watch?v=bYY1IOLaeHM.

ix
'WhatsApp: The Widespread Use of WhatsApp in Political Campaigning in the Global South'.

x
Grace Mutung'u, "Data and Digital Election Campaigning in Kenya,"

xi
"WhatsApp Admins Put on Notice Ahead of Hotly Contested Elections," Nairobi News, accessed March 6, 2019, https://nairobinews.nation.co.ke/news/whatsapp-admins-elections.

xii
Reuters, "Facebook's WhatsApp Flooded with Fake News in Brazil Election," Business Insider, accessed March 6, 2019, https://www.businessinsider.com/r-facebooks-whatsapp-flooded-with-fake-news-in-brazil-election-2018-10; Cristina Tardáguila, Fabrício Benevenuto, and Pablo Ortellado, "Opinion | Fake News Is Poisoning Brazilian Politics. WhatsApp Can Stop It.," The New York Times, October 19, 2018, sec. Opinion, https://www.nytimes.com/2018/10/17/opinion/brazil-election-fake-news-whatsapp.html.

xiii
Billy Perrigo, "How Whatsapp Is Fueling Fake News Ahead of India's Elections," Time, January 2019, http://time.com/5512032/whatsapp-india-election-2019/.

A screenshot of a voter data request from RoboCent's website featuring filters for location, demographics and phone numbers.

Source: 'Request Data', RoboCent, Inc. (blog), accessed 20 February 2019, https://robocent.com/request-data/
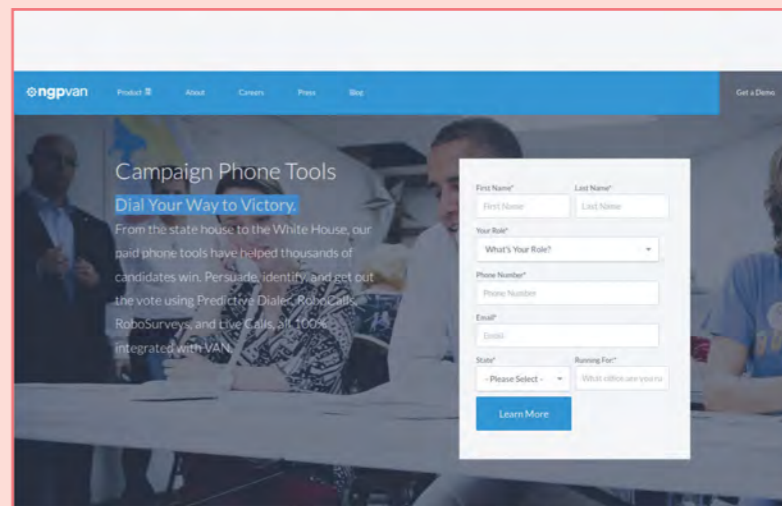
A screenshot of the robocalling services as advertised by NGP VAN, a data management system used by Democrats in the US.

Source: NGP VAN, 'Campaign Phone Tools', accessed 28 February 2019, https://act.ngpvan.com/paid-phones.

A description of techniques for acquiring voter data via texting services as advertised by CallHub.

Source: 'SMS Data Collection', CallHub (blog), accessed 13 February 2019, https://callhub.io/sms-data-collection/

A screenshot from Élections Québec's Twitter account warning voters against scam text messages being sent to voters.

Source: Québec, Élections. "Important! Un faux message texte circule présentement. Sachez qu'en aucun cas, Élections Québec ne demanderait une rétribution ou n'offrirait une rémunération liée à l'exercice du droit de vote aux élections générales. En cas de doute 1 888 353-2846. #polqc #QC2018 RTSVPpic.twitter.com/krHf3718Mx." Tweet. @electionsquebec (blog), September 30, 2018. https://twitter.com/electionsquebec/status/1046425834041618433/photo/1.

"RoboCent offers its version of 'ringless voicemail technology', which allows a prerecorded message to be delivered to voicemail without the device actually ringing."

How do I know if it's being used on me? (continued)

Similarly, RoboCent offers its version of 'ringless voicemail technology', which allows a prerecorded message to be delivered to voicemail without the device actually ringing, and advertises that the service 'opens the door to over 300 million mobile subscribers'.[34] The Federal Communications Commission has yet to rule on the legality of the technology.[35]

Considerations

↘ Robocalling and texting directly utilise a voter's personal data and engage intimately with the voter in order to deliver campaign materials and messages and conduct polls and surveys.

↘ Robocalling and texting could be considered a means of direct communication between politicians/parties and voters—a possibility that has only recently emerged on a mass scale.[36] This relationship could even extend beyond campaign season in maintaining engagement with voters, such as the case of Malaysian politicians sending birthday or seasonal greetings to supporters.[37]

↘ However, robocalls and texting in political campaigns can exacerbate the issue of increased segmentation and profiling of the electorate.

↘ There is increasing evidence that texting contributes to the proliferation of misinformation and fake news[38] during the course of an election campaign, such as in the run-up to the 2019 election in Nigeria,[39] or the SMS-based scam identified by Élections Québec in 2018 which fraudulently promised payment for political support.[40]

↘ Robocalls can also be used for nefarious purposes, such as the cases during the 2018 US Midterm elections where a white supremacist podcast initiated automated calls to voters in Florida and Georgia featuring racist and anti-Semitic messages targeting each state's African-American candidates.[41]

1

Kevin Roose, 'Campaigns Enter Texting Era With a Plea: Will U Vote 4 Me?', *The New York Times*, 2 August 2018, sec. Technology, https://www.nytimes.com/2018/08/01/technology/campaign-text-messages.html.

2

The technologies examined here are purposely centred on American examples in order to showcase some of the more unrestricted uses of voter data. These practices may be subject to different data and privacy protection regulations in different countries. Different electoral contexts also change the emphasis of some technologies over others. For example, while SMS-based texting remains popular in the US due in large to historically low costs per SMS, messaging platforms such as WhatsApp are much more prominent in other countries.

3

Sometimes simply referred to as SMS in promotional materials, see 'I Will Run Marketplace', accessed 8 February 2019, https://iwillrun.org/voter-contact/. In this piece, 'texting' refers to an overall category, containing sub-categories such as 'bulk SMS/robotexting', peer-to-peer texting via SMS or messaging platforms like WhatsApp.

4

'Push Polls and Surveys Get Live Results', RoboCent, Inc. (blog), accessed 11 February 2019, https://robocent.com/services/push-polls-surveys/.

5

'Twilio API for WhatsApp | Send Messages, Alerts and Notifications on WhatsApp Using Twilio WhatsApp Messaging API.', Twilio, accessed 15 February 2019, https://www.twilio.com.

6

Relay—Harness the Power of P2P Texting', Relay, accessed 11 February 2019, http://relaytxt.com/true.

7

'RoboCalls for Political Campaigns Starting at 1¢ per Dial', RoboCent, Inc., accessed 12 February 2019, https://robocent.com/.

8

'Reliable Voter Data for Only 3¢ a Record', RoboCent, Inc. (blog), accessed 12 February 2019, https://robocent.com/services/voter-data/.

9

Request Data', RoboCent, Inc. (blog), accessed 20 February 2019, https://robocent.com/request-data/.

10

'UCampaign - Apps That Engage Everyone', accessed 12 February 2019, https://ucampaign.co/.

11

'RumbleUp', accessed 12 February 2019, https://www.rumbleup.com/.

12

'Relay—Harness the Power of P2P Texting'.

13

'RumbleUp'.

14

'VAN Integration - Contact Import', Relay, accessed 12 February 2019, http://support.relaytxt.io/hc/en-us/articles/115002824514-VAN-Integration-Contact-Import.

15

PDI Integration', Relay, accessed 12 February 2019, http://support.relaytxt.io/hc/en-us/articles/360010074134-PDI-Integration.

16

NGP VAN, 'Campaign Phone Tools', accessed 28 February 2019, https://act.ngpvan.com/paid-phones.

17

'Upland Software', Upland Software, accessed 13 February 2019, https://upland-software.com/.

18

'Wendy Davis for Governor Campaign', Mobile Messaging, accessed 8 February 2019, https://uplandsoftware.com/mobile-messaging/resources/case-study/wendy-davis-governor-campaign/.

19

'SMS Broadcast | Automated Text Messaging | CallHub', accessed 13 February 2019, https://callhub.io/sms-marketing-software/.

20

'SMS Data Collection', CallHub (blog), accessed 13 February 2019, https://callhub.io/sms-data-collection/.

21

'Ridings', accessed 21 February 2019, https://lop.parl.ca/sites/ParlInfo/default/en_CA/ElectionsRidings/Ridings.

22

Federal Court Won't Remove MPs over Election Robocalls | CBC News', CBC, 24 May 2013, https://www.cbc.ca/news/politics/federal-court-won-t-remove-mps-over-election-robocalls-1.1331781.

23

For more details on CIMS, see Colin Bennett and Robin Bayley, 'Data Analytics in Canadian Elections', The Influence Industry (Tactical Technology Collective, 2018), https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-canada.pdf.

24

'Federal Court Won't Remove MPs over Election Robocalls | CBC News'.

25

'Former Conservative Party Staffer Guilty in Robocalls Trial | CBC News', CBC, accessed 18 February 2019, https://www.cbc.ca/news/politics/michael-sona-guilty-in-robocalls-trial-but-did-not-likely-act-alone-1.2735676.

26

Glen McGregor and Stephen Maher, 'Robocalls Court Filings Shed New Light on Case, Possible Sona Involvement', Canada.Com, 25 August 2013, http://www.canada.com/life/Robocalls+court+filings+shed+light+case+possible+Sona+involvement/8835526/story.html.

27

'Vindu Goel and Suhasini Raj, 'In "Digital India," Government Hands Out Free Phones to Win Votes', The New York Times, 19 November 2018, sec. Technology, https://www.nytimes.com/2018/11/18/technology/india-government-free-phones-election.html.

28

Boo Su-Lyn, 'The Influence Industry - Voter Data in Malaysia's 2018 Elections', The Influence Industry (Tactical Technology Collective, June 2018), https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-malaysia.pdf.

29

Boo Su-Lyn, 'The Influence Industry - Voter Data in Malaysia's 2018 Elections'.

30

Jasper Jackson, 'Leave.EU Campaign Fined £50,000 for Sending Spam Texts', The Guardian, 11 May 2016, sec. Media, https://www.theguardian.com/media/2016/may/11/leave-eu-campaign-fined-50000-for-sending-spam-texts.

31

'Political Campaign Robocalls & Robotexts', Federal Communications Commission, 27 October 2016, https://www.fcc.gov/political-campaign-robocalls-robotexts.

32

'Why Politicians Are Texting You So Much — And It's Only the Beginning', Time, accessed 19 February, 2019, http://time.com/5432309/politician-campaigns-midterm-election-text-messages/.

33

'TCPA Attorney - Are Unsolicited Political Text Messages Illegal? - YouTube', accessed 15 February 2019, https://www.youtube.com/watch?v=GQygZftJ6LI.

34

'Ringless Voicemail Drops (RVM) Let You Directly Target Cell Phones', RoboCent, Inc. (blog), accessed 19 February 2019, https://robocent.com/services/ringless-voice-mail-drops/.

35

'Court Says That Ringless Voicemail Messages Are TCPA Calls', KMT (blog), 6 August 2018, http://www.kleinmoynihan.com/court-says-that-ringless-voicemail-messages-are-tcpa-calls/.

36

'Voice Broadcasting - Call Center - SMS Broadcast Software', CallHub, accessed 3 May 2018, https://callhub.io/.

37

WhatsApp: The Widespread Use of WhatsApp in Political Campaigning in the Global South', accessed 19 February 2019, https://ourdataourselves.tacticaltech.org/posts/whatsapp/.

38

WhatsApp: The Widespread Use of WhatsApp in Political Campaigning in the Global South'.

39

"Analysis | Saturday Will Be Nigeria's First WhatsApp Election. Here's What We're Learning about 'Fake News.'", Washington Post, accessed 19 February 2019, https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigerias-first-whatsapp-election-heres-what-were-learning-about-how-fake-news-spreads/.

40

'Voters Warned of Fraudulent Text Messages Promising Payment for Supporting CAQ | CBC News', CBC, 21 November 2018, https://www.cbc.ca/news/canada/montreal/fraudulent-texts-election-quebec-1.4914208.

41

Justin Wise, 'Gillum Targeted by New Racist Robocall in Florida: Report', Text, TheHill, 23 October 2018, https://thehill.com/homenews/campaign/412782-gillum-targeted-by-new-racist-robocall-attacking-him-as-a-negro; Emily Birnbaum, 'Stacey Abrams, Oprah Targeted by Racist Robocall Funded by White Supremacist Group', Text, TheHill, 3 November 2018, https://thehill.com/homenews/campaign/414703-abrams-targeted-by-racist-robocall-in-georgia.
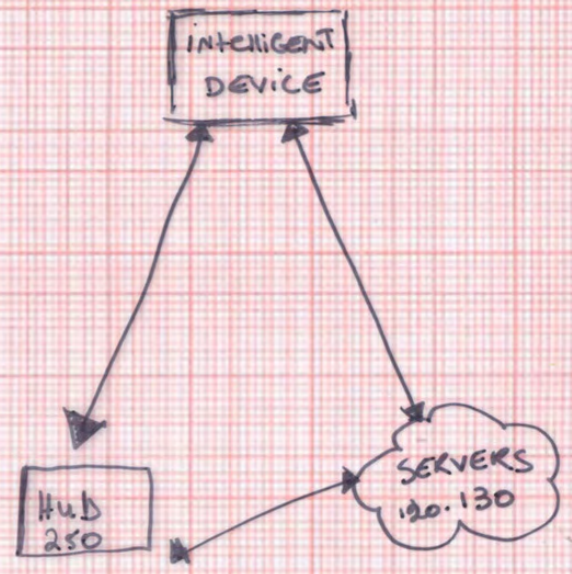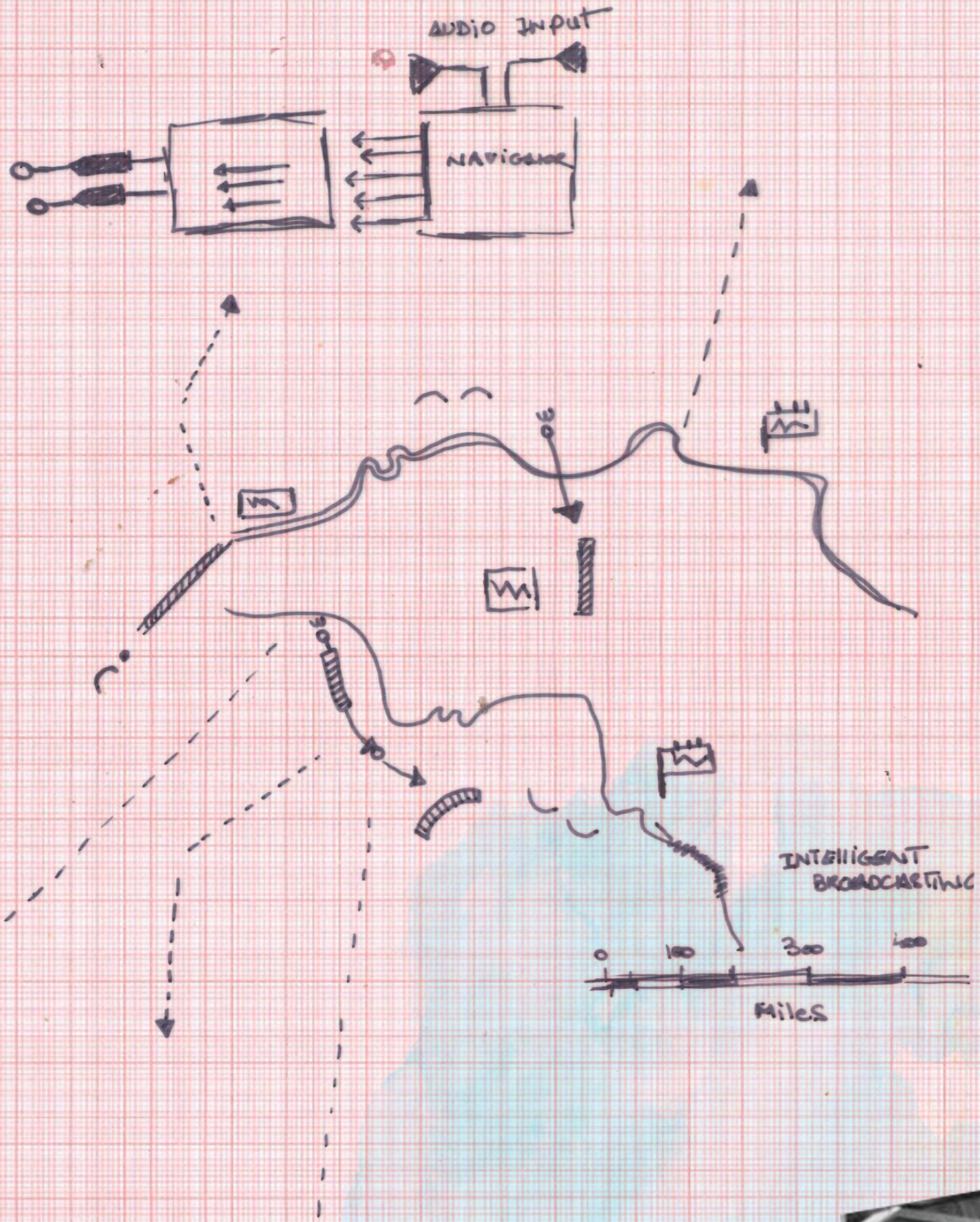
AUDIO INPUT

NAVIGATOR

INTELLIGENT DEVICE

HUB 250

SERVERS 120-130

FIG. 340

INTELLIGENT BROADCASTING

0   100   300   400

Miles

Psychometric Profiling:
Persuasion by personality

"Political strategists can use psychometric profiling to tailor their communications to influence political opinions and voter preferences."

What is psychometric profiling?

In March 2017, it was announced that the data firm Cambridge Analytica had quantified, in the words of its former CEO Alexander Nix, 'the personality of every single adult in the United States of America'. By using voter data harvested from Facebook, the firm reportedly helped elect Donald Trump.[1] While Cambridge Analytica has since filed for insolvency, the collection and use of personality-based data remains a valuable practice for private companies and political campaigns alike, especially as demand for psychometric services intensifies.[2, 3, 4, 5, 6, 7]

Psychometric profiling is the process by which your observed or self-reported actions are used to infer your personality traits. The marketing industry, public relations and politics have long used psychology to understand and influence individuals' beliefs, behaviours and motivations.[8] Psychometric profiling takes this a step further by mining vast quantities of personal data, which political strategists can use to tailor their communications to have greater influence on political opinions and voter preferences.

Psychometric profiles can be constructed multiple ways. The simplest option is to conduct a survey in which individuals answer questions that reveal aspects of the their psychological composition. For example, users who respond that they always follow a plan are considered high in conscientiousness, a trait that describes respect for authority, order and structure. While surveys like these can provide the basis for a psychometric profile, more recently data-driven analysis has allowed psychometric profiling to move beyond the question-and-answer format. Now, explicit user input is not even necessary for profiling individuals: researchers have claimed that personality traits can also be predicted from analysing how a person uses Facebook. That is to say, there's no need to ask how open someone is when liking a Facebook page about Leonardo da Vinci already suggests a high level of openness. This not only reduces the need for cumbersome surveys, but it also enables profiling at scale.[9]

One of the most popular psychometric profiling models is the OCEAN model, also called the 'Big Five' or the 'Five Factor Model', named for the five personality traits it measures: openness, conscientiousness, extraversion, agreeableness and neuroticism. Psychological research suggests that these five traits encompass a wider range of individual motivations and preferences than any other combination of five traits.[10] For campaigns and strategists with a political message to deliver, information about voters' OCEAN profiles is clearly valuable, as reflected in remarks by Cambridge Analytica's Nix: 'if you know the personality of the people you are targeting, you can nuance your messaging to resonate more effectively with those key audience groups. For a highly neurotic and conscientious audience, you're going to need a message that's rational and fear-based, or emotionally based'.[11]

How is your data used?

Unlike categories such as gender and age, psychometric characteristics are not directly observable, so they need to be inferred using statistical models. In 2013, Michal Kosinski—a pioneer in the field of psychometric profiling and digital behaviour —was the first to show that algorithms given Facebook likes could predict personality traits.[12] In 2015, Kosinski and his team published a report claiming that algorithms are better at judging personality from data than humans (surpassing the performance of subjects' friends, co-workers and partners with relatively modest amounts of data).[13] Most recently in 2017, they showed that ads tailored to psychological profiles in the real world are more effective than ads that are not.[14] Due to a whistleblower and intense media and governmental scrutiny, some of Cambridge Analytica's data sources and academic methodology have come to light, yet much about the for-profit psychometric profiling industry remains opaque.

Some examples

In the United Kingdom: Both the Conservative Party and Labour Party purchased services from Experian, a consumer credit reporting agency that delivers the kinds of personal data that can be used in psychometric profiling to clients internationally.[15] The data broker claims to hold data on over a billion people in Europe and the United States and earned over 4.6 billion USD in revenue in 2018.[16] There is no evidence to suggest that either party used Experian's psychometric data, but the company has invested resources in constructing these personality profiles and in making them available to clients. Among the many offerings of Experian Marketing Services was Audience IQ, a one-stop shop for marketers that apparently could 'influence voting behavior by interweaving demographic, psychographic, and attitudinal' characteristics.[17]

In the United States: Cambridge Analytica identified and targeted persuadable voters in the run-up to the 2016 US presidential election for candidate Ted Cruz, and later Donald Trump. Nix explicitly linked the company's targeting of personality traits with influencing voting behaviour: 'it's personality that drives behaviour, and behaviour obviously influences how you vote'. Through its parent company, Strategic Communication Laboratories, the firm was also involved in elections in at least 20 countries.[18] Using data originally harvested from Facebook, Cambridge Analytica claims it was able to deliver micro-targeted ads to voters on hot-button issues like gun ownership.[19]

How do I know if it's being used on me?

There are a few, isolated cases in which the use of psychometric profiling can be investigated. After the scandal erupted over the Cambridge Analytica revelations, Facebook released a tool letting users check whether their data had been compromised.[20] Additionally, though time-consuming, data subject access requests, like those authorised by the European Union's General Data Protection Regulation (GDPR), can be submitted and the results examined for evidence of personality-based predictions. However, there is no way to comprehensively know whether a psychometric profile has been built from your data.

Considerations

↘ Given the reported effectiveness of psychometric profiling, the method could be used to encourage unregistered voters to engage in the political process or to support non-partisan efforts to boost voter turnout.

↘ Intimate personality details can easily be used for manipulative purposes by companies and campaigns. For example, campaigns could harness psychographic data for voter suppression or more opaque forms of influence.

↘ Voters may lose trust in the political process if they deem the use of psychometric profiling in political campaigning as invasive or not transparent.

↘ Individuals may be profiled without their knowledge or consent and may have no recourse to avert the influence these profiles may have on their political decisions.

This image from a 2014 paper, 'Tracking the Digital Footprints of Personality', shows estimated levels of neuroticism (the inclination for worry, tension, and general anxiousness vs. emotionally groundedness) by US state based on psychometric profiles. Darker shades correspond to higher-than-average levels, while lighter shades correspond to lower than average. The image suggests, for instance, that Californians tend to be less neurotic than New Yorkers.

Source: R. Lambiotte and M. Kosinski, 'Tracking the Digital Footprints of Personality', Proceedings of the IEEE 102, no. 12 (December 2014): 1934–39, https://doi.org/10.1109/JPROC.2014.2359054

1. Facebook + Survey Data Collected
Individuals respond to a survey and grant access to their Facebook profile data. In this example, 10,000 people take part.

2. Data Compression
At this point, there are hundreds of data points from each user's Facebook page 'likes'. These are distilled into a smaller number of distinct categories. Each user is given a new profile comprised of these categories. For instance, 500+ page 'likes' can be condensed to 100 categories.

3. Prediction
The model generates a relationship between the category data and survey results for each user. For example, Category 5 may be predictive of openness, and Category 43 may be predictive of agreeableness. From here, the model's accuracy is assessed based on the differences between the predicted values and the actual survey outcome for each user.

4. OCEAN Profiles of Surveyed Users
If the model performs satisfactorily, then Facebook 'likes' have been demonstrated to predict survey responses and – by extension – users' OCEAN profiles.
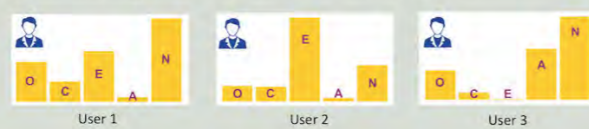
5. Extrapolating Results: OCEAN Profiles of Other Users
An estimated OCEAN profile can then be generated for users who haven't taken part in the survey. The model can predict OCEAN scores for any Facebook user whose data is accessible, as long as the user has enough 'likes'.

6. Putting it all together
Advertisements are designed for specific OCEAN profiles. They are selectively targeted to affect a desired outcome (e.g., a vote).

Icons from zidney and SBTS (The Noun Project)
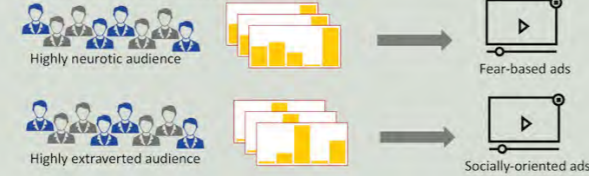
This schematic shows a simplified pipeline for psychometric profiling based on Facebook data, as conducted in published academic papers. In practice, information on intimate traits can be extracted from enticing, game-like online quizzes, purchased from data brokers, or inferred from digital records like Facebook 'Like' data.

Sources: Varoon Bashyakarla, 'Psychometric Profiling: Persuasion by Personality in Elections', 18 May 2018, https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling/; McKenzie Funk, 'Opinion | Cambridge Analytica and the Secret Agenda of a Facebook Quiz', The New York Times, 17 March 2018, sec. Opinion, https://www.nytimes.com/2016/11/20/opinion/cambridge-analytica-facebook-quiz.html

This screenshot from Experian's Audience IQ shows that the firm offers access to psychographic attributes for those interested in influencing votes. The company also offers an 'Audience Guide', whose tagline is 'get inside the mind of your consumers'. The guide lists several classes of individuals: affectionate, brave, dominating, refined, and efficient.

Source: 'Wayback Machine', 10 April 2018, https://web.archive.org/web/20180410114126/https://www.experian.com/assets/marketing-services/product-sheets/das-political-data-sheet.pdf

Leveraging psychometric data requires the ability to collect, mine and make inferences from troves of data. The winning campaign, described here by Cambridge Analytica, from the Advertising Research Foundation's (ARF) website used machine learning methods to identify and target persuadable voters for Donald Trump's 2016 presidential campaign. The ARF awarded Cambridge Analytica the gold prize in its 'big data' category for this work in 2017.

Source: 'Wayback Machine', 4 July 2017, https://web.archive.org/web/20170704165557/http://thearf-org-aux-assets.s3.amazonaws.com/downloads/ogilvy/2017/Cambridge-Analytica__Make-America-Number-One.pdf.
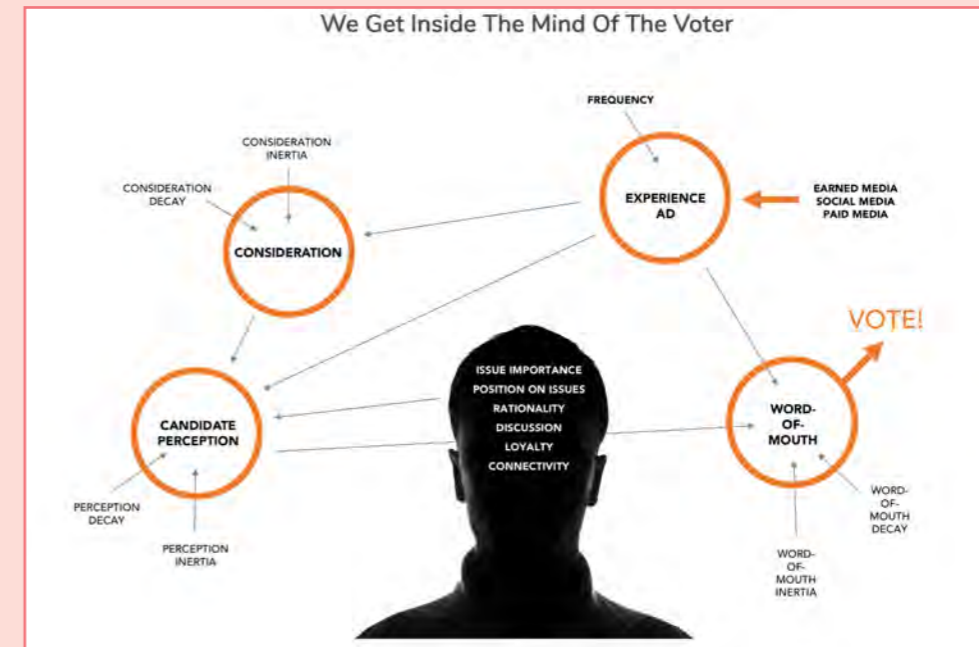
This screenshot taken from the website of Market-Predict, a media optimisation firm. It shows different voter considerations under the headline 'we get inside the mind of the voter'.

Source: 'Predict Voter Behavior in Real Time', Market Predict, accessed 4 March 2019, https://www.maket-predict.com/

"For a highly neurotic and conscientious audience, you're going to need a message that's rational and fear-based, or emotionally based."

ALEXANDER NIX, FORMER CEO OF CAMBRIDGE ANALYTICA

1

Concordia, Cambridge Analytica - The Power of Big Data and Psychographics, accessed 1 March 2019, https://www.youtube.com/watch?v=n8Dd5aVXLCc&feature=youtu.be&t=220.

2

'Home - Affectiva : Affectiva', accessed 1 March 2019, https://www.affectiva.com/.

3

'Realeyes', accessed 1 March 2019, https://www.realeyesit.com/.

4

Sensum, 'Empathic AI for Smart Mobility, Media & Technology', Sensum, 1 March 2019, https://sensum.co.

5

Anthony Crupi, 'Nielsen Buys Neuromarketing Research Company Innerscope | Media - Ad Age', accessed 1 March 2019, https://adage.com/article/media/nielsen-buys/298771/.

6

'Ford and Xaxis Score in Vietnam Using Emotional Triggers around the UEFA Champions League | The Drum', accessed 1 March 2019, https://www.thedrum.com/news/2016/10/18/ford-and-xaxis-score-vietnam-using-emotional-triggers-around-the-uefa-champions.

7

Jeff Chester and Kathryn C. Montgomery, 'The Role of Digital Marketing in Political Campaigns', Internet Policy Review 6, no. 4 (31 December 2017), https://policyreview.info/articles/analysis/role-digital-marketing-political-campaigns.

8

Edward Bernays, 'Propaganda by Edward Bernays (1928)', accessed 1 March 2019, http://www.historyisaweapon.com/defcon1/bernprop.html.

9

Michal Kosinski, David Stillwell, and Thore Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior', Proceedings of the National Academy of Sciences of the United States of America 110, no. 15 (9 April 2013): 5802–5, https://doi.org/10.1073/pnas.1218772110.

10

Michal Kosinski, David Stillwell, and Thore Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior'.

11

Concordia, Cambridge Analytica - The Power of Big Data and Psychographics.

12

Michal Kosinski, David Stillwell, and Thore Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior'.

13

Wu You,you, Michal Kosinski, and David Stillwell, 'Computer-Based Personality Judgments Are More Accurate than Those Made by Humans', Proceedings of the National Academy of Sciences 112, no. 4 (27 January 2015): 1036–40, https://doi.org/10.1073/pnas.1418680112.

14

S. C. Matz et al., 'Psychological Targeting as an Effective Approach to Digital Mass Persuasion', Proceedings of the National Academy of Sciences 114, no. 48 (28 November 2017): 12714, https://doi.org/10.1073/pnas.1710966114.

15

Archie Bland, 'Tories Identify Eight Groups of Voters as Labour Look to Obama', The Independent, 6 November 2013, http://www.independent.co.uk/news/uk/politics/tories-identify-eight-groups-of-voters-as-labour-look-to-obama-campaign-for-inspiration-the-8925374.html.

16

'Experian Plc - Key Financial Data', accessed 1 March 2019, https://www.experianplc.com/investors/key-financial-data/.

17

'Wayback Machine', 10 April 2018, https://web.archive.org/web/20180410114126/https://www.experian.com/assets/marketing-services/product-sheets/das-political-data-sheet.pdf.

18

'SCL Elections | Projects', accessed 1 March 2019, https://web.archive.org/web/20170520211639/sclgroup.cc/elections/projects.
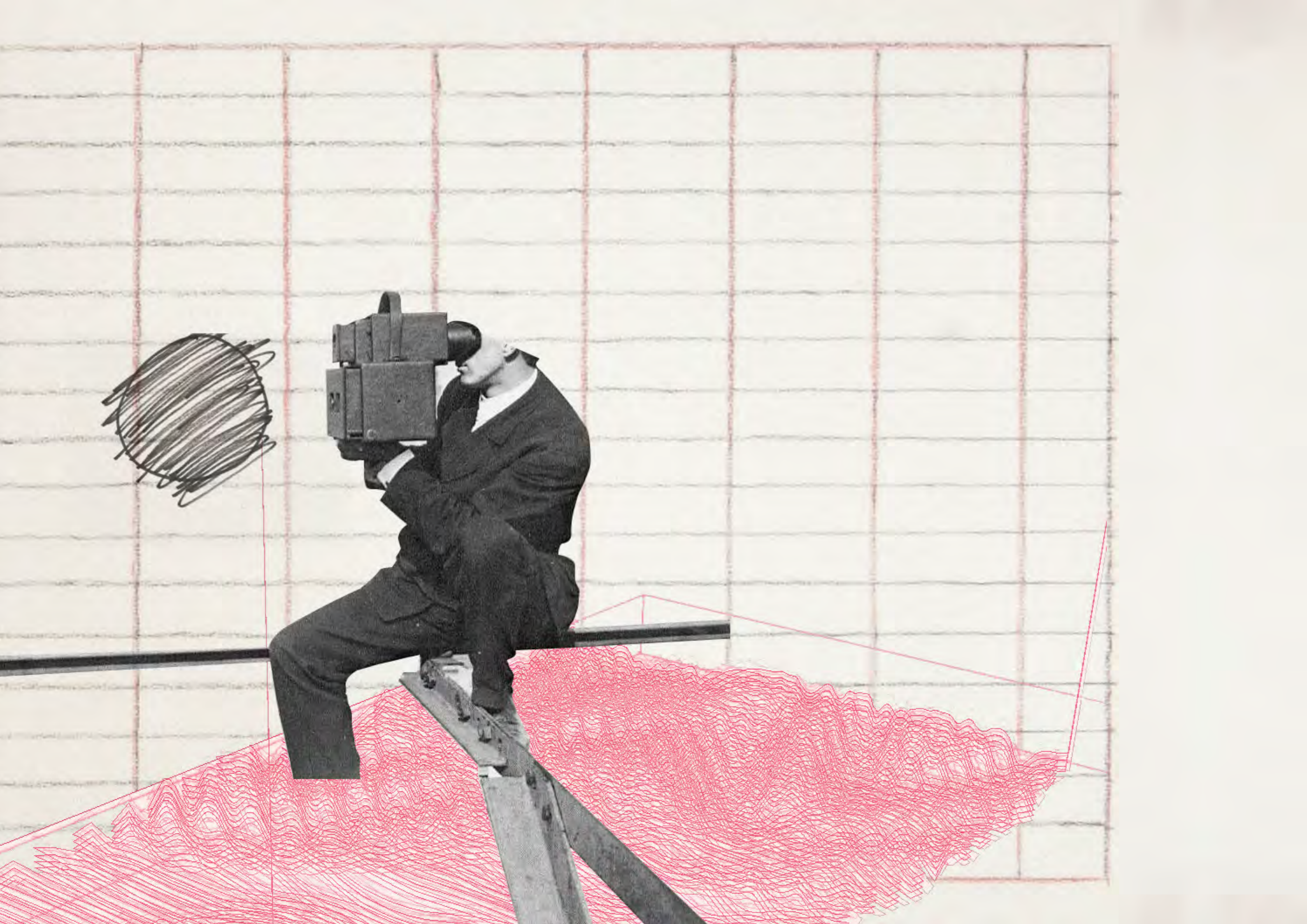
19

Concordia, Cambridge Analytica - The Power of Big Data and Psychographics.

20

'Which Banned Apps May Have Had Access to My Info? | Facebook Help Center | Facebook', accessed 1 March 2019, https://www.facebook.com/help/1873665312923476?helpref=search&sr=1&query=cambridge.

Upcoming Technologies:
The next frontier
in campaign technology

114   115

"The next generation of political chatbots are likely to be more sophisticated, especially as they glean more personal data."

What technologies are on the horizon?

Political tactics have long mirrored those of the marketing industry.[1] In fact, virtually all of the methods explained in this guide were pioneered by for-profit companies before their arrival in politics. Though it is impossible to predict how exactly political campaigning will evolve in the future, the commercial sector and emerging areas of research and experimentation provide some hints as to what campaigns will be doing.[2] This chapter explores several emerging technologies that use personal data and have gained some traction in recent political campaigns.

↘ Bots

The use of political bots and computational propaganda in influencing online discourse, like trending hashtags on Twitter, has been well-documented and remains an active area of research.[3,4,5] The rise of chatbots powered by personal data may lead to a more individualised version of this same phenomenon. As one researcher warns, 'in a few years, conversational bots might seek out susceptible users and approach them over private chat channels. They'll eloquently navigate conversations and analyse a user's data to deliver customized propaganda. Bots will point people toward extremist viewpoints and counter arguments in a conversational manner'.[6]

Bots appeal to political campaigns for many reasons: they allow campaigns to respond to voter inquiries efficiently, help users navigate today's deluge of political information, avoid the risk of human error, work across platforms, and can provide personalised responses to the users chatting with them.[7,8] They are also financially attractive: in April 2016, 'Facebook opened its hugely popular Messaging platform to bot developers', which is not only a cheaper option than bulk SMS but also enables campaigns to leverage a rich supply of Facebook data in the process.[9,10]

Campaigns are also eager to use bots because of the personal data bots can gather. 'A chatbot can ask users to select certain options or to answer specific questions', one communications specialist explained, 'In this way, the bot creates an instant database and provides statistics about people's preferences, suggestions, and doubts.'[11] In other cases, bots can target users with polls to measure responses to issues, allowing the campaign to collect further data.

Chatbots are also on the rise because they can be integrated into engagement efforts more seamlessly; they do not require any voter effort or initiative. After simply commenting on an article, a voter can be prompted to answer questions, sent to polls, asked to donate and more, all through bots.

Targeted political campaign bots are currently still quite basic. One startup in France, for example, built a bot that responded to any user message with one of 100 quotes from Donald Trump (and observed very high engagement rates).[12] Another bot called 'Dein Selfie mit Van der Bellen' (Your Selfie with [then-candidate and current Austrian President] Alexander Van der Bellen) helped users add an image of Van der Bellen to their Facebook profile pictures.[13]

The next generation of political chatbots are likely to be more sophisticated, especially as they glean more personal data. Campaigns are likely to make use of the same technologies and advances in natural language processing that Google, Amazon and Microsoft have used to make their bots more human-like.[14] Adam Meldrum, an entrepreneur and specialist on the use of AI and chatbots in political campaigning, wants to use chatbots 'to create a more natural relationship with voters'.[15] His vision, common in the industry, is to make chatbots 'respond like a human would'; that is, with enough improvement, bots can facilitate organic campaign interactions, unlike their current form—not much more than a 'glorified marketing site'.[16,17]

In a similar vein, researchers at the MIT Media Lab are attempting to build AI bots that respond like their human counterparts. In the context of politics, using a bot 'knowledgeable about a candidate's positions, as well as their demeanour, the virtual conversation could allow voters to ask questions hyper-specific to their community, and receive targeted answers in return'.[18] The idea behind the research is to probe whether our digital footprints reveal enough about our 'thoughts, interests, and personal identity' for an AI-powered bot to convincingly emulate us.[19] If viable, campaigns would probably use this 'swappable identity' capability to 'influence opinion and generate excitement among people it views as likely supporters of their candidate'.[20, 21]

↘ Eye tracking

Some political campaigns have also started refining their ads based on insights from eye-tracking research. In this work, a panel of people opt-in to having their eye movements recorded, either in a lab setting or using in-home devices. A blog post from Discida, a company that provides eye-tracking services to political campaigns, summarises the concept:

> Eye tracking is an excellent technique that allows you to see exactly what is (and is not) noticed, and how much attention components of a piece are getting. If the voter doesn't look at the key images or words, then the piece fails to deliver its message. The benefit of eye tracking over other techniques, such as focus groups, is the response is automatic for the voter. They do not have to recall what they looked at, nor are they influenced to follow another member of the group or respond in ways that please the interviewer. Eye tracking provides that critical first few seconds of information —where do they look first and then where do they go next? Where do voters linger longest?[22]

This technology allows political parties or candidates to tailor ads to voters for maximum impact. Researchers at the University of Vienna showed ads from the Austrian Green Party (liberal) and the Austrian Freedom Party (conservative) at the same time to liberal and conservative voters and observed their eye movements. The study found that people spent more time looking at the ads that aligned with their political views. While this may seem intuitive, a campaign could use it as rationale for many decisions to capture voters' attention, like crafting ads to voters' exact political leanings or publishing more polarising political ads. In turn, eye-tracking services will likely grow more personal as they optimise for increasingly granular groups. Eye-tracking technology contends, for example, that men and women look at different parts of ads.[23]

↘ Cognitive computing

Changes in technology have created ways to understand voters even more intimately, more quickly and supposedly more precisely. The marketing industry is exploring cognitive computing by conducting studies on the brain to understand how retention, emotion and attention are affected by the media we 'consciously and subconsciously' consume.[24] A United States Postal Service blog post entitled 'What neuromarketing means for political campaigns' showcased research findings that 'ads that contain faces are remembered more than those that contain

scenes or words'. The post also claims that physical campaigns (e.g., direct / physical mail) are better for raising candidate awareness because direct mail, when compared to other forms of media, demonstrated higher 'recall, desirability, and likability'. When combined with digital media, physical mail attracted 39% more attention than a single medium on its own.[25]

↘ Internet of Things

The sheer volume of information available to political campaigns is bound to increase dramatically. The number of connected devices worldwide is projected to surpass 30 billion by 2020 and campaigns are already positioning to extract as much value as possible from connected TVs, set-top boxes and media consumed online.[26,27] In the near future, IoT smart speakers like Amazon's Echo, Google Home, robotic vacuums, smart beds and others promise to capture even more rich, behavioural data.[28] Are members of a household concerned about safety issues? Campaigns no longer need to make predictions when an under-utilised smart alarm system can answer that question for them. One journalist predicted, 'for democracies, the Internet of Things (IoT) will transform how we as voters affect government—and how government touches (and tracks) our lives' via in-built sensors that 'never sleep'.[29, 30] Because many of these devices will live at home, the data we share with them will likely be even more intimate than the data we share with our devices today.[31] Ultimately, these nascent developments are believed to advance campaigns' efforts to target voters as precisely and accurately as possible at scale.
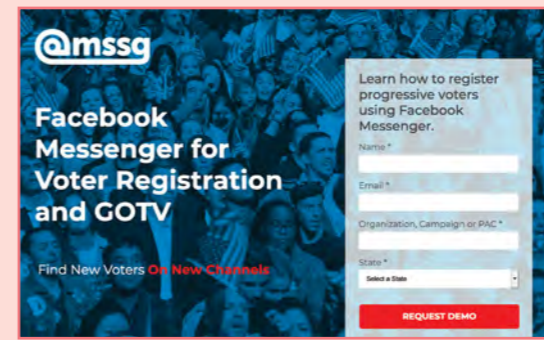
Some examples

In the United States: In November 2016, a Facebook Messenger bot created by @mssg was enlisted on behalf of three political groups; the Connecticut House Democratic Campaign Committee, the Pennsylvania Common Sense Political Action Committee and Bazta Arpaio, a community-driven campaign in Arizona, to vote Sheriff Joe Arpaio—accused of discriminatory practices—out of office. The bot asked voters for their address and returned the relevant voting location. While many websites to look up polling places existed at the time, @mssg's bot offered some advantages: a novelty factor, the convenience of a mobile-friendly experience and the opportunity to experiment.

Chatbots Magazine, an industry resource, published an article entitled 'Bots Are More Than "Fake News" Machines', which featured images generated by the chatbot 'Your Selfie with Van der Bellen'. These images were part of a Facebook chatbot developed at a hackathon.

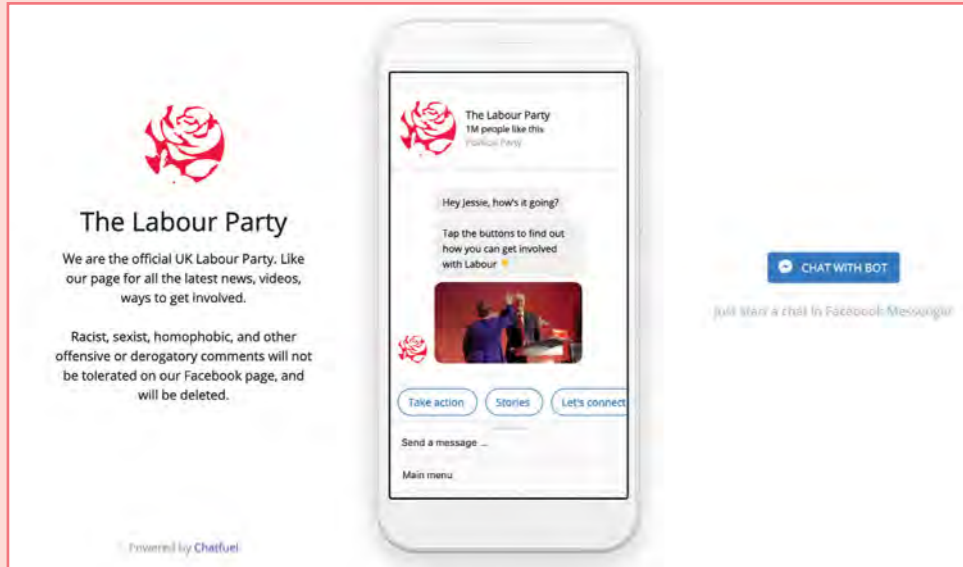Source: 'Bots Are More Than "Fake News" Machines', Chatbots Magazine, 23 February 2017, https://chatbotsmagazine.com/bots-are-not-per-se-fake-news-machines-c62a2fb6f571.

A screenshot of he UK Labour Party's chatbot, powered by the San Francisco-based company Chatfuel. Chatfuel boasts over 1 billion users with an 80% message open rate across its bots on Facebook Messenger.

Source: 'The Labour Party Chatbot', accessed 28 February 2019, https://chatfuel.com/bot/labourparty

A screenshot of political advertisements optimised via eye-tracking technology by the Kansas City-based political consulting firm Axiom Strategies. The visual heat map shows where subjects' eyes were drawn. Political campaigns are starting to adopt this technology to direct voters' eyes and attention as desired.

Source: 'Direct Mail – Axiom Strategies', accessed 18 February 2019, https://axiomstrategies.com/direct-mail/

This images was taken from the website DeliverTheWin.com, which was created by the United States Postal Service. It explains the benefit of using direct mail campaigns. The website has a section devoted to neuromarketing and how recent research has demonstrated its effectiveness in political campaigning.

Source: 'What Neuromarketing Means for Political Campaigns – USPS Deliver the Win', accessed 18 February 2019, https://www.deliverthewin.com/what-neuromarketing-means-for-political-campaigns/

A screenshot from @mssg, a company that offers an online chatbot to spur voter registration and get out the vote (GOTV) efforts.

Source: 'https://www.Atmssg.Com/Vote/', accessed 28 February 2019, http://www.atmssg.com/vote/
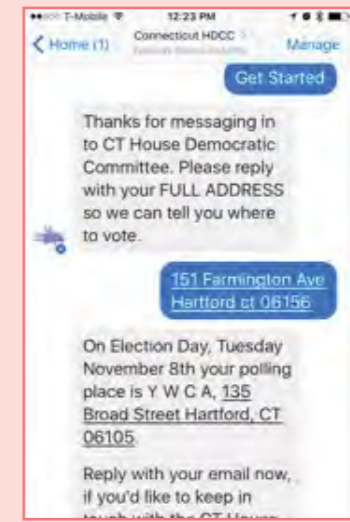
The company @mssg provides AI chatbots to clients via Facebook Messenger. Here, an @mssg bot asks a user for her address and returns her voting location. The service was enlisted by three campaigns in the US in November 2016.

Source: 'Case Study: Election Day Facebook Messenger Bot', @mssg, 14 February 2017, https://chatbotsmagazine.com/we-launched-a-bot-to-help-organizations-get-people-to-their-voting-location-5c8b-4da6b447
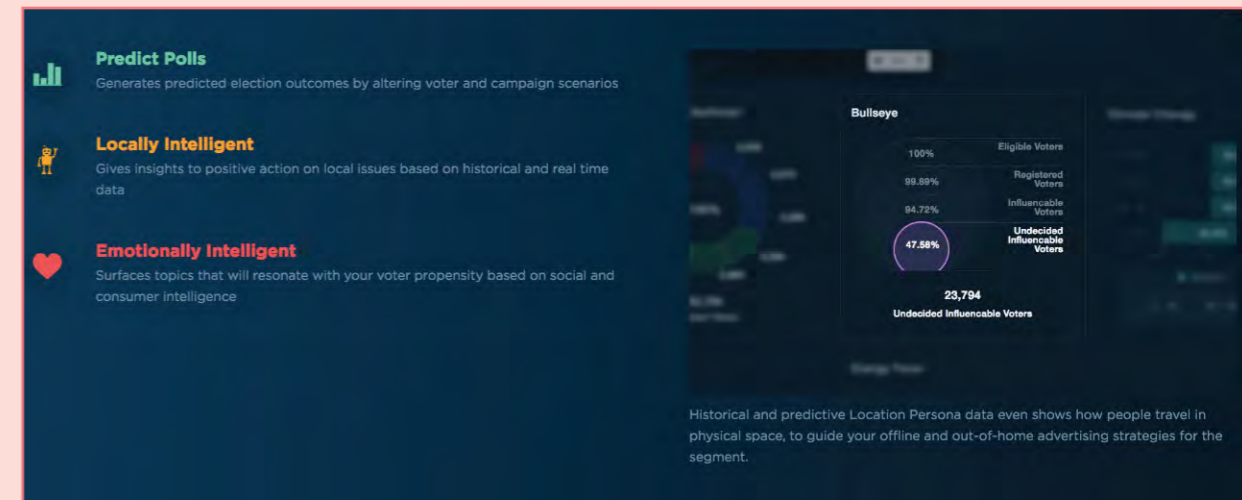

An analysis of Canadian Member of Parliament Elisabeth May's 2015 campaign website by the digital marketing firm Mediative shows that men and women engage with content differently. As the heatmap shows, women spend more time looking at the text in the bottom-left and at May's face. Men, on the other hand, seem more intrigued by the Green party logo.

Source: '5 Eye-Tracking Heat Maps Reveal Where Canadians Look When Reviewing Parties' Websites during the Federal Election', Mediative (blog), 15 October 2015, http://www.mediative.com/5-eye-tracking-heat-maps-reveal-where-canadians-look-when-reviewing-parties-websites-during-the-federal-election/.

A screenshot from the website of IQM, a company based in New York. Here, it advertises 'AI-powered voter intelligence' services and data on voters' whereabouts for more precise advertising capabilities.

Source: 'IQM - Solutions - Political', accessed 7 December 2018, https://iqm.com/political-solution

The rollout of the @mssg bot was paired with a test comparing the bot to a simple website. As Beth Becker, who runs a company helping progressive causes connect with their supporters, reflected, 'collecting data in a conversation is a novel approach, and the initial results are amazing. We can collect any and all types of data from these users—address, email, phone number, date of birth, etc. And now that Facebook has enabled person to person payments via Messenger, it's just a matter of time before organizations can collect donations in this manner, too'.[32]

In Canada: In the months leading up to the 2015 federal elections, performance marketing company Mediative assembled a small audience of five men and five women and reportedly used eye-tracking technology to 'tap into subconscious processes and decisions of an audience to understand which elements of the [campaign] websites' layouts trigger the fundamental brain circuits responsible to attention, cognition, and emotion'. The exercise used websites belonging to Canada's five major parties spanning the political spectrum and claimed to find, among other things, that men spent more time looking at logos, while women fixated more on family portraits. Some websites didn't help focus the eyes as much as others, suggesting areas for improvement. The blog post concludes, 'according to the findings of our study, it seems that Justin Trudeau is very popular among women; the conservative party's membership is more appealing towards men, the Bloc's layout can be confusing, the NPD is generating neutral emotions and the Green Party will attract more female voters. Joking aside, don't forget to vote and let democracy prevail!'[33] While some may question the efficacy and validity of eye tracking, it reflects how campaign decisions are becoming ever more personalised.

How do I know if it's being used on me?
While many of the technologies described here are not yet mainstream, they are likely to grow in popularity. If chatbots succeed in establishing rapport with voters, they will be difficult to distinguish from humans. Furthermore, there appears to be no way of knowing whether the ads or websites you consume have been enhanced using eye-tracking technology or cognitive computing tools intended to direct your eyes and mind to a specific message or image. The existence of connected IoT devices in your home does not necessarily mean that you are subject to precision targeting efforts by political campaigns, though the eagerness to leverage in-home devices for political purposes suggests this will change.

Considerations
↘ If implemented in a privacy-respecting and transparent manner, an advanced chatbot could engage in a question-and-answer session specific to a voter's needs. For example, a voter could engage in a conversation about the impact of a potential policy on their business.

↘ Bots avoid the risk of human error in simple tasks like looking up polling locations for a given address.

↘ Ill-intentioned political players could use personal data to feed users personalised propaganda and promote extremist views. Bots without access to personal data have already been found to do so.[34]

↘ Advanced chatbots could be made to mimic candidates' positions and promote spurious claims. Again in this case, voters may not know if they are communicating with bots or humans.

↘ IoT devices risk setting a precedent of dataveillance, the monitoring of online activities and digital actions for political insights. One academic commented, 'the IoT is essentially a massive surveillance network'.[35, 36]

↘ If techniques are combined, such as merging bots with micro-targeting, digital literacy challenges for voters and the complexity facing regulators will increase.

1
Jeff Chester and Kathryn C. Montgomery, 'The Influence Industry: Contemporary Digital Politics in the United States', accessed 28 February 2019, https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-usa.pdf.

2
Rose Acton, 'The Hyper-Personalised Future of Political Campaigning', CapX, 12 July 2018, https://capx.co/the-hyper-personalised-future-of-political-campaigning/.

3
Issie Lapowsky, 'Here's How Much Bots Drive Conversation During News Events', Wired, 30 October 2018, https://www.wired.com/story/new-tool-shows-how-bots-drive-conversation-for-news-events/.

4
Jamie Susskind, 'Opinion | Chatbots Are a Danger to Democracy', The New York Times, 4 December 2018, sec. Opinion, https://www.nytimes.com/2018/12/04/opinion/chatbots-ai-democracy-free-speech.html.

5
Fabio Chiusi and Claudio Agosti, 'The Influence Industry: Personal Data and Political Influence in Italy', accessed 28 February 2019, https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-italy.pdf.

6
Lisa-Maria Neudert, 'Future Elections May Be Swayed by Intelligent, Weaponized Chatbots', MIT Technology Review, accessed 4 February 2019, https://www.technologyreview.com/s/611832/future-elections-may-be-swayed-by-intelligent-weaponized-chatbots/.

7
Vyacheslav Polonski, 'How Artificial Intelligence Conquered Democracy', The Conversation, accessed 22 January 2019, http://theconversation.com/how-artificial-intelligence-conquered-democracy-77675.

8
Alex Boedigheimer, '5 Reasons Why Your Political Campaign Should Use Chatbots', IMGE, 9 September 2018, https://imge.com/news/5-reasons-why-your-political-campaign-should-use-chatbots/.

9
Deepak Puri, 'How to Make Fake Friends and Influence People Politically with Botnets', CIO, 6 April 2017, https://www.cio.com/article/3188011/election-hacking/how-to-make-fake-friends-and-influence-people-politically-with-botnets.html.

10
Nancy Scola, 'How Chatbots Are Colonizing Politics', POLITICO, accessed 22 January 2019, https://www.politico.com/story/2016/10/chatbots-are-invading-politics-229598.

11
Irene Del Carmen Pérez-Merbis, 'Bots Are More Than "Fake News" Machines', Chatbots Magazine, 23 February 2017, https://chatbotsmagazine.com/bots-are-not-per-se-fake-news-machines-c62a2fb6f571.

12
Thomas Maître, 'Donald Trump Chatbot Experiment', Chatbots Magazine, 8 November 2016, https://chatbotsmagazine.com/donald-trump-chatbot-experiment-f027b9a1caea.

13
Del Carmen Pérez-Merbis, 'Bots Are More Than "Fake News" Machines'.

14
Neudert, 'Future Elections May Be Swayed by Intelligent, Weaponized Chatbots'.

15
Nick Fouriezos, 'Meet the GOP's Chatbot and Artificial Intelligence Guru', OZY, accessed 14 February 2019, http://www.ozy.com/rising-stars/the-gops-chatbot-and-artificial-intelligence-guru/92254.

16
Scola, 'How Chatbots Are Colonizing Politics'.

17
Fouriezos, 'Meet the GOP's Chatbot and Artificial Intelligence Guru'.

18
Neil Hughes, 'Personalized Politician Chat Bots Predicted to Be next Big Thing Targeting Voters', One World Identity (blog), accessed 06 March 2019, https://oneworldidentity.com/personalized-politician-chat-bots-predicted-next-big-thing-targeting-voters/.

19
Neil Hughes, 'Researchers Seek to Mimic Digital Identities by Analyzing Email, Online Interactions', One World Identity (blog), accessed 12 February 2019, https://oneworldidentity.com/researchers-seek-mimic-digital-identities-analyzing-email-online-interactions/.

20
Hughes, 'Researchers Seek to Mimic Digital Identities by Analyzing Email, Online Interactions'.

21
Hughes, 'Personalized Politician Chat Bots Predicted to Be next Big Thing Targeting Voters'.

22
'The Eyes Have It | More Effective Political Ads – Discida', accessed 17 January 2019, https://www.discida.com/2014/09/more-effective-political-ads/.

23
Hicham Damahi, '5 Eye-Tracking Heat Maps Reveal Where Canadians Look When Reviewing Parties' Websites during the Federal Election', Mediative (blog), 15 October 2015, http://www.mediative.com/5-eye-tracking-heat-maps-reveal-where-canadians-look-when-reviewing-parties-websites-during-the-federal-election/.

24
'Connecting for Action - Canada Post Neuroscience Report', International Post Corporation, accessed 28 February 2019, https://www.ipc.be/sector-data/direct-marketing/research-analysis/reports/connecting_for_action.

25
'What Neuromarketing Means for Political Campaigns – USPS Deliver the Win', accessed 18 February 2019, https://www.deliverthewin.com/what-neuromarketing-means-for-political-campaigns/.

26
'IoT: Number of Connected Devices Worldwide 2012-2025', Statista, accessed 18 February 2019, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

27
Jordan Lieberman, 'The Digital Lessons of Election 2018', accessed 13 February 2019, https://www.campaignsandelections.com/campaign-insider/the-digital-lessons-of-election-2018.

28
Brittney Borowicz, 'The Internet of Things Is Transforming the Political Landscape', accessed 13 February 2019, http://blog.gridconnect.com/blog/general/the-internet-of-things-is-transforming-the-political-landscape.

29
Phil Howard, 'Politics Won't Know What Hit It', The Agenda, accessed 18 February 2019, https://www.politico.com/agenda/story/2015/06/philip-howard-on-iot-transformation-000099.

30
'Impact of IoT on Political Systems | Mark Skilton Personal Blog', accessed 13 February 2019, https://www.markskilton.com/single-post/2016/10/27/Impact-of-IoT-on-political-systems.

31
Borowicz, 'The Internet of Things Is Transforming the Political Landscape'.

32
'We Launched a Bot to Help Organizations Get People to Their Voting Location', Chatbots Magazine, 1 November 2016, accessed 12 March 2019, https://chatbotsmagazine.com/we-launched-a-bot-to-help-organizations-get-people-to-their-voting-location-5c8b4da6b447.

33
'5 Eye-Tracking Heat Maps Reveal Where Canadians Look When Reviewing Parties' Websites during the Federal Election'.

34
'How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral—POLITICO', accessed 28 February 2019, https://www.politico.eu/article/how-twitter-bots-and-trump-fans-made-releasethememo-go-viral/.

35
'Data Politics and the Internet of Things', Silicon Republic, 21 December 2016, https://www.siliconrepublic.com/enterprise/internet-of-things-ethics-security.

36
Connected World Staff, 'Politics in an Internet of Things World', Connected World (blog), accessed 13 February 2019, https://connectedworld.com/article/politics-in-an-internet-of-things-world/.

Considerations:
For regulators, political parties,
companies and voters

This guide seeks to broaden the debate surrounding technologies that leverage personal data for political campaigns, moving the discussion toward a more nuanced understanding of how they work, from geofencing campaign rallies in the United States to a massive robocalling effort in India and from breaches of voter files in Mexico and Taiwan to experimentation with eye-tracking technology on Austrian political ads. This research was founded on the premise that it is not only essential to have a better understanding of the tools in order to know how to respond to their use, but also to move beyond the question of their impact on individuals at the point of casting their vote. By taking a wider view, we can explore how personal data can be turned into political power and how particular methods can affect an entire community or a national political moment.

We can reasonably predict that digital technologies that leverage personal data will proliferate in the coming years, creating significant challenges for the consent and digital literacy of voters and for democratic processes overall. The fact that political campaigning is so closely tied to the commercial data industry means we can expect their methods to continue to advance in parallel. As these techniques become more commonplace and affordable, they will be used by a wider variety of political entities and influencers, beyond traditional party systems and outside of traditional election cycles. This is something we are already beginning to see evidence of.[1]

In understanding how each of these methods work we have also shown:

↘ Independently researched, detailed information about the inner workings of the technologies is essential for decision makers, regulators, journalists and voters.

↘ Transparency and openness by political parties and companies is key to the research process; it ensures that overviews such as this guide can be relevant and timely.

↘ Data-driven political campaigning methods should not be assessed as a single issue. Without looking at the individual methods in depth it is not possible to look at questions of efficacy, harm and political impact.

↘ The political resonance and impact of technologies changes in different contexts. They should be assessed in the political context in which they are being implemented and with attention to the particular strategies that are driving them.

↘ The time-bound nature of documentation and research presented in this guide shows that demonstrating how methods are being used, when, where, how and by whom, is an ongoing task.

What needs to be done?

While Cambridge Analytica no longer exists as a company, most of the technologies they used persist. The scandal coincided with a major change in European data projection law (GDPR). With these new regulations, and combined with mounting evidence of disruption to subsequent elections, a handful of the larger technology platforms have chosen to self-regulate. Some of their measures are welcome changes such as increased transparency; others only scratch the surface or have been interpreted as designed to increase market positions rather than protect user privacy.[2] Since mid-2018, several political parties and small-scale companies have modified their practices to ensure they are not misinterpreted or deemed controversial; others have simply become more discreet in their activities.

Multiple studies by policy makers, lawyers, technologists and researchers have been published since mid-2018. Many of these have recommendations: some for regulators focusing on necessary policy changes, others that make recommendations for large-scale technology companies.[3] Based on our research, we identified several key questions and considerations that stakeholders need to address.

For regulators

Most changes in electoral law take place in response to shifts in the environment or isolated incidents. This means that political processes are often exposed in 'all-or-nothing' campaigns such as referendums. In addition, because appropriate data protection laws are not enforced in all democracies, it is extremely difficult for regulators to proactively deal with challenges on the horizon. Addressing only the issues that rise to the surface leads to solutions that only deal with one aspect of the problem.

↘ Regulators need to look at technologies and their effects in a more granular way. For example, technologies like geofencing are more open to potential abuse in certain political contexts than others. How could regulations establish clear boundaries for some practices, while reducing the potential harm of others? Could mechanisms such as 'quiet periods', in which parties refrain from messaging immediately preceding an election, be more widely observed?

↘ Regulators are largely advised by the major technology platforms themselves, who favour self-regulation. Their rationale is based on the fact that their technology is complicated and that ill-advised regulation may prevent them from mitigating and reducing problems. How can regulators get more rounded, independent technical advice without relying solely on the dominant players?

↘ Regulation is often a balance between electoral laws and data protection laws, with an eye on free speech, particularly during election periods. Are there ways for regulators to deal with issues that may fall between the gaps in these two categories of regulation, such as the spread of misinformation through the content of micro-targeted ads? And how can they navigate the more debatable distinctions between campaign strategies and ethics, particularly as campaigns become more atomised and viral in nature?

↘ In some countries, existing rules and regulations on spending reporting call for transparency around data-driven political campaign practices. These rules need to be brought up to date to enforce 'meaningful transparency' from political parties so that their spending and related campaigning activities can be clearly declared.[4]

↘ Data-driven campaigning technologies cross borders, often implemented by companies who export and import services. As they translate to different political, social and cultural environments their impact on the democratic process is transformed. If regulators are primarily concerned with the impact on their own national political systems, how might they also tackle questions of overreach, interference or the cumulative political influence of large-scale platforms on a global scale?

For political parties

Political parties use data-driven techniques to varying degrees and in different contexts. Some are just experimenting, some are using volunteers or in-kind support, others have extensive, well-funded strategies. Amongst political campaign strategists, there are a wide range of attitudes about the effectiveness and relevance of such techniques. Some believe they will give them a more modern edge in a new style of politics, others think of them as 'snake oil' or inviting a kind of political campaigning they would not like to emulate. Either way, in those contexts where the mood is cautious, many parties don't want to accidentally expose themselves to risk, and others can't afford not to try the techniques in case they really do work.

↘ Leaders within political parties need to take responsibility for a set of practices that are often outsourced to third parties or put into the hands of marketing, technical or junior support within a campaign. When deciding what approach a political party wants to take, can they align their ethos with their political strategy?

↘ If these practices become normalised in political campaigns then there should be a common agreement about the best ways of implementing them in the democratic process. A consensus about best practices is urgently needed for parties who want to experiment but don't want to seem too invasive, drawing clearer lines between ethical and unethical techniques and strategies.

↘ Easy-to-use and cheap-to-deploy techniques, such as micro-targeting services, have the potential to be an equalising force but also to create unfair advantages. These services are easy to set up and affordable; as such, less well-resourced political parties report that they are welcome alternatives to relying on media coverage, which can be hard to get. However, they also advantage larger parties who have spending power and resources to work at scale. Could measures like spending caps help level the playing field?

↘ In some contexts, political parties have talked about a common agreement in which none of the parties use these techniques in a given election. Such agreements can't hold unless all the parties running in a particular election or campaign agree. There are no known, successful examples of such an agreement to date. Is there an argument for this to be tested again, and how might it be enforced?

↘ A lot of attention is paid to the use of these tools with regards to the acquisition of power. However, evidence shows that such tools are also increasingly being experimented with for the maintenance of power, leading to political parties that run a kind of 'permanent campaign'. Should we define the 'rules of the game' for parties running ongoing influence campaigns outside of election cycles?

For companies

Large-scale platforms who have come to dominate the internet, such as Facebook and YouTube, were initially considered to have a democratising force. As the scale, uptake and ease of use of data-driven tools has proliferated, there is a growing consensus that while these technologies are important for political debate and organising, they are also destructive. This creates an urgency for companies large and small to reflect on the services they offer and their potential consequences. The rate of change in the political sphere and the ways in which people can utilise these tools for debate, engagement and outreach have gone beyond the control of the companies themselves and present new challenges that they are forced to address. While the large-scale platforms begin to grapple with these problems, many of the same challenges will trickle down to more specialised data-driven technology companies.

↘ The culture of 'testing in the wild' that prevails in the technology sector means that there is a high level of experimentation with these methods in democratic processes. Is this an appropriate methodology for technologies that can be used in different contexts, some of them with very different social and political cultures and histories? How connected should companies be to the political and social realities of the environments they are working in and what difference could this make to the tools they create?

↘ Large-scale platforms that facilitate micro-targeting allow voters to get more relevant information, yet they have multiple disadvantages. These include problems such as allowing for prioritisation of who is considered a valuable voter and who is not (for example swing states or key target constituencies) and for granular segmentation and differentiation of messaging, which could lead to the polarisation of public opinion. What responsibilities do technology companies have when providing services regardless of the client, purpose or context? How neutral can tools really claim to be, and who holds the responsibility when they are used outside the original context of their design?

↘ Technology companies often change their practices in response to scandals. They need to determine whom else they should work with to change their polices and practices in advance, not only when it comes time to react to public pressure. When companies anticipate such problems and make proactive changes, they should be more widely communicated.

↘ Since March 2018, in some limited cases, data brokers and large-scale platforms have begun to treat their work with political parties differently—for example, requiring a declaration of who is paying for a political advertisement. These measures need to be rolled out with consistent testing and iteration, on a more global scale and outside of election periods.

↘ Technology companies have a vested interest in selling services to political parties, as a significant income generator or in some cases as their main business model. In these cases they should be consulting with regulators, but not directly advising them without the equal access of independent parties who understand the technology.

↘ If large technology platforms are invested in facilitating healthy democratic processes, should they even be treating political advertising as an income generator at all? In what scenarios could they consider treating pre-election periods as a no-fee period with equal access to advertising slots for political parties?

For voters and citizens

Voters and citizens today are faced with a shifting political landscape combined with rapidly evolving technologies that can be hard to comprehend and follow. Increasing complexity, along with the opacity of the tools that are being used to persuade them, can create an overwhelming environment for voters and citizens, which could lead to disengagement.

↘ Many of the mechanisms for regulating and controlling users' data are consent-based. How realistic is 'meaningful' and 'informed' consent in the context of complex and opaque technologies?

↘ Even if individuals do consent, it does not resolve the problem of the impact of these techniques on the overall political system. More studies are needed that look at their implementation in context and their impact on the overall political moment.

↘ Individuals targeted by political ads are not always convinced such techniques can persuade them to vote for a certain candidate. However, the larger concern may be that such techniques actually seek to suppress votes or confuse voters by spreading misinformation or creating a politically divided environment.

↘ Some argue that with the proliferation of sources of information for voters, individuals should be able to contextualise the messaging they receive from political campaigns. Yet in some cases, content found online may be their sole source of information, particularly with rising concern about the impact of filter bubbles on voters. Studies have shown that this is particularly the case for digital natives[5] who predominantly use online information sources, as well as for some communities who use 'zero rating' services which allow free data access to only specific platforms, such as Facebook or WhatsApp.[6]

↘ As voters become more aware of data-driven campaigning practices, their granular nature, and the way that they are analysed and targeted, they may lose trust in politicians, political parties and the democratic system overall. How can voters understand the mechanisms at play without losing faith in political parties? The public's trust in the political system depends on it.

1

See also Greg Elmer, Ganaele Langlois and Fenwick McKelvey, The Permanent Campaign: New Media, New Politics, Digital Formations, vol. 81 (New York, 2012).

2

Ginny Marvin,'Facebook's Removing Third-Party Targeting Data: What Marketers Need to Know', Marketing Land, accessed 12 March 2019, https://marketingland.com/facebooks-removal-of-third-party-targeting-data-whatwe-know-237260.

3

Some of our recommended resources include: Dipayan Ghosh and Ben Scott, 'Digital Deceit: The Technologies Behind Precision Propaganda on the Internet', https://www.newamerica.org/public-interest-technology/policypapers/digitaldeceit/; Cristina Tardáguila, Fabrício Benevenuto and Pablo Ortellado, 'Fake News Is Poisoning Brazilian Politics. WhatsApp Can Stop It.', New York Times, https://www.nytimes.com/2018/10/17/opinion/brazilelection-fake-news-whatsapp.html; Julianne Kerr Morrison, Ravi Naik and Stephanie Hankey, 'Data and Democracy in the Digital Age', https://consoc.org.uk/publications/data-and-democracy-in-the-digital-age/; Section on data use and data targeting in the final report of the Digital Media Culture and Sport Committee on fake news, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm, Privacy International's recommendations available at: https://privacyinternational.org/topics/data-and-elections.

4

See the Data and Politics team on spending in the UK for more details, 8 August 2018, https://ourdataourselves.tacticaltech.org/posts/overview-uk/.

5

Mauricio Moura, Melissa R. Michelson, 'WhatsApp in Brazil: mobilising voters through door-to-door and personal messages', Policy Review, accessed 12 March 2019, https://policyreview.info/articles/analysis/whatsapp-brazilmobilising-voters-through-door-door-and-personal-messages.

6

Raquel Renné, 'The Widespread Use of WhatsApp in Political Campaigning, 13 November 2018, https://ourdataourselves.tacticaltech.org/posts/whatsapp/

Get a digital copy of the guide: *How it Works* and see the accompanying visual gallery
What's for Sale? at:
tacticaltech.org/projects/data-politics

Contact us at: ttc@tacticaltech.org
For press inquiries: press@tacticaltech.org

About Tactical Tech:
Tactical Tech is a Berlin-based NGO that investigates the evolving impact of digital technologies
on society. Through our work we aim to educate, advocate and create practical solutions that
contribute to the wider socio-political debate around digital security, privacy and the ethics of data.

About Tactical Tech's Data and Politics project:
Inside the Influence Industry: The Global Business of Using Your Data in Elections, is a
practitioner-led research initiative conducted by the international non-profit organisation,
Tactical Tech and its partners. The initiative documents and provides a framework
for understanding the use of personal data in political campaigns worldwide.

TACTICAL
TECH

www.tacticaltech.org