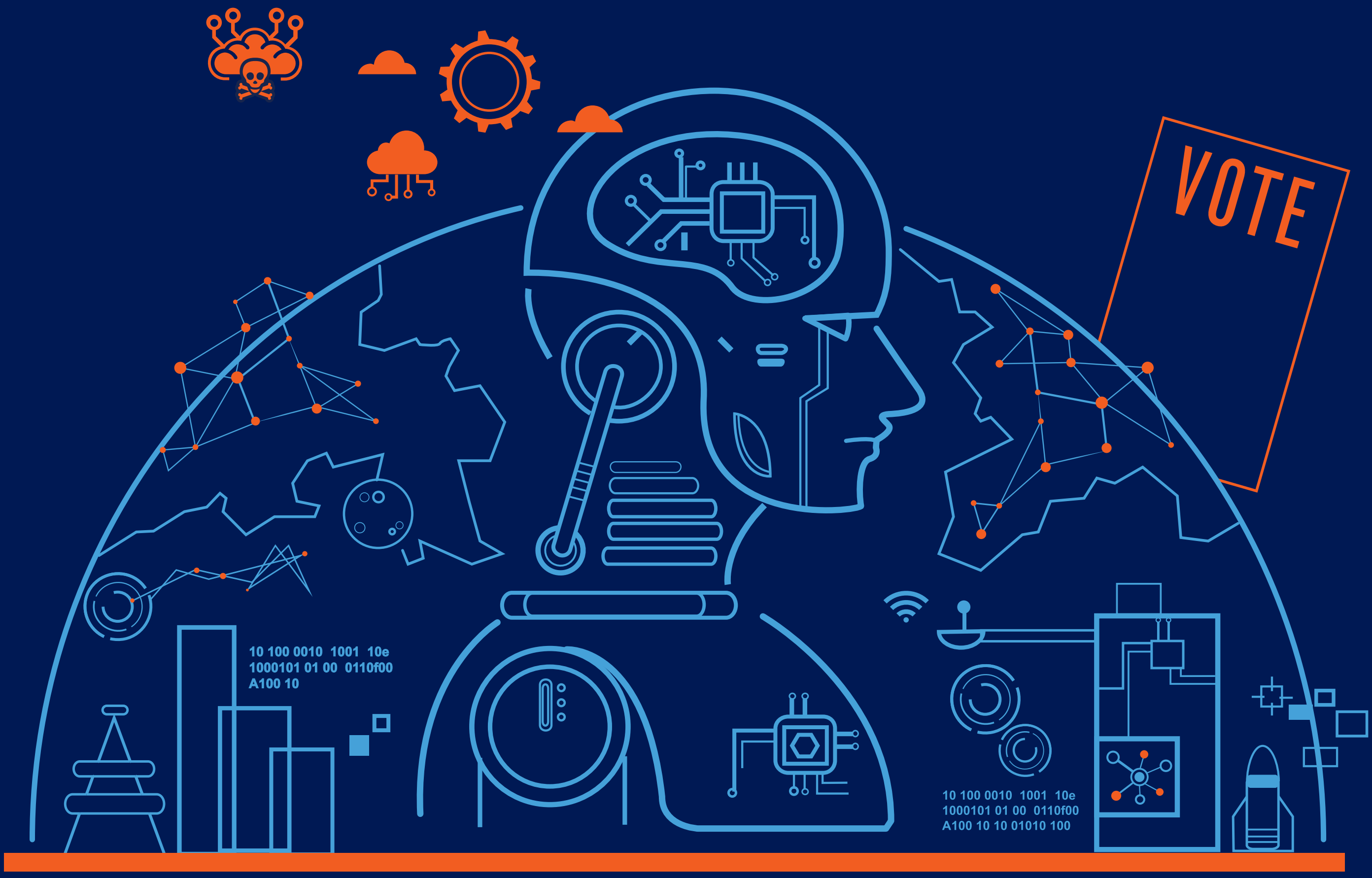
OXTEC
Oxford Technology & Elections Commission

OXFORD INTERNET INSTITUTE

UNIVERSITY OF OXFORD



READY TO VOTE:

ELECTIONS, TECHNOLOGY & POLITICAL CAMPAIGNING IN THE UNITED KINGDOM

OXFORD TECHNOLOGY & ELECTIONS COMMISSION (OxTEC)
WRITTEN & RESEARCHED BY LISA-MARIA NEUDERT & PHILIP N. HOWARD

16 OCTOBER 2019

READY TO VOTE:

ELECTIONS, TECHNOLOGY & POLITICAL CAMPAIGNING IN THE UNITED KINGDOM

OXFORD TECHNOLOGY & ELECTIONS COMMISSION (OXTEC)
WRITTEN & RESEARCHED BY LISA-MARIA NEUDERT & PHILIP N. HOWARD

16 OCTOBER 2019

OXTEC
Oxford Technology & Elections Commission

OXFORD INTERNET INSTITUTE

UNIVERSITY OF OXFORD

CONTENTS

FOREWORD

The Internet has transformed virtually every aspect of public life in contemporary democracy. Perhaps this becomes most evident during elections and political campaigning. New forms of democratic engagement, civic collective action, and public discourse thrive over online networks.

Yet in the wake of the Brexit referendum and the Cambridge Analytica case, it has become clear that the very technologies that we celebrate as a catalyst for democracy are vulnerable to abuse and deception.

Increasingly, regulators and social media companies are taking action. But dishonest campaigning practices, opaque data harvesting, obscure political advertising, and other types of interference continue to flourish.

To protect democracy and keep our elections free and fair, we need new public rules for private platforms. Making rules for the Internet is one of the most defining policy issues of our time.

The effects of the malicious use of social media are impactful and widespread but there are many things that policy-makers, industry, and civil society can do to safeguard elections and referenda in the United Kingdom.

At the beginning of 2019, we started the Oxford Technology & Elections Commission, OxTEC, to unite experts on politics, technology, security, and human rights to re-envision trusted guidelines for managing modern elections.

In the last ten months, OxTEC has produced four research reports on issues concerning the impact of technology on elections and has collected evidence from numerous expert consultations with stakeholders from policy, law, industry, academic research, and non-governmental and watchdog organizations.

In this report, we present recommendations to integrate democratic norms and practices into the use of information technologies, social media, and big data in political campaigns. We are committed to protecting the integrity of elections in ways that harness the opportunities that digital technology provides for democracy and that underscore civic freedoms.

Because technology has become deeply entrenched in political life, we need rules for it that go beyond protecting democracy by utilizing these very technologies to strengthen it.

Philip N. Howard

Commissioner, Oxford Technology & Elections Commission and Director of the Oxford Internet Institute, University of Oxford.

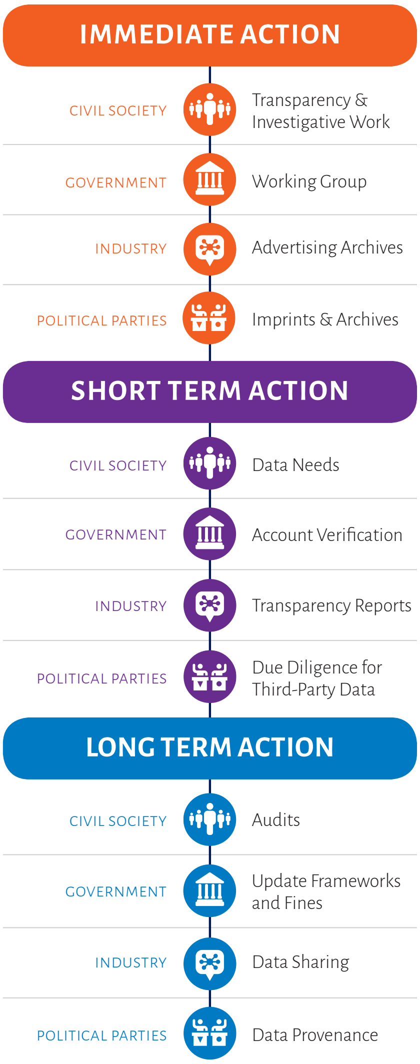
EXECUTIVE SUMMARY

Contemporary political life has become deeply interwoven with networked technologies. Although digital technology was once heralded as a boon for democracy, policy-makers around the globe are growing increasingly concerned about the impact that technology, and specifically social media, is having on democracy.

With accumulating evidence of foreign meddling in the elections and referenda of major democracies, growing concerns about disinformation, non-transparent campaigning practices, the use of data-driven profiling to subvert democratic processes, and opaque data brokers like Cambridge Analytica, there is a pressing need for new rules for the democratic use of digital technologies in the United Kingdom.

In this report, we develop recommendations tasked to counter complex issues concerning the impact of technology political campaigning and democracy in relation to the algorithmic spread of nefarious content, non-transparent political advertising, obscure campaign reporting and opaque data-driven campaigning. Our recommendations address systemic problems and intend to update successful regulatory frameworks designed for a digital age while protecting civic freedoms and utilizing digital technologies for democracy. We draw from evidence collected by the Oxford Technology & Elections Commission, OxTEC, between January and October 2019. This evidence includes four designated research reports; twelve expert briefings with stakeholders from policy, law, industry, academic research, and non-governmental and watchdog organizations; and numerous round-table discussions with these stakeholders.

Several different kinds of stakeholders will need to act in coordinated ways to address – and redress – the problems that concern the use of technology in public life. We identify four key stakeholder groups: (1) *civil society*, which includes stakeholders in journalism, research, and various civic organisations, charities and interest groups; (2) *government*, which includes the various branches of government and regulatory offices; (3) *industry*, which includes social media companies, technology platforms, and various data analytics companies; and (4) *political parties*, which includes their candidates, campaign staff, and registered campaigners. To organize the policy ideas that OxTEC recommends, we group our recommendations in the following order: the things that should be done immediately, the tasks that need to be done in the short term, and the long-term goals for how we manage elections.


IMMEDIATE ACTION

CIVIL SOCIETY – Transparency & Investigative Work

GOVERNMENT – Working Group

INDUSTRY – Advertising Archives

POLITICAL PARTIES – Imprints & Archives

SHORT TERM ACTION

CIVIL SOCIETY – Data Needs

GOVERNMENT – Account Verification

INDUSTRY – Transparency Reports

POLITICAL PARTIES – Due Diligence for Third-Party Data

LONG TERM ACTION

CIVIL SOCIETY – Audits

GOVERNMENT – Update Frameworks and Fines

INDUSTRY – Data Sharing

POLITICAL PARTIES – Data Provenance

IMMEDIATE ACTION

CIVIL SOCIETY: Civil society should use advertising archives and available social media data for investigative work and to achieve meaningful transparency.

GOVERNMENT: The UK government should form a working group of relevant stakeholders from major public agencies with a regulatory role in keeping elections free and fair, to support information sharing and exchange.

INDUSTRY: Social media platforms should create full advertising archives to make available helpful and accurate information about all sponsored content at all times. The data should be relevant for statistical analysis, freely accessible to any citizen, searchable, and machine-readable.

POLITICAL PARTIES: Political parties in the United Kingdom should provide imprints about the campaigner and sponsorship of all digital ads and other forms of sponsored content and should archive all sponsored messages they run in accessible online databases.

SHORT-TERM ACTION

CIVIL SOCIETY: Civil society should identify the types of data that social networks must supply to confirm that they work in a transparent way and to ensure that the data can be used for research.

GOVERNMENT: The UK Electoral Commission (UKEC) should verify the social media accounts of all registered campaigners.

INDUSTRY: Social media platforms should submit detailed reports and supporting data about content moderation and takedowns on their platforms specifically for the United Kingdom.

POLITICAL PARTIES: Political parties should develop a code of practice for the use of third-party data and analytics software and for ensuring due diligence when obtaining third-party data.

LONG-TERM ACTION

CIVIL SOCIETY: Independent stakeholders from civil society should conduct audits of social media companies and their technologies and practices that reflect the expectations of election administrators and regulators.

GOVERNMENT: Existing regulatory frameworks for spending reporting and invoice reporting and the fines they can impose need to be updated to fit the digital context of modern campaigns.

INDUSTRY: Social media companies should be required to share data about public activities on their platforms in machine-readable formats in real time for independent research. Where there is evidence of interference in elections, platforms must alert the relevant government agencies immediately and share data.

POLITICAL PARTIES: Political parties should provide information about the data they use for campaigning and democratic engagement, including the sources of data, the types of data, and the in-house and external software used to process data.

1 INTRODUCTION

Digital technologies have long been celebrated as beacons of democracy. The Internet, and specifically social media, has transformed virtually every aspect of modern citizenship.

From increasingly digital economies to the instantaneous access to vast amounts of information, to networked communication with peers, to collective action on petition platforms, to political campaigning during elections, digital technologies are deeply intertwined with public life. Platforms like Facebook, Instagram, Twitter, WhatsApp, and TikTok support new forms of political participation and civic discourse. In the United Kingdom, policy-makers have widely embraced the opportunities that digital provides for democratic engagement and electioneering. Parties and candidates maintain an online presence and targeted online ads have become an indispensable tool in any campaign's electoral kit, with strategies becoming more sophisticated in every election cycle. However, the contemporary political reality has underscored the ways in which technology can undermine the integrity of elections and political processes.

Social media platforms and digital technologies have been at the centre of regulatory interest in the United Kingdom for quite some time (Robinson, Coleman, & Sardarizadeh, 2019). Key issues around human rights, cybersecurity, e-commerce, Internet access, tech monopolies, surveillance and law enforcement, and intellectual property rights have been some of the traditional areas for regulatory attention. In the aftermath of the Brexit referendum and the case of Cambridge Analytica – the British consulting firm that illegally mined personal user data from millions of Facebook users and used it for deceptive political marketing – concerns about interference in democratic processes and the role of technology in public life emerged prominently on the political agenda.

With accumulating evidence around foreign meddling in the elections of major democracies, growing concerns about disinformation, non-transparent campaigning practices, and the use of data-driven profiling to subvert democratic processes, questions surrounding the role of technology for democracy pose an ongoing challenge for society (Thwaite, 2019). Increasingly, policy-makers and platform operators are taking action but measures frequently fall short of achieving real change and addressing systemic flaws (Bradshaw, Neudert, & Howard, 2018; Hoffmann, Taylor, & Bradshaw, 2019). Elections and referenda are among the most important exercises of democratic life. To harness digital technology as a force for democracy, we need guidelines – including legislative change where necessary – to ensure its fair and free use. In order to be effective and future-proof, these guidelines must tackle systemic maladies rather than symptomatic issues and update analogue frameworks for a digital age.

In this report, we develop recommendations for the democratic use of technology in elections and political campaigning. We make recommendations for immediate, short-term and long-term action that address four key stakeholder groups: (1) *civil society*, which includes stakeholders in journalism, research, and various civic organizations and civil rights groups; (2) *government*, which includes the various branches of government and regulatory offices; (3) *industry*, which includes social media companies, technology platforms, and various data analytics companies; and (4) *political parties*, which includes their candidates, campaign staff, and all registered campaigners. Our recommendations target three phases of modern electioneering: the preparation stage between major elections when political data is gathered and strategies are tested; the campaign period, when administrative responses need to be agile; and the post hoc analysis stage, which involves evaluating behaviour and sanctioning political actors who have behaved illegally.

The recommendations presented are drawn from evidence collected by the Oxford Technology & Elections Commission, OxTEC, between January and October 2019. This evidence includes four designated research reports; twelve expert briefings with stakeholders from policy, law, industry, academic research, and non-governmental and watchdog organizations; and numerous round-table discussions with these stakeholder groups.

2 TECHNOLOGY AS A POLICY ISSUE

Issues surrounding the use of technology during elections, political campaigns, and day-to-day public life are complex and multifaceted.

Computational propaganda is the malicious use of automation, algorithms, and big-data analytics tasked with manipulating public life (Woolley & Howard, 2016). However, there are also issues that are inherently connected to the use of modern technology and the ways it has become embedded in everyday civic life. Policy issues that concern the democratic use of modern technology span a variety of issues related to the digital public sphere, including the spread of junk news and disinformation, illegal data harvesting and micro-profiling, deceptive advertising practices and insufficient consent, the exploitation of social media platforms for influence operations, the amplification of political lies through fake accounts and bots, questions to do with algorithmic black boxes, and regulatory frameworks that have become ill-equipped to enforce good behaviour and transparency. We outline four key challenges affecting elections and democracy in the United Kingdom that stakeholders in policy, industry, and civil society must address.

Algorithmic Spread of Nefarious Content

There has long been a tension between allowing free speech to flourish and limiting the spread of nefarious forms of online content, such as that involving child abuse and terrorism, but also hate speech and political falsehoods. As clickbait, conspiracy theories, and junk news continue to thrive on social media algorithms, questions about how to curb their spread without stifling freedom of expression are pressing (Vicario et al., 2016; Vosoughi, Roy, & Aral, 2018). Various forms of content restrictions and media literacy campaigns were key elements of regulatory frameworks introduced for print and broadcasting in many countries. Yet these measures have proven mostly ill-equipped to address deeper issues rooted in the very design and size of technology platforms. Social media companies have established rules for content regulation on proprietary platforms that rely on human and automated moderation. However, these procedures remain non-transparent and thus elude scrutiny (Gillespie, 2018). New guidelines are needed, but to develop effective countermeasures, policy-makers require information about the proliferation of various forms of nefarious content online – both organic and automated – the mechanisms of the platform algorithms that spread it, and economic incentive structures that reward virality over veracity.

Non-Transparent Political Advertising

Digital advertising has emerged as a key element of modern-day political campaigning. Increasingly, political actors in the United Kingdom rely on social media ads and other forms of sponsored content on platforms like Facebook, Instagram, Snapchat, and YouTube to target citizens with political messages (Hankey, Morrison, & Naik, 2018). But digital advertising differs from other popular forms of political advertising, such as print or broadcast ads, in important ways. Regulation about imprints for campaign material does not extend to online ads (The Electoral Commission, 2018). Advertisers can therefore obscure their identity for political purposes. Online, advertising is data-driven and frequently targeted at small groups in the population. The effect of such micro-targeting is that we are no longer able to see what is going on 'next door', which in turn creates advertising echo chambers. This becomes especially problematic when these techniques are used to discriminate or to send conflicting messages to different audiences (Angwin & Parris Jr., 2016). Transparent political advertising makes accessible information about sponsorship and campaign messages.

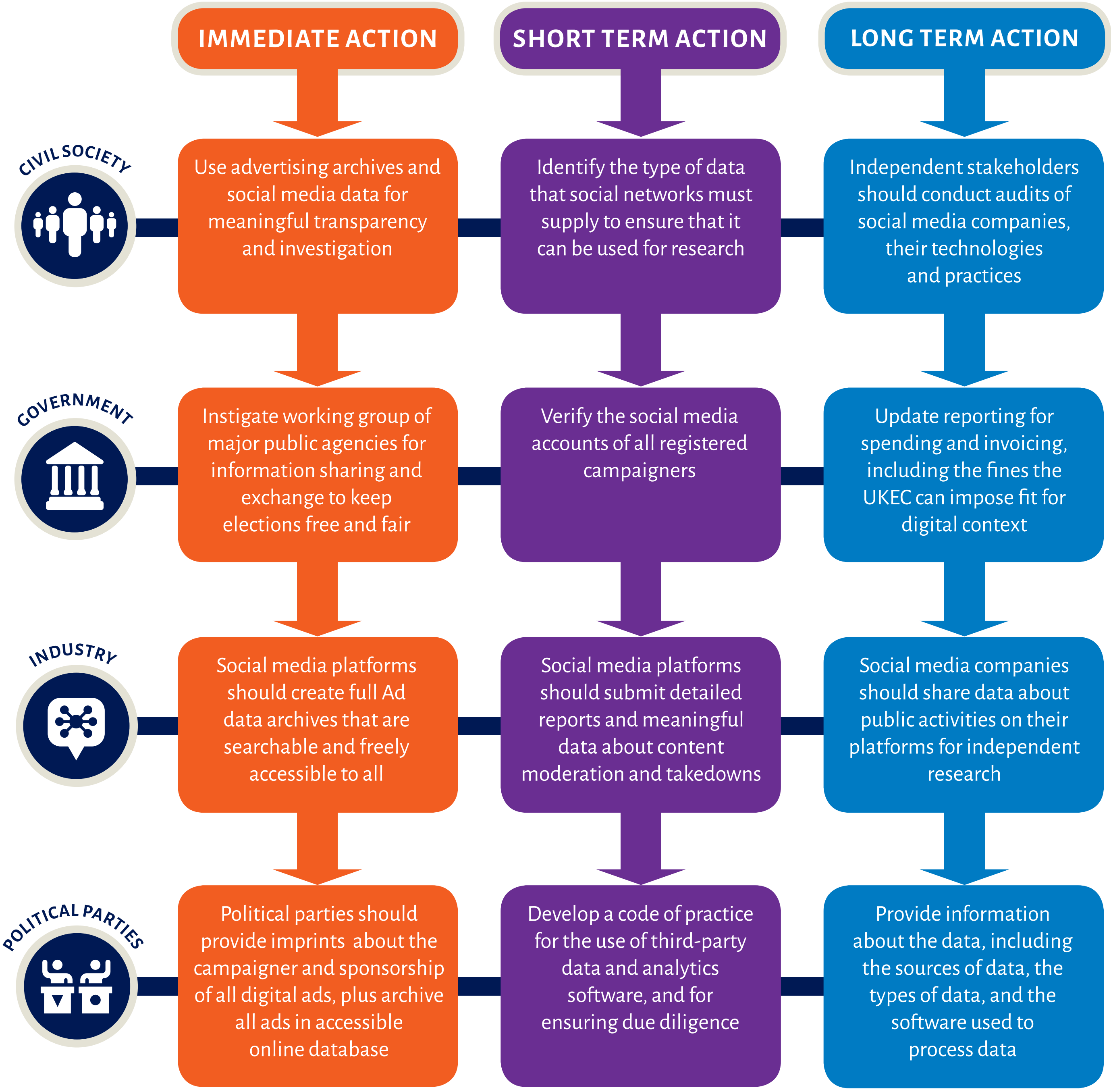
Obscurity of Campaign Reporting

Digital advertising and content marketing have proliferated into a multi-billion-dollar industry (Hoffmann et al., 2019). Increasingly, political campaigners spend their budget on digital services and technology, including social media ads, voter files offered by data brokers, and analytics tools for profiling. While digital strategies have become a cornerstone of political campaigns, now-obsolete reporting obligations that were developed for analogue campaigns combined with non-transparent data processing and advertising practices have obscured electioneering. Democratic public life demands that voters have access to meaningful information about campaign spending and donations and disclosure about who is behind the sponsored messages they are targeted with.

Opaqueness of Data-Driven Campaigning

In a digital age, big data has become ubiquitous. It includes personal data on voters, their demographic background, their political opinions, and their wants and needs. In public life, data can be leveraged for democratic engagement, for mobilizing voters, and for connecting citizens to information that is relevant to them (Kreiss, 2016; Shorey & Howard, 2016). Data analytics tools, profiling software, and customer relationship management applications employ powerful algorithms to process data in ways that can accurately infer deeply personal information about voters. As third-party data brokerage flourishes, tech platforms thrive on data-driven ad auctioning for targeted messages, and political parties employ A/B testing to optimize their campaigns, but pressing issues surrounding privacy, transparency, and human rights persist that reach beyond current regulatory frameworks. Commonly, advertisers use and combine numerous data sets, including special category data and inferred forms of political data. Although user consent is required to process data, it remains questionable whether users understand how their data is used. Personal data must be processed lawfully and in a fair and transparent manner that requires individuals to provide meaningful consent.

3 ACTION SUMMARY



	IMMEDIATE ACTION	SHORT TERM ACTION	LONG TERM ACTION
CIVIL SOCIETY	Use advertising archives and social media data for meaningful transparency and investigation	Identify the type of data that social networks must supply to ensure that it can be used for research	Independent stakeholders should conduct audits of social media companies, their technologies and practices
GOVERNMENT	Instigate working group of major public agencies for information sharing and exchange to keep elections free and fair	Verify the social media accounts of all registered campaigners	Update reporting for spending and invoicing, including the fines the UKEC can impose fit for digital context
INDUSTRY	Social media platforms should create full Ad data archives that are searchable and freely accessible to all	Social media platforms should submit detailed reports and meaningful data about content moderation and takedowns	Social media companies should share data about public activities on their platforms for independent research
POLITICAL PARTIES	Political parties should provide imprints about the campaigner and sponsorship of all digital ads, plus archive all ads in accessible online database	Develop a code of practice for the use of third-party data and analytics software, and for ensuring due diligence	Provide information about the data, including the sources of data, the types of data, and the software used to process data

4 IMMEDIATE ACTION

There is a range of policy actions that are immediately available to key stakeholder groups concerned with elections and technology. These are actions that should be taken before an election even if the next election is only a few months away.

CIVIL SOCIETY: Civil society should use advertising archives and available social media data for investigative work and to achieve meaningful transparency.

Civic groups and watchdog organizations, journalists, and independent researchers should develop capacities to collect and analyse social media data that is available through advertising archives and Application Programming Interfaces (APIs) to achieve meaningful transparency and for investigative work about the use of online networks for political purposes. They should take advantage of the reporting tools and engagement opportunities offered by government and industry to help flag disinformation, evidence of malicious automation, dishonest campaigning practices, and security and data breaches that may be affecting elections.

GOVERNMENT: The UK government should form a working group of relevant stakeholders from major public agencies with a regulatory role in keeping elections free and fair, to support information sharing and exchange.

The Advertising Standards Authority, the Cabinet Office, the Electoral Commission, the Information Commissioner's Office (ICO), and Ofcom should form a working group to exchange information, share expertise, coordinate, and agree on mutual policy objectives. The working group should involve an inclusive range of agencies and involve agency leadership and boards. The working group should hold formally scheduled quarterly group phone calls or face-to-face meetings. In the lead-up to an election, that might reasonably be monthly or even weekly calls. On an informal level, exchanges among agencies already occur, but they are infrequent and rarely result in lasting cooperation. Regular meetings of various agencies would reinforce the processes of knowledge transfer, information sharing, and the exchange of expertise and would be bound by clear guidelines and policies for inter-agency collaboration.

INDUSTRY: Social media platforms should create full advertising archives to make available helpful and accurate information about all sponsored content at all times. The data should be relevant for statistical analysis, freely accessible to any citizen, searchable, and machine-readable.

Several social media companies in the United Kingdom release data about political advertising on their platforms on a voluntary basis. But the data is usually rendered useless for statistical analysis because of inconsistent or incomplete metrics that make it impossible to compare and understand trends (Mozilla, 2019). Relevant information about how advertisers have targeted their ads and the audiences that see an ad is widely excluded. Many archives only provide data about political ads when the definition of what constitutes such content lies with the social media companies. All ads, at all times, need to be available in public archives. Meaningful data about audience demographics, targeting, pricing, reach, and interactions needs to be disclosed in searchable and machine-readable databases. Where relevant, social media companies should disclose whether an advert or a version of it was tested (e.g., A/B testing) and whether the advert uses automated content optimization.

POLITICAL PARTIES: Political parties in the United Kingdom should provide imprints about the campaigner and sponsorship of all digital ads and other forms of sponsored content and should archive all sponsored messages they run in accessible online databases.

Political parties, candidates and all registered campaigners must provide information about the registered campaigner behind all forms of sponsored digital content, including ads and campaign material, and embed funding disclosure information in the design. Providing information about campaigners and sponsors ensures that voters and the UKEC can comprehend who is behind sponsored content. This is especially relevant since digital ads can appear to come from individuals expressing a personal opinion rather than making transparent their relationship with campaigns. Furthermore, archiving political ads should be considered a normal part of campaign reporting. At the moment, each of the major political parties archives campaign documents, records, and ephemera at major public libraries. But parties should not assume that the archives provided by profit-driven firms are sufficient disclosure of campaign activities. They must also develop their systems to archive sponsored content run on platforms.

5 SHORT-TERM ACTION

Whether or not there is a national election in our immediate future, there are a number of changes in public policy that could be made in the short term before London has its mayoral race in 2020 and the next mandatory general election happens in 2022.

CIVIL SOCIETY: Civil society should identify the types of data that social networks must supply to confirm that they work in a transparent way and to ensure that the data can be used for research.

Social media companies have pledged their willingness to share data and improve their platforms to protect democracy and promote the public good – but they have called on regulators to develop rules for the Internet (Pasquale, 2018). In order to develop good rules that provide effective solutions to relevant problems, we must first obtain information about activities on social networks and about fundamental technological mechanisms. This data is absolutely pivotal to identify with certainty systemic harms and the patterns and causes of problematic uses and applications of social networks. Civil society stakeholders should advise on the data requirements needed to identify systemic harms and the patterns and causes of problematic uses of social networks in the domain of their expertise. This should include concrete recommendations on what action to take regarding gaps in current data-sharing programs and on the data formats required to allow meaningful analysis of the data. Data sharing must be lawful and protect user privacy.

GOVERNMENT: The UKEC should verify the social media accounts of all registered campaigners.

The UKEC should create a database of the verified social media accounts of all registered campaigners in the United Kingdom, which should encompass political parties, recognised third-parties, and candidates, including those running in local council elections and mayoral races. This should apply to all social networks with a substantial user base in the United Kingdom. This measure would increase transparency of campaigning materials, support independent fact-checking, and ensure that sources of political information are credible. The UKEC already maintains a register of registered campaigners, including political parties and recognised third-parties. Official social media accounts should be considered to be all those that are managed by a party, a candidate, a recognised third-party campaigner, their staff, or a third-party acting on their behalf.

INDUSTRY: Social media platforms should submit detailed reports and supporting data about content moderation and takedowns on their platforms specifically for the United Kingdom.

Social media companies should share evidence about content moderation and takedowns on their platforms in a publicly accessible transparency report for the United Kingdom. These reports should include statistics about the nature of material (e.g., terroristic content, child abuse material, forms of illegal speech) that was deleted or restricted in terms of visibility, as well as statistics about fake accounts, account suspensions, and de-platforming. The reports must also state the reasons for taking action, which are usually violations either of existing law or of the terms of service of platforms. The reports should be published regularly and at the very least bi-annually; during active campaigning they should be supplied on a monthly basis. They must specifically refer to activity in the United Kingdom.

POLITICAL PARTIES: Political parties should develop a code of practice for the use of third-party data and analytics software and for ensuring due diligence when obtaining third-party data.

The General Data Protection Regulation (GDPR), the Data Protection Act (DPA), and the Privacy and Electronic Communications Regulations (PECR) provide detailed frameworks for the use of data for political campaigning in the United Kingdom. Parties and political campaigners are required to comply with these frameworks and must be able to demonstrate compliance and be accountable. When obtaining data from third-party organizations, such as data brokers, parties are required to carry out due diligence. They need to ensure that data has been collected lawfully and that appropriate consent was sought from individuals. In practice, due diligence processes for obtaining and processing third-party data lack a common framework for determining whether data collection and processing are compliant with the law. Political parties should develop a code of practice for due diligence when obtaining and processing third-party data and when using third-party data analytics software that frequently combines different types of data and draws inferences about individuals from data.

6 LONG-TERM ACTION

There are a number of measures that will require substantial planning or changes to existing law. The proposed changes are relevant to elections and year-round political campaigning and should be implemented as soon as possible.

CIVIL SOCIETY: Independent stakeholders from civil society should conduct audits of social media companies and their technologies and practices that reflect the expectations of election administrators and regulators.

Civil society should develop capacities for auditing social media companies and their technology and practices in relation to political campaigning and elections. The role of social networks and their staff regarding consulting with campaign staff and providing advice on campaign material and advertising, as well as the management of public pages of political actors, lacks transparency and oversight (Kreiss & McGregor, 2018). Similarly, technical tools for content optimization, including automated ones, and testing and analytics features that are provided for important accounts remain widely unexplored. Civil society should serve as an independent auditor that makes the practices of collaboration and consultation between tech platforms and political campaigners transparent, helps understand technological features and their relevance for campaigning, and develops best practices and codes of practice.

GOVERNMENT: Existing regulatory frameworks for spending reporting and invoice reporting and the fines the UKEC can impose need to be updated to fit the digital context of modern campaigns.

Existing regulatory frameworks for campaign reporting and their fines need to be revised to fit digital contexts and empower the UKEC. Currently, spending on campaign activities is reported in very broad categories (The Electoral Commission, 2018). The spending categories should be revised to reflect different types of political advertising and campaigners should be required to disclose what advertising suppliers they place their ad with (e.g., Google AdSense, Facebook Ads Manager). This should also be required for budgets spent via media buying agencies. Currently, campaigners need to provide invoices for spending over £200. Invoicing limits should be lowered to reflect the low cost of targeted advertising campaigns. Invoices should also reveal information about the ads that were placed, including their content and area of distribution. Moreover, the maximum fines of the UKEC should be increased to a percentage of total campaign budget or a fixed sum, whichever is higher, to effectively punish non-compliance with the law.

INDUSTRY: Social media companies should be required to share data about public activities on their platforms in machine-readable formats in real time for independent research. Where there is evidence of interference in elections, platforms must alert the relevant government agencies immediately and share data.

In the aftermath of prominent cases of abuse of personal user data for political purposes in the United Kingdom, leading social media platforms have heavily restricted access to public data on their platforms. While private and personal information must be protected, publicly distributed information about consenting users needs to be accessible for independent research and review. Social media platforms in the United Kingdom need to share machine-readable data for scholarly and public enquiry. Despite the monitoring efforts of social media companies, on numerous occasions it has been independent researchers and security experts who have first detected foreign interference and meddling in elections. Social networks should report information about reach and other engagement metrics (e.g., shares, retweets, follows), the history of accounts, and whether a post was generated automatically. Where there is evidence about interference in elections and public life, platforms must be required to report this to the government and share relevant data.

POLITICAL PARTIES: Political parties should provide information about the data they use for political campaigning and democratic engagement, including the sources of data, the types of data, and the in-house and external software used to process data.

As an extension to their financial reporting on advertising expenses, political parties should reveal information about the data they use for political campaigning and democratic engagement both during and outside election cycles. Parties should be required to report clear information about the sources of the data they acquire and use to make transparent the full provenance of that data. This should include data from the electoral register, third-parties, and data brokers, open data, and their own sources of data. In particular, parties should disclose how they collect and use personal data and special category data. Furthermore, they should disclose what tools they use to process data. This should extend to customer relationship management software, data analytics software, profiling tools, and ads managers. Providing detailed information about the origins of data and about the practices relating to collecting and using data will increase transparency, advance the creation of accountable codes of practice, and aid inquiries into the possible unlawful use of data.

7 CONCLUSION

While calls to regulate online harms on digital platforms remain vocal, effective policy making must protect civic freedoms and underscore democratic expression rather than stifle it. Our goal has been to identify the immediate, short-term, and long-term rule changes needed to keep our elections safe, free, and fair and to revise regulatory frameworks and guidelines in ways that strengthen citizenship in contemporary democracies.

We have developed a set of twelve comprehensive recommendations that engage stakeholders in civil society, the tech industry, government, and political parties and that pinpoint what needs changing.

Political parties, foreign governments, and industry lobbyists make use of the very same digital strategies and data-mining services but with starkly diverging consequences for democracy. To advise on rules for their use that underscore democracy rather than subvert it, we need new guidelines, some of which this report recommends. Our recommendations highlight only a few important areas for concrete policy action. Yet looking beyond that, our report highlights the need for continuous dialogue between policy-makers and platforms to make transparent the technological underpinnings of social networks and how they are used in modern public life. Policies that are fit for purpose must stem from a meaningful understanding of the issues surrounding elections and technology.

Elections are among the most important exercises of democracy but protecting them is not the only way to keep our institutions resilient. Having public resources for teaching citizens about the risks and rewards of using social media for political conversation, for empowering citizens to use technology for political participation, and for high-quality public news reporting will all have positive effects. And while most of our recommendations concern the stakeholders that are perhaps most directly involved in modern electioneering, there is a host of other public agencies that need to develop their own specialized capacity to handle election-related issues in their own domain. As political life has become deeply intertwined with digital networks, it is the responsibility of the public sphere as a whole to deliberate on how to utilize technologies in ways that strengthen democracy rather than undermine it.

The work of protecting our ability to discuss public policy options, evaluate good ideas, and champion political causes is essential to healthy public spheres. Protecting democratic norms should be an obligation for technology firms that have had the freedom to flourish in open societies, and taking care of democratic institutions is clearly a way to sustain their long-term business models. In the long run, technology companies will likely develop alternative revenue models that reward civic engagement rather than short-term attention. Until then, it is not just social media platforms that need better rules for the democratic use of the Internet. Several important aspects of the current regulatory frameworks for political campaigning are no longer fit for purpose in a digital age. Shortcomings of policies on the use of data and digital electioneering allow for dishonest campaign practices to thrive, often legally so. Watchdog organizations and civil rights groups need to make these practices transparent and provide the necessary access to data. To protect democracy in the United Kingdom, regulators, industry, and civil society must act in coordination to develop rules for the democratic use of technology.

ACKNOWLEDGEMENTS

The Oxford Technology and Elections Commission gratefully acknowledges the support of the European Research Council for the research project, 'Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe,' Proposal 648311, 2015-2020, Philip N. Howard, Principal Investigator. Additional support for this study has been provided by Microsoft, Luminate and the Adessium Foundation. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders, the Oxford Internet Institute, or Oxford University. For their assistance and advice on this research we are grateful to Victoria Nash, Rasmus Kleis Nielsen and Joss Wright in their role as Technical Advisors to the Oxford Technology and Elections Commission. We are also very grateful to Samantha Bradshaw, Alistair Coleman, Stacie Hoffmann, Ravi Naik, Olga Robinson, Shayan Sardarizadeh, Emily Taylor and Alice Thwaite for the insightful research they have conducted. Furthermore, we would like to thank John Francis, John Gilbert, Mark Healy, Mark Malbas, Isabelle Malcom, Charles Phillips, Duncan Passey, Sara Spinks and Beverly Sykes for their support and assistance to OxTEC.

REFERENCES

Angwin, J., & Parris Jr., T. (2016, October 28). *Facebook Lets Advertisers Exclude Users by Race*. Retrieved from ProPublica website: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

Bradshaw, S., Neudert, L.-M., & Howard, P. N. (2018). *Government Responses to Malicious Use of Social Media* (Working Paper No. 2018.2; p. 19). Retrieved from NATO StratCom Centre of Excellence website: https://www.stratcomcoe.org/government-responses-malicious-use-social-media

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press.

Hankey, S., Morrison, J. K., & Naik, R. (2018). *Data and Democracy in the Digital Age*. Retrieved from: https://consoc.org.uk/publications/data-and-democracy-in-the-digital-age/

Hoffmann, S., Taylor, E., & Bradshaw, S. (2019). *The Market of Disinformation* (No. 4). Retrieved from:https://oxtec.oii.ox.ac.uk/publication/the-market-of-disinformation/

Kreiss, D. (2016). *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*. New York, NY: Oxford University Press.

Kreiss, D., & McGregor, S. C. (2018). Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle. *Political Communication*, 35(2), 155–177.

Mozilla. (2019). Open Letter: Facebook, Do Your Part Against Disinformation. Retrieved from: https://blog.mozilla.org/blog/2019/02/11/open-letter-facebook-do-your-part-against-disinformation

Pasquale, F. A. (2018). *Tech Platforms and the Knowledge Problem* (SSRN Scholarly Paper No. ID 3197292). Retrieved from: https://papers.ssrn.com/abstract=3197292

Robinson, O., Coleman, A., & Sardarizadeh, S. (2019). *A Report on Anti-Disinformation Initiatives* (No. 1). Retrieved from: https://oxtec.oii.ox.ac.uk/publication/bbc-monitoring-report/

Shorey, S., & Howard, P. N. (2016). Automation, Big Data and Politics: A Research Review. *International Journal of Communication*, 10 (Special Issue), 20.

The Electoral Commission. (2018). *Digital Campaigning—Increasing Transparency for Voters*. London, UK: The UK Electoral Commission.

Thwaite, A. (2019). *Literature Review on Elections, Political Campaigning and Democracy* (No. 2). Retrieved from: https://oxtec.oii.ox.ac.uk/publication/litreview/

Vicario, M. D., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Quattrociocchi, W. (2016). The Spreading of Misinformation Online. *Proceedings of the National Academy of Sciences*, 113(3), 554–559.

Vosoughi, S., Roy, D., & Aral, S. (2018). The Spread of True and False News Online. *Science*, 359(6380), 1146–1151.

Woolley, S. C., & Howard, P. N. (2016). Political Communication, Computational Propaganda, and Autonomous Agents–Introduction. *International Journal of Communication*, 10(0), 9. Retrieved from: http://ijoc.org/index.php/ijoc/article/view/6298

OXTEC
Oxford Technology & Elections Commission

OXFORD INTERNET INSTITUTE

UNIVERSITY OF OXFORD

OXTEC.OII.OX.AC.UK

Cite this report as: Oxford Technology & Elections Commission written & researched by Lisa-Maria Neudert & Philip N. Howard (2019). *Ready to Vote: Elections, Technology & Political Campaigning in the United Kingdom.* (16 p.) Oxford, UK: Oxford Technology & Elections Commission. Retrieved from: https://oxtec.oii.ox.ac.uk/publication/ready-to-vote/