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

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

Authors
Varoon Bashyakarla
Stephanie Hankey
Amber Macintyre
Raquel Rennó
Gary Wright

Cover and Illustrations
Maria Kassab

Creative Direction
Stephanie Hankey

Design Support
Philippe Collinge

Editor
Christy Lange

Research support
Nicole Ayo von Thun
Sascha Gubskaya
Morana Miljanovic

Copy editor
Michael Runyan

Communications
Caisy Kief

Tactical Tech’s country-study partners:
Articulo 12 (Mexico)
Bao Su-Lyn (Malaysia)
Coded Rights (Brazil)
Claudio Agosti and Fabio Chiusi (Italy)
Calin J. Bennett and Robin M. Bayley (Canada)
Elronad Hickok (India)
Eticas Foundation (Catalonia)
Fundación Datos Protegidos (Chile)
Grace Mutung’u (Kenya)
Jeff Chester and Kathryn Montgomery (United States)
José Luis Peñarredonda (Colombia)
Judith Dupont (France)
Marianela Milanes (Argentina).

© and ℗ 2019 Tactical Tech.
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.

This guide is typeset in Lato.

This guide was possible thanks to the support of:

OAK FOUNDATION
Sida

and Tactical Tech’s other funders.

Introduction
by Stephanie Hankey

Data as an asset

Consumer Data: The fuel of digital campaigns
by Gary Wright

Voter Files: Political data about you
by Amber Macintyre

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

Data as intelligence

A/B Testing: Experiments in campaign messaging
by Varoon Bashyakarla

Campaign Apps: Tap to participate
by Varoon Bashyakarla

Third-party Tracking: Cookies, beacons, fingerprints and more
by Varoon Bashyakarla

Digital Listening: Insights from social media
by Amber Macintyre

Data as influence

Geotargeting: The political value of your whereabouts
by Varoon Bashyakarla

Search Result Influence: Reaching voters seeking answers
by Raquel Rennó

Addressable TV: Who’s watching what you’re watching?
by Varoon Bashyakarla

Robocalls and Mobile Texting: Automated campaign outreach
by Gary Wright

Psychometric Profiling: Persuasion by personality
by Varoon Bashyakarla

Upcoming Technologies: The next frontier in campaign technology
by Varoon Bashyakarla

Considerations: For regulators, political parties, companies and voters
by Stephanie Hankey

Contents
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 and how public relations directors at the time boasted that strategies designed to sell candidates to voters ‘like toothpaste’, and how political parties used to sell shoes to consumers. The result of this is that we need to understand the breadth, depth and scale of the techniques that we can begin to understand their relevance to the current political moment.

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 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 and how public relations directors at the time boasted that strategies designed to sell candidates to voters ‘like toothpaste’, and how political parties used to sell shoes to consumers. The result of this is that we need to understand the breadth, depth and scale of the techniques that we can begin to understand their relevance to the current political moment.

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 largest political campaign budgets for experimentation. The fact that data-driven campaigning techniques originated in the US, with George W. Bush’s 2004 presidential campaign8 and Barack Obama’s 2008 presidential campaign9 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 our 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 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.
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 use of personal data at some point in the process of political campaign its leading edge. 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 uninvasion has been claimed by some campaigners to be key to their success. 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.
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 parties with more money or access to resources can gain advantages, potentially changing who can participate. The accumulation and intra-party trade of data over time can also create inequities between candidates and across parties.

Voter databases can become assets, traded or 'gifted', creating significant advantages across 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 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.
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.’ Using that data, Experian boasts it can address 85% of the US, link to 500 million email addresses 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.’ But the company is not only offering their data to marketers: their ‘Political Personas’ segmentation tool defines categories like ‘Super Democrats’ and ‘Green Traditions’ to give political parties insights into issues, attitudes and trends among voters. All of this 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. 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. 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. In a deep-dive on this topic, technologist and researcher Wolfe Christ's report ‘Corporate Surveillance in Everyday Life’ categories consumer data into several flavours, including: volunteered data, observed data, actual data and modelled/inferred data, which is based on analysed activities and behaviours. 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. 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 and vendors of ‘smart’ devices 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 campaigning. 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 traditional data brokers such as Acxiom, Epsilon and Experian (including Brazil-based Serasa Experian, which holds the largest consumer data sets in the Latin American region) 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, 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. 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.

- 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, Google Maps, 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. Google, meanwhile, claims that eight of its products reach over a billion users each, along with two billion active Android users. 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. 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: audience data was provided by both Acxiom and Serasa Experian 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’ and Google’s ‘customer match’), and extended ‘searches’ for customers (Facebook’s ‘lookalike audiences’ and Google’s ‘similar audiences’). 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 conservative-leaning firm largely funded by the Koch brothers—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. Similarly, Advocacy Data consultancy 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. Aristotel provides datasets ‘complete with donor history, demographics and lifestyle information’. Political data consultants who use consumer data as part of their data strategies have been identified in elections in Brazil, Argentina and India to name a few.

- Other sources: Beyond traditional 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 campaigns. 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. Their findings include that neighbourhoods with more sedans than pickup trucks were more likely to lean to the Democratic Party. Satellite data has been actively implemented by political data consultants in their offerings to customers. HaystackDNA, 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.

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 actual 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, and devices 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.’
- Voters can be increasingly segmented into ‘in’ or ‘out’ categories, respectively their support for or against a campaign.
A screenshot showing an excerpt of search results after querying the Electoral Commissions public database for party spendings at Experian.


The composition of i360's database for political campaigning, including over 700 consumer data points.

Voter Files: Political data about you

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 or data brokers—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 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 benefited 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 individual interests.

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.1

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.2 Before elections or referendums the registers are sent to official campaigns for use to send out promotional material.3 The open register, which citizens can opt out of, can be bought by any person, company or organisation for any reason.4 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 robo calling. 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 streaming 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.5 Another provider, I2, 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.6

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, 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.7

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.8 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.9

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).10 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.11

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.12 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 uses this data to create a score 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].13 In the deregulated environment there is little transparency about exactly what the data 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 an in-house database software called Contact Creator, which contains data on preferences, interests, voting behaviour and socio-economic information.14 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 and maintained Excel spreadsheets to host supporter information.15
This screenshot from GitHub shows fields belonging to US voter registration data.

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

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

A screenshot of the Canadian Conservative Party’s scale of different voter support levels, ranging from non-supporter (-15) to supporter (+15).

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.
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. In the UK, the Labour Party and Conservative Party have had issues with their databases, from persistent glitches to crashes.

• 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.

2. Political H2, ‘NyamataDNA’.
6. Coventry City Council, ‘The Electoral Register and the Open Register | Registering to Vote.
Breaches, Leaks and Hacks: The vulnerable life of voter data

What are breaches, leaks and hacks?

Data breaches, leaks and hacks go beyond consumer data. 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 wide international media coverage has largely looked at data hacks and breaches in elections through the loss of leaked emails, nation-state involvement in misinformation campaigns, or insecure infrastructure (such as vulnerabilities in voting booth software), 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 citizens are unaware that their data has been compromised, according to a report by the Center for Strategic and International Studies and McAfee. 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 53 million people, including the president, finance minister, and police minister. The data included income, address, and phone numbers.1

What kind of data is involved?

Compromised voter data generally comprises data from two possible sources:

- **Official voter registers:** While variations 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, such information is stored on digital spreadsheets and can be emailed to those purchasing the voter files;2 depending on the state. 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.3

- **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, 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.4 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.5

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.6 Simultaneously, a website went live claiming to contain the full 340-gigabyte database of 55 million registered voters.7 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.8

**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 the 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.9

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.10 The leak included names, addresses, birth dates and national ID numbers and was detected with 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 falling to properly secure its copy of the list.11

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 ‘modelled ethnicity’ and ‘modelled 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.12

**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.13 While the affected data appeared to be from 2008, Isik Malat, a Turkish privacy activist stated to Wired “I searched my name on the list and reached my whole family... 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.”14

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 crowdsource 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 BLC vendor ‘may have persistent access and/or contact with government officials from each state’.15

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 dis- and mis-information campaigns in national or even small scale elections.16 Often, compromised voter data is covered by specialists blogs, cyber-security 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.

As much as data on voters can be a political asset, it can also be a liability.17
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, during a cursory Shodan search.


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.


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


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.


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

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 of arguably lesser value, other examples of breached data have more serious implications. For example, in October 2018 a security researcher was able to access an unreported and internet-connected digital storage instance belonging to Rice Consulting, a US fundraising firm hired by the Democratic Party. 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 firm hired by the Democratic Party.

Ultimately, the value of voter data is significant, especially if it becomes exposed on the open internet. There is 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 care.

Considerations

1. 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, however, means that there is little insight into who 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 André Sepúlveda and other reported activity in Latin America and cases where compromised voter data was used to disrupt the election process.

2. 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 of arguably lesser value, other examples of breached data have more serious implications. For example, in October 2018 a security researcher was able to access an unreported and internet-connected digital storage instance belonging to Rice Consulting, a US fundraising firm hired by the Democratic Party. 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 firm hired by the Democratic Party.

3. Ultimately, the value of voter data is significant, especially if it becomes exposed on the open internet. There is 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 care.
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 adopted 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.
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 way they ask for money. 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’, which performed the default message by a whopping 18.6%. When they tested the prompt alongside six different photo and video options, the winning combination boosted their sign-up rate by more than 3%. While this number may seem small, the campaign estimated that this single change contributed to nearly three million new email address sign-ups by 161%. 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%. A/B testing, sometimes called split testing, compares two or more variants of an advertisement or message to determine which one performs best. One of the most popular uses of this method is for experimenting with the donation experience. 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.

Some examples
In the UK: Dominic Cummings, the 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 visitors 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. 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.

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, no personal data 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 may deem you a promising voter.

In the United States: Political campaigns are using A/B testing at a staggering scale in the US, even compared to private companies.22 Nowhere was this more clear than in Donald Trump’s 2016 presidential run. Gary Cooby, the director of digital advertising and fundraising for the Trump campaign, called their use of experimentation A/B testing on steroids.23 The campaign reportedly ran 40,000 to 50,000 variants on a given idea,24 and these experiments proved lucrative. As Michael Balsak, former director of marketing technology at the Republican National Convention claimed, ‘The RNC’s Performance, Optimization & Experiments Team […] ran over 300 tests on DonaldTrump.com from July through November 2016, generating over $130 million in added revenue’.25 The team concluded that pro-Trump messages always beat out any anti-Hillary or otherwise negative copy.26 While the election, in May 2018, Cooby declared on Twitter that the campaign still had over 4,000 ads active for ‘testing and learning’, extending the campaign’s intelligence-gathering activities beyond the election.

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 experiments; moreover, permission is often requested by algorithms can create exponentially more 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.

As an 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.” 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.

A/B testing services become more automated, algorithms can create exponentially more 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.

As A/B testing services become more automated, algorithms can create exponentially more 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.

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 about voters.

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.” 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 exponentially more 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.

As an 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.” 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 exponentially more 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.

As an 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.” 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 exponentially more 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.

As an 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.” 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 exponentially more 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.

As an 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.” 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 exponentially more 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.

As an 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.” 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 exponentially more 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.

As an 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.” 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.
A/B testing is moving towards algorithmic generation of variants. Using data to create the most compelling ad for a given user, algorithmically-generated variants allow computers to decide what users see by customizing different ad creatives for different individuals. This screenshot was taken from promotional Facebook video by Facebook, a popular experimentation platform for political campaigns. The voiceover audio explains that advertisers supply images, video, text, and calls to action, budget, and target audience, and the product will decide which combinations work best with any given audience.

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

An article published on medium.com explored 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. This was tested through his website, BenCarson.com, which was no longer active at the time of writing.

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, encouraged 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 $US 15 and were seen between 10,000 and 60,000 times.


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.

Source: https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_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 showed how Donald Trump’s campaign tested these two background images against each other on their donation page. The image of Trump performed about 80% better than the image of Clinton.

Considerations (continued)

3. Political campaigns maintain that the method is an effective testing ground for politicians—a space to trial an idea and conceal it if it fails, or promote it if it works.

4. 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 solutions: “Why debate when you can test?”

5. At its extreme, A/B testing risks ‘circuiturning the reasoning process altogether in the search for what works,’ redirecting campaigns’ attention from issues to button colours.

6. 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.


17. ‘Optimization at the Obama Campaign’.


25. Babcock.

26. According to Facebook’s new political ad portal, the Trump campaign has bought more than 3,000 ad-variants since July 7th of this year. Lots of A/B testing with different text/image/variants. https://www.facebook.com/politicalcontentads/Active_status=all&active_status=1&action=7&ad_type=political_and_issue_ads&country=US

27. “You have almost certainly been part of an A/B test.”
Campaign Apps: Tap to participate

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-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 those 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.

- Games and gaming 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. These games, which tend to use 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 to defeat a rigged system... Together we can win!’ 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. 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 the 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.’

Campaign apps typically collect four types of data:

- 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.’
- 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 neighbors, generating valuable cross-section data on the supporters’ political views, activism affinities and personal network, essential information for a modern, data-driven campaign.’ While Cambridge Analytica’s final product was not an app, the data for its psycho-metric 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.) 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.

- 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 individual 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.

In France: In the lead-up to the 2017 French Presidential elections, Nicolas Sarkozy’s campaign developed an app called Knockii, 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 of data-driven electioneering in the country.

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 numbers, a unique number that identifies mobile phone users and can potentially be used to track or eavesdrop on users.

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.

“We’re in a race against time to defeat a rigged system... Together we can win!”

TEXT FROM THE ONLINE POLITICAL GAME CORBYNRUN

In the lead-up to the 2017 French Presidential elections, Nicolas Sarkozy’s campaign developed an app called Knockii, 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 of data-driven electioneering in the country.

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 numbers, a unique number that identifies mobile phone users and can potentially be used to track or eavesdrop on users.

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.


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 can upload data into the 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

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 as other political rivals. The app gamifies the process by measuring how many personal messages the user has sent to meet their ‘Personal Goal.’


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, shows 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.’


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.


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.


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.

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.

By profiling voters’ homes and tailoring canvassers’ talking points, enhanced canvassing apps can make interactions more personalised, but 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 the ‘right doors’ and making the ‘right calls’ implicitly attempt to avoid spending resources on their assumptions about politically misaligned or unengaged individuals. 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 both the ideological diversity of larger social networks, they risk creating filter bubbles or confirmation biases.

Because these digital products often survive in some form post-election, they set a precedent for a never-ending campaign season.
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 Binder's New Hampshire Senate campaign did in 2010 with the help of a marketing firm called RapLeaf. But how did RapLeaf know who was interested in the Bible and also concerned about the environment? And how do donations, address, age, and even hobbies'?

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. These first-party cookies improve your user experience and generally do not create as many complications as third-party cookies, which track your browsing and match your browsing between sites.

Beacons: Beacons are physical devices that wirelessly register the presence of nearby mobile devices. Beaconstart, 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 attend-
es. Attendance could then be combined with other data points obtained, for instance, by a companion mobile app for the campaign.

IP Targeting, Geofencing, and Other Technologies:
Campaigns are expanding beyond tracking cookies into more sophisticated techniques such as IP targeting and geofencing. IP addresses identify not only a specific connection to the internet, they also reveal the campaigner’s approximate geographical location. Political campaigns are targeting set-top boxes and other relatively static connected devices to “anchor” to a home’s physical location through its IP address. Mobile devices can be tracked through geofencing, which tracks users’ locations based on their GPS data or connections that can be registered by beacon technologies such as Blue-tooth, Wi-Fi and radio frequencies. Many other techniques are proliferating: a recent assessment identified 70 different tracking technologies at work in common email campaigns.

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 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.”

Across the European Union: A 2018 investigation found that a number of European political parties 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 agen-
cies. 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 our website.”

How can I avoid being tracked?
Recently browsers have implemented a ‘Do Not Track’ request; however, it is not binding, a tracker can simply ignore the request. Browser extensions and ad blocking firewalls offer more robust defenses. Yet, cookies are currently too useful for non-tracking purposes to easily block outright. However, 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.

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. Notices of voter privacy are changing how some political campaigns deal with voter information, seeking consent for communications and offering some degree of transparency regarding their collection of data, even permitting corrections.

Some services are becoming more transparent: Google allows users to review what information the company has amassed on them for advertising purposes. 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.
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.


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’.


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’.


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.


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


A visualisation of potential trackers on UK political party campaign websites from June 2017, based on an investigation at Tactical Tech. Labour’s website exceeded the trackers on the Conservatives’ website.

Source: Tactical Tech, 2018
Considerations

Tracking can prevent users from seeing the same ad repeatedly.26

Cookie matching can enable political campaigns to exclude voters who are not politically engaged from seeing political ads.25

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.25

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.

Cookie matching helps political campaigns exclude voters who are not politically engaged from seeing political ads.25

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.

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.

Cookie matching helps political campaigns exclude voters who are not politically engaged from seeing political ads.25

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.

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.

Cookie matching helps political campaigns exclude voters who are not politically engaged from seeing political ads.25

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.

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.

Cookie matching helps political campaigns exclude voters who are not politically engaged from seeing political ads.25

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.

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.

Cookie matching helps political campaigns exclude voters who are not politically engaged from seeing political ads.25

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.

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.

Cookie matching helps political campaigns exclude voters who are not politically engaged from seeing political ads.25

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 this 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 a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor. Additionally, simply soliciting users for access (e.g., click ‘Accept all cookies to access this website’) is not a political actor.
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. 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 catalyse product choice, and more. Through their authentic voices, you get real, nuanced, and unexpected insight into consumer behaviour.”

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 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. Portent.IO, rebranded as YouGov Signal, carries out text and behaviour analysis on Twitter to ‘distill 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.

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.’ Among their services they offer to help political actors to ‘stay on top of what voters are thinking,’ create lists of 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.’

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.’ 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.

Another company, Ossalabs, markets their Election Impact tool specifically for political campaigns. Ossalabs advertise that through their tools they can help politicians ‘prepare for public questions by keeping your fingers on the pulse of current 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.

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 AutoPolitics worked on the mayoral campaign for Taipei in 2014, AutoPolitics, in their words, ‘crawls and transforms social media data into actionable intelligence.’

A first-time candidate running for Mayor of Taipei, Ko Wen-je worked with AutoPolitics. 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.’

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.

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.

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.

“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.”
Canada Has Legalized Weed and Banff National Park is Loving It
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.

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.

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.

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.
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’, 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.

References

8 Politics - NUVI - Real-Time Social Intelligence.
10 Bernie Sanders and Kamala Harris Most Discussed Democratic Party Candidates.
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 your daily habits and routines to personality traits and 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 practiced 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 registries, third-party providers and more.3 As the number of sensors around the world increases, location data will become even more accessible.5 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 individual 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 those inferences.
- **Mobile and property geotargeting**: targeting political messages to less granular geographic segments or aggregations, such as postal codes via the post or mobile phones.

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 a trove 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 Jumpstart, 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.2

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.8 In the US, Snapchat deployed a voter registration campaign before the 2018 midterm Congressional elections.9

Political campaigns have also started IP targeting. DSPotential, a political consultancy based in Washington D.C., 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.10 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 re-election 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 Murkowski’s ad appear 7,000 times. In January 2018, the head of the Interior Department formally approved construction of the road.11

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 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.12 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.13

In France: The firm Liegey Muller Pons (LMP) has provided election services to over 1,000 campaigns across European countries.14 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.15 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 to 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.’16

Nearly all campaigns use popular technology platforms to geotarget ads, whether on the city, district, neighbourhood or individual household level.”
A screenshot from the Snapchat website showing that Rob Portman’s 2016 re-election 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.


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


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 their physical addresses.


A screenshot from El Toro’s website shows the company’s geospatial technology can assist political campaigns.


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 their physical addresses.

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.

The personal profiles created based on geolocation data are not transparent.

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 showcase their successes by publishing “high-value areas,” leading some to wonder how these same services treat “low-value” areas. Others have underscored the importance that organizations make, the bigger concern is the way these biases can undermine democratic principles, such as by excluding people from the political process.

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. 5 Reports of law firms sending ads to patients in emergency rooms have also been documented. Geotargeting tactics like these can be used towards ethically dubious ends and are subject to very little oversight.

Considerations

1. 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.

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

3. 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.

4. The personal profiles created based on geolocation data are not transparent.

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

6. 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 showcase their successes by publishing “high-value areas,” leading some to wonder how these same services treat “low-value” areas. Others have underscored the importance that organizations make, the bigger concern is the way these biases can undermine democratic principles, such as by excluding people from the political process.

7. 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. Reports of law firms sending ads to patients in emergency rooms have also been documented. Geotargeting tactics like these can be used towards ethically dubious ends and are subject to very little oversight.

---


"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.”
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.6

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.7 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. 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 services, 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 on AdWords extensions, like phone number. Additionally, Responsive Search Ads allow advertisers to make ads that have multiple variables—such as different headlines 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 US12 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 ads 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 ‘Unfair (maize flour)’ was used, the first result promoted a news-type article claiming that Kenya 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
Mobile phone screenshots obtained from research with Kenyan country partner in the run-up to the 2017 Kenyan general election showing advertising in Google search results that discredited Raila Odinga (the opposition) and praised Uhuru Kenyatta (the then president).

Source: Tactical Tech, 2018

Tweets from Donald Trump in August 2018, claiming that Google’s search results are biased.

Source: Twitter, 28 August 2018, https://twitter.com/realDonaldTrump/status/103445273364243076
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.’

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 flipside, 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 Shamoon McGregor documented the work of Microsoft, Facebook, Twitter and Google’s sales teams during the 2016 US presidential cycle. 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.

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.

Considerations

12. At the time of writing this service was only available for US political advertisements.
28. “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.”
Addressable TV: Who’s watching what you’re watching?

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 advertisers new possibilities for political advertising and microtargeting, 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 campaigns to target advertisements to TVs with the same precision as those delivered over the internet, displayed on mobile phones, and sent via the post. The method is still quite 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 internet—gives advertisers the ability to target voters via Addressable TV using basic demographics like their ethnicity, as well as more intimate details like their purchasing habits.3

That data comes from three sources: 3

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

2. **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.

3. **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. For instance, the digital advertising company Attico 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 purchasing habits. 4

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. Ben Tat-ta, former CEO of Cablevision, 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’. 5-8 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
- **mits:** The multi-channel network mits launched a campaign to focus on driving bilingual, millennial Latinx 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 Rodríguez, a Puerto Rican-American actress.

- **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.10 D2 Media’s advertising platform delivers addressable ads to nearly 22 million households.11 The company forged partnerships with data providers for both major American political parties including (360 and DeepRaid Analytics, both of which service Republican campaigns, and TargetSmart, which caters to centre-left candidates.12, 13, 14 In 2016, D2 Media provided Addressable TV ads to over 100 political campaigns.15

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.16 These 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’.17 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’.18 Between the 2014 and 2016 American election cycles, the use of Addressable TV increased about 60%.19 Addressable TV is expanding to Latin America and Europe, but its adoption in political campaigning outside the United States appears to be slower.20, 21, 22

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.23 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 introduced the right to watch anonymously.24

- **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 unfruitful 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.**

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


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.


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=0LLt-a6dI_0, accessed 5 March 2019
Robocalls and Mobile Texting: Automated campaign outreach

What are robocalls and mobile texting? These longstanding campaigning methods of direct mail and phone banking have evolved: advances in technology have allowed these “old-fashioned” techniques to be used at a far wider scale and scope than ever before. The growing accessibility of voter data now provides robocalling and mobile texting 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 may seek to increase voter segmentation by conducting surveys and polls. 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 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.

How is your data used? Calling and texting both aim to reach you as directly as possible by using 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 advertises “yellable voter data [at] just 3¢/record,” 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.

Texting services are similar in that they also obtain and utilize mobile phone numbers from existing voter lists or self-sourced voter files. Services such as uCampaign, RumbleBots and Relay 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.” 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 and Political Data Inc.

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 phone to answer questions. This data can be quickly processed to enhance the data assets of campaigns and voter data platforms like NGP Van.

In the field of texting, Upstream Software’s Mobile Messaging 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’ phones numbers to invite them to join the mobile list.” Callhub’s SMS Marketing Software 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’” 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 robo-calling 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 in Canada were subject to a voter suppression campaign 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 maintained and controlled by the Conservative Party of Canada,” accessed for that purpose by a person or persons currently unknown. In 2014, a former Conservative Party staff member was found guilty of violating Canada’s Elections Act for his involvement in the robo-calling misinformation campaign. The former staff member had made several thousand robocalls to voters in Guelph, Ontario with a disposable mobile phone.

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 about the political campaign of the state’s Chief Minister and 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. Additionally, data gathered by the robo-calling campaign was analysed in order to “steer party activists [sic] to visit voters’ with political leanings toward the opposition Indian National Congress Party. In response, the Congress Party filed complaints with the national 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 robo-calling. A report for Tactical Tech details several instances of voters being contacted via phone by the ‘National Census Department.’ 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 Interviewe stated that she had been contacted by one of Malaysia’s leading outsourced 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 and how the voter contact data was obtained or how the results of the calls would be processed.

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.

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 robo-calling or texting campaign: voters will notice their inbox and phones bombarded by political messages from candidates or causes.

Mass and direct voter contact through robo-calling and texting are often regulated by local consumer protection laws to contact voters only with their consent. 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.

Despite these restrictions, US-based robocalling 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. 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 “robocall,” even when it involves sending mass, canned responses to thousands of voters’ mobile phones.
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 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 and is the most popular messaging app in large parts of Africa, Asia, Europe and Latin America, where it is used by friends and family to communicate directly, but also by large groups of people who share common interests – fans of a particular football team to those who share similar political views. It has been used as an effective tool for political and social organizing.

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. 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.

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 sources. 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, bulk messaging to large number of users and analysis of group chats such as sentiment analysis.

In addition, our partner country’s 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.

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, so much so that the country’s Communications Authority threatened to hold group administrators responsible for the contents spread in their groups. 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 had digital marketing firms to spread tens of thousands of attack ads on WhatsApp. 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.”
Similarly, RoboCent offers its version of ‘ringless voicemail technology’, which allows a prerogated 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’. The Federal Communications Commission has yet to rule on the legality of the technology.\(^\text{[16]}\)

**Considerations**

- **Robocalling and texting directly utilize 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 and parties with voters—a possibility that has only recently emerged on a mass scale.\(^\text{[18]}\)** 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.\(^\text{[19]}\)

- **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\(^\text{[20]}\), during the course of an election campaign, such as in the run-up to the 2019 election in Nigeria,\(^\text{[21]}\) or the SMS-based scan identified by Elections Quebec in 2018 which fraudulently promised payment for political support.**\(^\text{[22]}\)

- **Robocalls can also be used for nefarious purposes, such as the cases during the 2018 US Midterm elections where a white supremacist podcat initiated automated calls to voters in Florida and Georgia featuring racist and anti-Semitic messages targeting each state’s African-American candidates.**\(^\text{[23]}\)

---

1. The technologies examined here are purposely centered on American examples in order to showcase some of the more untested sides 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 to large in historical low costs per SMS, messaging platforms such as WhatsApp are much more prominent in other countries.


27. ‘Robocalling and texting directly utilize a voter’s personal data and engage intimately with the voter in order to deliver campaign materials and messages and conduct polls and surveys.**

28. ‘Robocalling and texting could be considered a means of direct communication between politicians and parties with voters—a possibility that has only recently emerged on a mass scale.\(^\text{[18]}\)** 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.\(^\text{[19]}\)

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

30. There is increasing evidence that texting contributes to the proliferation of misinformation and fake news\(^\text{[20]}\), during the course of an election campaign, such as in the run-up to the 2019 election in Nigeria,\(^\text{[21]}\) or the SMS-based scan identified by Elections Quebec in 2018 which fraudulently promised payment for political support.**\(^\text{[22]}\)

31. Robocalls can also be used for nefarious purposes, such as the cases during the 2018 US Midterm elections where a white supremacist podcat initiated automated calls to voters in Florida and Georgia featuring racist and anti-Semitic messages targeting each state’s African-American candidates.**\(^\text{[23]}\)
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. 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.1, 3, 4, 6, 11

Psychometric profiling is the process by which your observed or self-reported actions are used to infer your personality traits in order to customise the messages you receive. The marketing industry, public relations and politics have long used psychology to understand and influence individuals’ beliefs, behaviours and motivations.2 Psychometric profiling takes this a step further by relying on 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 psychological composition. For example, users who respond that they always perform 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 recent data-driven analysis has allowed psychometric profiling to move beyond the question-and-answer format. Now, direct 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 little need to ask explicitly about whether someone likes art when a person’s liking of a Facebook page about Leonardo da Vinci is publicly observable. This not only reduces the need for cumbersome surveys, 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 main personality traits it measures: openness, conscientiousness, extraversion, agreeableness and neuroticism. Psychological research suggests that these five traits encompass a wider range of individual motivations or preferences than any other combination of traits.15 For campaigns and strategists with a political message to deliver, information about voters’ OCEAN profiles is clearly valuable, as shown 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. Michael Kosinski, a pioneer in the field of psychometric profiling and digital behaviour, was the first to show claim in 2013 that algorithmic analysis of Facebook likes could reveal personality traits.16 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).17 Most recently in 2017, they showed that ads tailored to psychological profiles in the real world are more effective than ads that are not.18 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.

Psychographic, and attitudinal’ characteristics.12

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 other countries.19 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

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.13 The data broker claims to hold data on over a billion people in Europe and the United States and earned over 4.6 billion US$ in revenue in 2018.14 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 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

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.

> If users consent to sharing their data for a given purpose in an apolitical context, transferring this data for use in political campaigns undermines the consent process.

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.

“Psychometric profiling relies on 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.”
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 profiling techniques. 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.


3. Facebook + Survey Data Collected

This schematic shows a simplified pipeline for psychometric profiling based on Facebook data, as implemented in published academic papers. In practice, information on intimate traits can be extracted from engaging, game-like online quizzes, purchased from data brokers, or inferred from digital records like Facebook ‘Like’ data.


4. OCEAN Profiles of Surveyed Users

If the mock pipeline accurately reflects the Facebook ‘Like’ data has been demographically matched to psychometric traits and psychographic orientations (e.g., openness, conscientiousness, extraversion, agreeableness, neuroticism).

5. Extrapolating Results: OCEAN Profiles of Other Users

The model suggests that people who have similar Facebook habits or data will be more likely to have similar OCEAN profiles. This can then be used to predict the profiles of other users based on their Facebook activity and loading these attributes into the psychometric profiling model.

6. Putting It All Together

Advertisements are designed for specific OCEAN profiles. They are selectively targeted to their intended audience (e.g., a video ad showing a happy, outgoing personality for people who are open and extraverted). This allows for a more personalized and effective marketing strategy.


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 individual demographics, interests, attitudes, relevant, and efficient.


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.


This screenshot taken from the website of Market Predict, a media optimization firm, shows different voter considerations under the headline, ‘we get inside the mind of the voter’.


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


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


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

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


"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
Upcoming Technologies: The next frontier in campaign technology

What technologies are on the horizon?

Political tactics have long mirrored those of the marketing industry. 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. This chapter explores several emerging technologies that use personal data and has 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. 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 analyze a user’s data to deliver customized propaganda. Bots will point people toward extremist viewpoints and counter arguments in a conversational manner.

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). Another bot called ‘Dein Spitze mit Van der Bell’ [Your Star with [their candidate and current Austrian President] Alexander Van der Bell] helped users add an image of Van der Bell to their Facebook profile pictures.

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.

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. His vision, common in the industry, is to make chatbots ‘respond like a human would’; that is, by improving their language, which he currently characterises as that of a ‘glorified marketing site’.

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 demeanor, the virtual conversation could allow voters to ask questions hyper-specific to their community, and receive targeted answers in return’.

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. If feasible, campaigns would probably use this ‘swappable identity’ capability to ‘influence opinion and generate excitement among people it views as likely supporters of their candidate’.

**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?

This technology allows political parties or candidates to tailor ads to voters for maximum impact. For example, eye-tracking technology contends that men and women look at different parts of ads. 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. Their 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.

**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 ‘consume and unconsciously consume’. 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.

**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.

In the near future, IoT smart speakers like Amazon’s Echo, Google Home, robotic vacuums, smart beds and others promise to capture even more of our rich, behavioural data.

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’.

Because many of these devices will live at home, the data we share with them will likely be more intimate than the data we share with our devices today.

Ultimately, these nascent developments are believed to spur campaigns’ efforts to target voters as precisely and accurately as possible, and at scale.

**Some examples**

**In the United States:** In November 2016, a Facebook Messenger bot created by ‘messie’ was piloted on behalf of three political groups, the Connecticut House Democratic Campaign Committee, the Pennsylvania Common Sense Political Action Committee and Baas’ Apologia, 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 took up polling places existing at the time, (messie)bot offered some advantages: a novelty factor; the convenience of a mobile-friendly experience and the opportunity to experiment.
Chatbots Magazine, an industry resource, featured an article entitled ‘Bots Are More Than “Fake News” Machines’, which featured selfies provided by the chatbot Your Selfie with Van der Bellen. These images were part of a Facebook chatbot developed at a hackathon.


A screenshot of the UK Labour Party’s chatbot, powered by the San Francisco-based company Chatfuel. Chatfuel boasts over 1 billion users with 80% message open rate across its bots on Facebook Messenger.


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 integrate this technology to direct voters’ eyes and attention as desired.


A screenshot 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 also has a section devoted to neuromarketing and how recent research has demonstrated its effectiveness in campaigning.


A screenshot from @mssg is a company that offers an online chatbot to spur voter registration and get out the vote (GOTV) efforts.

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 conversations is a novel approach, and the initial results are amazing. We can collect any and all types of data from these users—name, 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.\(^\text{32}\)

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 to find, among other things, that men spent more time looking at logos, while women fixated more on family portraits. Some

- III: Intentional political could use personal data to feed users individually tailored propaganda and promote extremist views. Bots without access to personal data have already been found to do so.\(^\text{34}\)
- 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 interests. One academic commented, the IoT is essentially a massive surveillance network.\(^\text{33,34}\)
- If technologies are increasingly merged, such as combining bots with micro-targeting, the digital literacy challenges for voters and the complexity facing regulators will increase.

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 become increasingly likely.

Considerations
1. 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.
2. Bots avoid the risk of human error in simple tasks like locking up polling locations for a given address.

"Eye-tracking services will likely grow more personal as they optimise for increasingly granular groups."
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 geo-fencing campaign rallies in the United States to a massive rebocking 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 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:

- 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.
- Independently researched, detailed information about the inner workings of the technologies is essential for decision makers, regulators, journalists and voters.

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 protection 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 to be 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.

- Data-driven political campaigning methods should not be assessed together. 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.

- Regulators need to look at technologies and their effects in a more granular way. For example, technologies like geo-fencing 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? How can we 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?

“"What we are doing is no different from what the advertising industry at large is doing across the commercial space."

ALEXANDER NIX, FORMER CEO OF CAMBRIDGE ANALYTICA\(^1\)
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 that have come to dominate the internet, such as Facebook and YouTube, were initially considered to have democratising potential. 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 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?

Technology companies have a vested interest in selling services to political parties, as a significant income generator or 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?

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 prioritization 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 policies 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 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?

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-free 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 too far from sources 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 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. 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 the system?
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 an 18-month practitioner-led research initiative conducted by the international non-profit organisation, Tactical Tech and its partners. The initiative seeks to map, document and provide a framework for understanding the use of personal data in political campaigns worldwide.