



THE
WILBERFORCE
SOCIETY



Privacy and Politics in the Age of Technology

Writers: Sophie Ashford, Daniel Gayne, Connor MacDonald, Joshua Watts

Abstract

This paper discusses the challenges associated with data use in both political and commercial contexts. In particular, we discuss how organizations and corporations (particularly political parties and telecommunications firms), have used data in recent controversies and elections. In addition, we consider the legal regimes governing data arrangements and usage in a number of jurisdictions, notably Canada, the United Kingdom, Australia and the United States. In particular, we note that legal regimes have not kept pace with data usage, particularly in the political sphere. In some cases, notably Australia, this takes the form of under-regulation. In other cases, including both Canada and the United Kingdom, this involves improper regulation or regulation not fit for the purposes of electioneering, with the result that political parties are unnecessarily impeded while electors are not properly protected. In terms of commercial settings, the paper highlights that current regulation disempowers consumers and provides companies with ample opportunity for abuse. In Part 1, the paper details policy proposals to improve political data usage regulations. In part 2, policy proposals are put forward to empower consumers and protect privacy, with a particular emphasis on privacy agreements and customer-corporate relations.

Acknowledgement

This paper is made possible through the support of Mr. Brendan Tan,
TWS Director of Publishing.



Table of Contents

Acknowledgement 3
Introduction 5
Thinking about data privacy: Nissenbaum’s contextual integrity 6
Part One: Technology, Privacy, and Politics 6
Case Study: Canadian Election 2015 7
Case Study: United Kingdom 10
Policy proposals 17
Part Two: Privacy and Technology in a Commercial Setting 19
State agencies and illegal hackers: rendering norms of information flow obsolete? 20
Everyday erosion of information flow norms: the perceptions gap 21
Policy proposals 25
Conclusions 26
Appendix 1 – Example use of data – Constituency in New Brunswick, Canada 28
Appendix 2 – Graphic Representation of Appendix 1 30
Bibliography 31

Introduction

This paper will examine the collection, storage and use of data by political and commercial organizations, with a view to improving the quality of citizen and consumer privacy. We develop a critical understanding of privacy as based on a degree of agency over the use of one's data, and, most importantly, the ability to make informed choices about what information it is suitable to disclose. We feel that these issues are particularly pertinent for young people, as our generation will be the first to live their entire lives in both the material and digital worlds. Whilst concerns about privacy infringement by the state and other organizations have been long running, and are often linked to new technologies, from early photography¹ to CCTV, the scale of data disclosure brought about by digital technology is unprecedented, but risks being normalized for a generation who have grown up 'online'.

Privacy is a vexing issue, a single value or right stretched across the full spectrum of public life is likely to become diffuse. We reflect this by structuring this paper in two parts. The first will consider privacy in an explicitly political sphere, the purest form of which is represented in liberal democracies by the institution of the political party. The second section examines the privacy of citizens in their capacity as consumers and customers of commercial organizations.

In both spheres it is apparent that the use of data is far more complex than a simple opposition between organizations and the individual's whose data they hold. Political and commercial organizations have yet to fully adapt to the possibilities of the digital age, and, as our case studies demonstrate, have done so to varying degrees. In our eyes, this represents an opportunity for dialogue and reflection on the appropriateness of data collection, which may yet result in an appropriate balance between privacy, technology, and the state.

¹ *Warren and Brandeis, (1890) The Right to Privacy, Harvard Law Review Vol.5*

Thinking about data privacy: Nissenbaum's contextual integrity

In thinking about issues of Privacy in relation to political and non-political self-expression it is useful to establish a theoretical basis. Such a framework can be usefully provided by Nissenbaum's conceptualization of privacy as conditional on two competing norms. A 'norm of appropriateness' is breached when information is disclosed of a nature which would not be considered appropriate given the relation between the discloser and the person with whom the information is shared. Additionally, a 'norm of information flow' is breached when the disclosure of information results in it spreading in ways that the discloser had not or could not have anticipated. Essentially, "personal information revealed in a particular context is always tagged with that context and never "up for grabs".² Both of these norms can be considered under threat as technology, and the actions of the state, undermine privacy, and it is with reference to these that we now proceed. We thus understand privacy through the lens of agency: policy proposals will be made which, we feel, would increase the ability of users to make informed decisions about what information to put online, by identifying how the current handling of sensitive digital information undermines the agency of those users who generate it, and how this could be redressed.

Part One: Technology, Privacy, and Politics

Our first section looks at the influence of data on the relationship between citizens and parties during election periods, and the concerns this raises for privacy. While there has been a great deal of academic and policy work on the problem of privacy in relation to governance, comparatively little has been written in to relate this problem with the party bureaucracy. Central this discussion of privacy is R.K Nielson's descriptive, 'minimalist' interpretation of liberal democracy; in which the involvement and activity of the average citizen is relatively limited. From such a starting point, the party emerges as the central institution in a democracy, mediating between citizen and government.

² Nissenbaum (2004) 'Privacy as Contextual Integrity', *Washington Law Review* Vol. 79:119 pp.119-158

Rosenblum's definition of political party is useful, as it relies on a literature consensus to create a helpful definition: "parties are associations organized for political conflict...a group organized to contest for public office...that claims a substantial number of followers, a base".³ It is important to note further that during an election period, the 'contest for public office' takes on a Weberian hue in which the parties seek to satisfy this one rational goal, paying little regard to the effect of their electioneering methods on the integrity of democracy itself. In this section, we will examine how political parties collect personal information in both Canada and the United Kingdom. Thus, we will examine political parties purely in the context of election campaigns, and how they use data to manage and allocate resources during an election. In addition, we notice that Canada has a data regime and laws regarding communication between electors and political parties that make it easier to collect data with voter's consent, compared to the United Kingdom. To study both systems, the 2015 Canadian election is examined, with an in depth focus on the Liberal Party of Canada's efforts in the Province of New Brunswick. As this was the first major electoral campaign fought by the party using a substantial online data system (known as Liberalist), the campaign offers important insights into the future of data use for political purposes. It is important to note how much more 'advanced' North American countries, like Canada, are in this regard. Whilst Bennett and Bayley state that "...the direct targeting of potential voters by political parties is still not a widespread practice" they do point out the notable exception of the United Kingdom. However, even in the UK privacy laws prohibit the use of data, if not its collection.⁴

Case Study: Canadian Election 2015

Firstly, the Liberal Party campaign was unique in that it was digitalized at every stage of the data collection. The central database (Liberalist) was synced with an online application known as miniVAN, designed by American firm NGP Van. This application could be uploaded with names and addresses of electors, shown in Appendix 1. Each

³ Rosenblum, Nancy L. *On the Side of the Angels: An Appreciation of Parties and Partisanship*. Princeton: Princeton UP, 2008. Print.

⁴ Bennett, Colin J., and Robin M. Bayley. "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis." *CANADIAN FEDERAL POLITICAL PARTIES AND PERSONAL (2012)*: 10. Web.

elector would have a series of questions attached to them, including what party they would likely support, number of children, important issues for them, etc. Using this application on the tablet, volunteers canvassed and selected answers for each voter. At the end of a canvassing cycle, this information was uploaded via the cloud to Liberalist. From here any party employee with access could view the information of any voter that had been canvassed.

This represents a large departure from previous practice for two reasons. Firstly, previous campaigns were predominantly managed by pen and paper – meaning that more time was spent transferring data into a computer system. The use of digital technology drastically reduced the required labor. Secondly, data is now transferable, in the sense that it can be shared between campaigns horizontally and vertically. Prior to this election, data was largely primitive in nature, given the time spent entering it into the system. As such, it was harder to share information between campaigns because very little of it was digitized and placed on internet servers. Now, data has become instantly transferable and collectible meaning that access and use has become far simpler.

This in turn has changed the nature of political campaigns in Canada. As a National Field Worker noted, previous campaigns had been about ‘exposure’, being present and visible within the constituency to reach as many voters as possible.⁵ Since there was no way of accurately acquiring the voting preferences of local voters, save through polls done by the national campaign, old style campaigns tried to maximize the exposure of local candidates through signs, radio appearances and large rallies – essentially mediated events that limited direct contact with the politician in favor of being able to reach large numbers of people simultaneously. The resulting difficulty to gauge support was heavily stress by the national field worker. Digitalized data, on the other hand, allows you to do this instantly, though not without problems. It also allows a political party to estimate support prior to an encounter – for instance, if a certain demographic such as ‘single mothers making between \$30,000 and \$50,000’ has a tendency to vote for a certain party, the party can automatically and more reliably target this demographic.

⁵"Interview with Provincial Field Director - Liberal Party." Online interview. 28 Nov. 2015.

Additionally, the Campaign Chair, seconded by the Field Director, recognized that this method “made human resources more efficient.”⁶ As Election Day approached, political parties were able to target ‘undecided voters’ who as the Field Director emphasized, “are extremely valuable because you can return to them”.⁷ In other words, in a bid to switch them to ‘your party’ you could devote further canvassers and mail drops at those residences who declared themselves undecided. The Campaign Chair also stressed that this focus on data allowed the parties to ‘outsource’ simple data harvesting, such as voter identification, to call centers while focusing community volunteers on reaching out to the undecided. Unlike previous campaigns, where it was impossible to target resources, data allowed the campaigns to use their human resources optimally and reach out to as many voters as possible.

The Figure shown in Appendix 1, taken from one of the constituencies Liberal campaign teams, demonstrates how in the later months of August, when parties had accumulated enough money to pay for call-center (human) calls, there was a corresponding increase in canvassing attempts. In this case, volunteers were being employed to canvass residents that had declared themselves undecided on the phone, and, importantly, the number of respondents declaring themselves Liberal increased from 64 people the week of August 3, 2015 to 303 the week of August 24, demonstrating the effect of human contact on the electoral process, made possible by data. This may seem counter-intuitive, but is a natural outgrowth of the targeting that data allows. Most political parties, the Liberal Party included, ranks support based on likelihood to vote and commitment to a political party. By accumulating data through human and robo-calls prior to volunteer ‘doorstep’ contact, political parties are vastly more likely to target undecided and wavering households, while reaching out to strong supporters to volunteer. In essence, political parties are more capable of responding to the needs of individual voters and give more human volunteer contact time to voters who remain ambivalent

⁶ “Interview with Provincial Campaign Co-Chair – Liberal Party” Online interview. 14 Nov. 2015.

⁷Ibid.

or unsure. In the 2015 election, the first to use widespread data, turnout actually increased by 7.3 percentage points, and achieved the highest turnout since 1993. While this cannot solely be attributed to data use by political parties, it should be noted that in the constituency considered in the case study, which operated one of the most successful data operations in the country, turnout increased 13.2 percentage points. Thus, on both a local and national level, the use of data did have a role to play in greater voter engagement.^{8,9,10}

Case Study: United Kingdom

The positive impact of data has important electoral implications, and may provide an important model for the UK to adopt more extensively. In the United Kingdom, the young and the poor have increasingly removed themselves from politics over the last 30 years. In 1987, the turnout rate for the poorest was four points below the wealthiest income group, but by 2010 this had grown to 23 points. Similarly, an 18-point gap could be seen in 1970 between the 18-24 range and the over 65s, compared to the 32 point gap seen in 2010. What is more, non-voters were noticeably more pessimistic than voters, with 40% believing that life will be better in 2020 compared to 45% of voters.¹¹ It is worth noting that according to the blog, *Survation*, the most likely thing to encourage non-voters to vote was 'receiving a leaflet about a candidate', which is made more likely if data is collected and targeted.¹²

Thus, given the data's positive impact on elections, and the potential for greater engagement, this is a tool that political parties appear likely to continue to use. However, there are some significant concerns that arise from this use of data:

- There is a potential conflict of interest between politicians in a governing capacity, between their governing duties and compilation of private data in their duties as a Member of Parliament

⁸ "Voter Turnout at Federal Elections and Referendums." *Elections Canada*. Elections Canada, n.d. Web. 13 Dec. 2015.

⁹ "Federal Election 2015: Voter Turnout Highest in Decades." *Global News Federal Election 2015 Voter Turnout Highest in Decades*. N.p., 20 Oct. 2015. Web. 13 Dec. 2015.

¹⁰ Liberal Party Provincial Records, Anonymized for Privacy Protection Reasons

¹¹ Flinders, Matthew. "Look beneath the Vote | OUPblog." *OUPblog Look beneath the Vote Comments*. N.p., 04 Mar. 2014. Web. 05 July 2016.

¹² Barker, Nicholas. "Apathy in the UK - A Look at Attitudes." *Survation.com*. *Survation.com*, n.d. Web.

is not necessarily accompanied by a complete awareness of just how much personal data they are sharing.

It is apparent that many users have inadequate understandings of where personal data or information which they provide online may flow. This is not entirely the fault of providers, as a degree of disinterest or even wilful ignorance appears to persist amongst users, with Solove detailing that almost 90% of Facebook users have never read its privacy agreement. However, this is not simply a case of self-inflicted ignorance over data flows, and thus a wilful relinquishing of information flow norms. Many consumers may find information about how their data is used or what elements are stored difficult to find, thus restricting their ability to exercise judgment over disclosure. Fuchs demonstrates this in an analysis of Facebook's privacy agreement, finding it to be obfuscatory and ultimately to illuminate little about the flow of user's data once it has been collected.⁴⁷ Indeed, in this instance "the main form of privacy on Facebook is the intransparency of [advertisers'] use of personal user data that is based on the private appropriation of user data by Facebook."^{48,49} This is clearly not limited to simply Facebook, through the popularity of the firm makes it a useful metonym. In some instances, the difficulty of users in ascertaining what aspects of their personal data are flowing where is compounded by the undermining of existing data legislation by firms. This is highlighted by a 2014 study undertaken by the University of Sheffield under the EU funded Increasing Resilience in Surveillance Societies (IRSS) project, which highlights widespread inadequate compliance with the spirit of existing UK data laws. As discussed in section one, under UK law, members of the public are entitled to contact data controllers and request information on what data the organization holds on them. However, the study reported that in nearly a fifth of the organizations sampled they were unable, after repeated attempts over various mediums, to locate contact details for the data controller.

⁴⁷ Solove, D 'The Future of Reputation: gossip, rumour and privacy on the internet' (2007) New Haven, Yale University Press

⁴⁸ Fuchs, C (2011) 'An Alternative View of Privacy on Facebook', *Information* 2, 140-165

⁴⁹ Ibid, 157

In addition, the study highlighted a generally poor knowledge about data rights within the organizations contacted, which formed an impediment to contacting the (generally knowledgeable) data controllers. If knowledge about data protection and management is restricted to specialized employees within an organization, then it becomes harder for members of the public to ascertain where their information is flowing. Widespread lack of knowledge about data privacy may also increase the risk of data leaks, as staff are ill-informed about best practice, or what types of information it is appropriate to disclose. Here, we note that similar concerns have been raised within this paper regarding political parties, with data harvested for explicitly campaigning purposes being integrated into databases accessible by a wider pool of MP's and staffers. In one instance the convoluted nature of data requests was such that the authors state that: The obscurity, ambiguity and ultimately the failure to clearly identify the data controller and/or data protection department and its contact details appear to demonstrate not only bad practice on Facebook's behalf but also bad faith."^{50,51,52} Such bad practice, if not bad faith, is clearly problematic with regards to enabling, or even allowing, users to exercise well-informed judgment on their information sharing.

The study identified a generally higher standard of best practice regarding data access in the public sector. This indicates that there is clearly scope for private organizations to improve access to knowledge about the holding of personal information, and thus to facilitate clearer understandings by users of information flow. For instance, the right to be forgotten or to remove shared information is significantly under-regulated and difficult for consumers to achieve. As young people who are currently sharing views all over the internet, and for younger generations who live their entire lives online there is often little long term mindedness about the potential repercussions their statements and data might have on their futures. Once that information is put into the web it is very difficult to control just how it is used or how to remove it completely. This raises

⁵⁰ Norris, Clive, Prof., and Xavier L'Hoiry, Dr. "Increasing Resilience in Surveillance Societies (IRISS)." *International Legal Materials* 5.2 (2014): 1-65. 29 Apr. 2014. Web.

⁵¹ *Ibid*, 19

⁵² Data Protection Act, 1998, § 7(1) (Government of the United Kingdom). Print.

the difficult question of who is responsible for securing the Internet? Only through an active government, transparent and accountable private sector companies, and well informed citizens can data be more carefully handled.⁵³

The problem is threefold. For not only are consumers unable to easily access what data is being collected, unable to have the power to avoid being profiled and remove their past shared data, the companies themselves often collect the data without clear objectives of what exactly this data is being collected for. Brookman has persuasively argued that a perception that it is essential to collect this data to gain the upper hand over competitors and more effectively target consumers and win business dominates online companies. The idea prevails among companies that they have 'the right to collect this data on behalf of our client and we'll figure out what to do with it later.'⁵⁴ But with the pace and dynamism of the technology world this poses significant problems for data and concerns for the individual about where their information goes. For example, the mergers of smaller companies being bought by the giants of the technology world means it is difficult for the consumer to ascertain where their information is being gathered and for what means it is being used. As has already been suggested in the Talk Talk example, ignorance among companies themselves about why they are collecting data and what they are doing with that data are unanswered questions.

A more chilling thought altogether is the lack of oversight over the algorithms and code which construct pinpointed advertisement and manage data. Governments allow firms to essentially self-regulate this. But as Samir Chopra has discussed autonomy might well lie beyond not only the company but beyond the initial programmer. Without a human mediator it is hard to envisage just what their rights, duties and obligations are

⁵³ Herre, Trey, and Eric Ormes. "Understanding Cybersecurity Part 2." *AFPC.org*. N.p., 15 Apr. 2015. Web.

⁵⁴ Thompson, Cadie. "Companies Aim to Cash in on Your Intimate Social Data." *CNBC*. N.p., 30 Oct. 2013. Web. 05 July 2016.

to the individual's ⁵⁵ privacy concerns. This must be the subject of more extensive research and The Wilberforce Society is conducting further research into Artificial Intelligence and its repercussions.

Policy proposals

With regards to privacy in the flow of personal information online we have thus far identified several issues which we feel compromise privacy. Whilst some of these cases, notably the extraction of data by state security services and by illegal hackers, are clearly difficult to address, we believe that some action can be taken more broadly. This stems from our understanding that modern privacy online is compromised by a lack of situational judgment by users, who are unable to properly assess the likely flows of their data once they render it online. In order to ensure that users are better able to exercise real agency in the flows of their private information we suggest the following:

1. A simplification or standardisation of privacy agreements, perhaps with a standardised template or checklist. This would enable users to more easily determine what might happen to the information they choose to share online. Greater transparency and standardisation may also allow customers to distinguish more easily between the levels of privacy on offer by firms, incentivising greater respect for information flow norms by companies competing for users. Firms must be legally obliged to outline publicly precisely what data they are collecting and for what purpose.
2. Improved accessibility of data controllers to members of the public, in order to further enable users to ascertain where their information is ending up, and to gauge the scale of their 'online identity'. This would ameliorate one of the major flaws identified by the IRSS study, flaws which could be further reduced by:

⁵⁵ A Legal Theory for Autonomous Artificial Agents

3. Greater institutional awareness of data laws and rights. This is essential to support data requests, whilst fostering good practise in terms of data and privacy management. Greater learning opportunities will also enable employees to make more informed choices with regards to their own online presence.
4. A national dialogue on security and data sharing. In order for members of the public to understand the level of risk the government must initiate a public awareness and education campaign. In particular this must be directed at young people building on existing programmes in schools. Undoubtedly the private sector and the public sector have to work together to mount a serious defence and to secure the data of individuals and to educate the public more broadly about the implications of sharing their data.

Conclusions

This paper has aimed to draw out some of the complexity of contemporary debates surrounding privacy and data collection technology. Where such debates are lacking we hope that we have stimulated thought. International case studies have provided particular emphasis on the as-yet-unformed nature of the accommodation between the vast potential of data technology for both commercial and political organisations, and the understated degree of agency and knowledge currently afforded to consumers and citizens.

A common theme across the issues we have discussed is that of consent. Whilst organisations are currently able to claim widespread consent for data collection from their users, we argue that the largely tacit or assumed consent that this constitutes is not strong enough. This is an especially acute concern given the apparent vulnerability of data to hacking or state interference, and given the ill-defined parameters of how organisations will sue this data. In some cases, this remains a mystery even to those within the organisations, leaving individuals unable, in our view, to exercise sound judgment. Instead, we have argued, policies ought to be instigated which will increase both awareness of the flows of data beyond the simple interaction between users and organization,

and the judgments which this will enable must be empowered by a stricter understanding of consent to data collection.

When users entrust their data to organizations, there must be a sounder structure of practice and policy to support this trust. The burden in this case lies with organizations to ensure that their practices do not breach the reasonable expectations of the consumers who hand over their data, and to properly safeguard data collections against breaches.

Clearly the dynamic and fast changing nature of the digital technology world will necessitate regular revisions of policy in this area. Establishing a more substantive dialogue and common understandings of the duties, as well as opportunities, which come from data technology, is the best way to empower individuals with the information and agency that they require. Doing so, and doing so soon, offers the best chance to establish a sound and flexible framework to manage the interactions of privacy, politics and data technology.

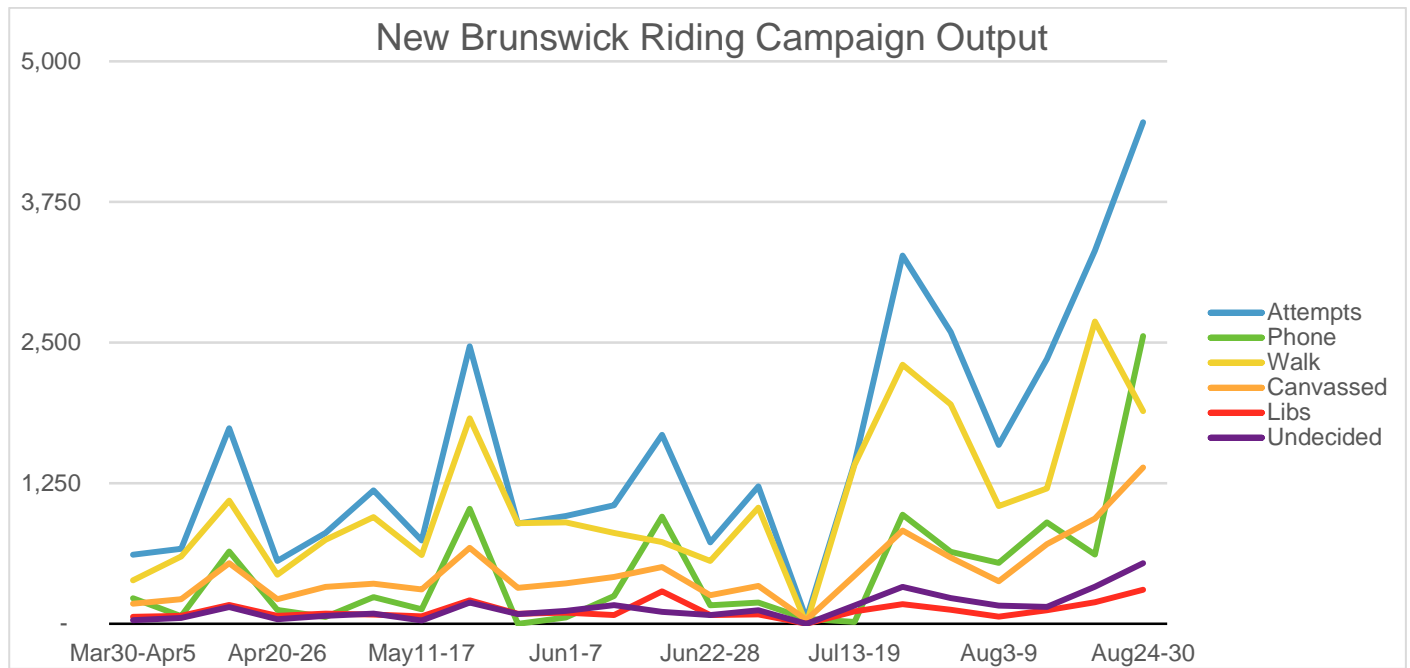
Appendix 1 – Example use of data – Constituency in New Brunswick, Canada

Attempts denote total attempts to contact voters using Liberalist software. Walk denotes in-person canvassing attempts and Phone denotes contact made by telephone. Canvassed includes successful contacts made with voters through attempts. Libs denotes voters who identified as Liberals and Undecided denotes voters who remain undecided. Results tabulated using Liberalist (database) software.

Dates	Mar3 0- Apr5	Apr6 -12	Apr1 3-19	Apr2 0-26	Apr2 7- May3	May4 -10	May11- 17	May18 -24	May25- 31	Jun1-7	Jun8- 14	Jun15 -21
Attempts	614	667	1,738	559	807	1,186	740	2,466	891	959	1,054	1,680
Phone	227	68	643	123	61	237	129	1023	-	57	247	953
Walk	387	599	1,095	436	746	949	611	1826	894	902	807	727
Canvassed	178	219	538	218	328	357	305	675	319	360	416	505
Libs	62	71	168	71	90	82	66	208	89	99	77	288
Undecided	32	52	149	41	70	90	30	189	86	115	166	106

Dates	Jun2 2-28	Jun 29- Jul5	Jul6- 12	Jul13 -19	Jul20 -26	Jul27 - Aug2	Aug3 -9	Aug1 0-16	Aug 17- 23	Aug2 4-30	Total	Aver- age
Attempts	723	1,221	44	1,430	3,273	2,593	1,590	2,354	3,318	4,458	24,235	1,562
Phone	164	189	44	16	970	639	542	902	616	2,557	6,332	473
Walk	559	1,032	-	1,414	2,303	1,950	1,046	1,203	2,687	1,890	18,283	1,094
Canvassed	254	337	35	429	829	588	378	708	936	1,389	7,268	468
Libs	77	83	1	110	175	125	64	120	191	303	2,006	119
Unde- cided	77	120	0	163	328	228	161	150	329	539	2,203	146

Appendix 2 – Graphic Representation of Appendix 1



Bibliography

- Abbott, Paul. "Paul Abbott: Scrap VoteSource. Empower the Digital Team. Sync Databases. How to Maximise CCHQ's Use of IT." *Conservative Home*. N.p., n.d. Web. 20 Dec. 2015.
- Barker, Nicholas. "Apathy in the UK - A Look at Attitudes." *Survation.com*. Survation.com, n.d. Web.
- Bennett, Colin J., and Robin M. Bayley. "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis." *CANADIAN FEDERAL POLITICAL PARTIES AND PERSONAL (2012)*: 10. Web.
- Bennett, Colin. "The Politics of Privacy and the Privacy of Politics." *The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies* | Bennett | *First Monday*. First Monday Journal, 28 June 2013. Web. 13 Dec. 2015.
- The Canadian Press. "Tory Database Draws Ire of Privacy Experts." *CTVNews*. The Canadian Press, 18 Oct. 2007. Web. 11 Dec. 2015.
- Carrell, Severin. "Lib Dems Broke Privacy Rules with Cold Calls." *The Guardian* [London] 25 Sept. 2008: n. pag. Print.
- Data Protection Act, 1998, § 7(1) (Government of the United Kingdom). Print.
- Delacourt, Susan. *Shopping for Votes: How Politicians Choose Us and We Choose Them*. Toronto: Douglas & McIntyre, 2013. Print.
- "Fact Sheets." *Office of the Privacy Commissioner of Canada*. N.p., n.d. Web. 13 Dec. 2015.
- "Federal Election 2015: Voter Turnout Highest in Decades." *Global News Federal Election 2015 Voter Turnout Highest in Decades*. N.p., 20 Oct. 2015. Web. 13 Dec. 2015.

Flinders, Matthew. "Look beneath the Vote | OUPblog." *OUPblog Look beneath the Vote Comments*.

N.p., 04 Mar. 2014. Web. 05 July 2016.

"Government Data-requests to Facebook." *The Economist*. The Economist Newspaper, 17 Nov. 2015.

Web. 05 July 2016.

"Guidance on Political Campaigning." *Information Commissioner of the United Kingdom* (2011): n.

pag. *Ico.org*. 2011. Web.

Herre, Trey, and Eric Ormes. "Understanding Cybersecurity Part 2." *AFPC.org*. N.p., 15 Apr. 2015.

Web.

Hodgson, Martin. "Investigation Launched into Tory Database Bungle." *The Guardian* [London] 22

May 2008: n. pag. Print.

Howard, Philip N., and Daniel Kreiss. "Political Parties and Voter Privacy: Australia, Canada, the

United Kingdom, and United States in Comparative Perspective | Howard | First Monday."

Political Parties and Voter Privacy: Australia, Canada, the United Kingdom, and United States

in Comparative Perspective | Howard | First Monday. First Monday Journal, 11 Nov. 2010.

Web. 13 Dec. 2015.

"Interview with Daniel Zeichner." Interview. 24 Nov. 2015: n. pag. Print.

"Interview with New Brunswick Campaign Co-Chair." Online interview. 15 Nov. 2015.

"Interview with Provincial Field Director - Liberal Party." Online interview. 28 Nov. 2015.

Naughton, John. "The TalkTalk Hack Can't Be Shrugged off | John Naughton." *The Guardian*. Guard-

ian News and Media, 15 Nov. 2015. Web. 05 July 2016.

Norris, Clive, Prof., and Xavier L'Hoirry, Dr. "Increasing Resilience in Surveillance Societies (IRISS)."

International Legal Materials 5.2 (2014): 1-65. 29 Apr. 2014. Web.

Privacy Act, Last Amended July 2015 33 §§ 31-31 (Government of Canada 2015). Print.

Staff. "Someone Is Watching You." - *Editorials*. N.p., 20 Oct. 2007. Web. 11 Dec. 2015.

Staff. "Someone Is Watching You." *The Telegram*. N.p., 20 Oct. 2007. Web. 11 Dec. 2015.

Strategies, EMC. *The Conservative Party*. 2010. EMC Strategies Paper. EMC Corporation, London.

"TalkTalk Hack 'affected 157,000 Customers'" *BBC News*. BBC, 06 Nov. 2015. Web. 05 July 2016.

Thompson, Cadie. "Companies Aim to Cash in on Your Intimate Social Data." *CNBC*. N.p., 30 Oct. 2013. Web. 05 July 2016.

United Kingdom of Great Britain and Northern Ireland. Information Commissioner of the UK. *Advice for Elected and Prospective Local Councillors*. London: n.p., 2015. Print.

United Kingdom of Great Britain and Northern Ireland. Information Commissioner of the UK. *Warning to Political Parties: Compliance with the Data Protection Act*. London: Information Commissioner, 2015. Print.

United Kingdom of Great Britain and Northern Ireland. Information Tribunal. *Scottish National Party and the Information Commissioner*. By Vivian Bower and Elizabeth Hodder. Edinburgh: n.p., 2005. Print.

"Voter Turnout at Federal Elections and Referendums." *Elections Canada*. Elections Canada, n.d. Web. 13 Dec. 2015.

Watt, Nicholas, and Julian Borger. "Tories Reveal Secret Weapon to Target Voters." *The Guardian* [London] 9 Oct. 2004: n. pag. Print.