When Data Crimes are Real Crimes:
Voter Surveillance and the Cambridge Analytica Conflict

by

Jesse Gordon
BA Honours, University of Saskatchewan, 2016

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of

MASTERS OF ARTS

in the Department of Political Science

Supervisory Committee

When Data Crimes are Real Crimes:
Voter Surveillance and the Cambridge Analytica Conflict

by

Jesse Gordon
BA, University of Saskatchewan, 2016

Supervisory Committee

Dr. Colin Bennett, Department of Political Science
Supervisor

Dr. Arthur Kroker, Department of Political Science
Departmental Member

Abstract

This thesis asks what conditions elevated the Cambridge Analytica (CA) conflict into a sustained and global political issue? Was this a privacy conflict and if so, how was it framed as such? This work demonstrates that the public outcry to CA formed out of three underlying structural conditions: The rise of the alt-right as an ideology, surveillance capitalism, and a growing and unregulated voter analytics industry. A network of actors seized the momentum of this conflict to drive the message that voter surveillance is a threat to democratic elections. These actors humanized the CA conflict and created a catalyst for a large scale public outrage to these previously ignored structures. Their focus on democratic threat also allowed this conflict to transcend the typical contours of a privacy conflict and demonstrate that the consequences of CA are societal, rather than personal. Despite the democratic threat of voter surveillance, Canada and the United States have yet to address the wider implications of voter surveillance adequately. Thus, how these systems are used will be a question of central importance in upcoming elections.

Table of Contents

.

List of Tables

List of Figures

Acknowledgments

I would like to acknowledge all of the people that helped me complete this thesis. I extend my endless appreciation to my supervisor Colin Bennett for introducing me to surveillance literature and for his time. His patience and invaluable guidance over these past two years have helped me grow as an academic, and I am a better scholar because of it. I would also like to extend a thanks to Arthur Kroker and Peter Chow-White for taking the time to be on my committee.

To my parents John and Audrey Gordon, I extend a thanks for fostering my curiosity and love of learning, and your years of emotional support. You have helped to shape me into the man I am today. To my sister Sara, I would like to thank you for teaching me to question and defy authority. Though at times this trait has made my life considerably more difficult, it was exceptionally useful during this thesis.

To my friends, who have now spread from coast to coast, around the world, and throughout this department. Your successes in life inspire me to be better, and though I may not have seen much of some of you in the past two years, you are always in my heart. I truly admire everyone of you beautiful weirdos. Thank you for shaping my ideas and understandings of the world. And for providing me with academic advice, solicited or otherwise. A part of each of you is in this work. Thank you for your support over these past few years, I also appreciate you for enduring my rants about surveillance.

To my dog Emma, thank you for demanding a cuddle when I am clearly stressed, and for encouraging me to go for a nice long walk to clear my head. Your endless patience while I promise “just one more page and we can go for a walk” is noted and appreciated.

Finally to my puzzle piece, my partner, and the love of my life, Ashley. Thank you. You encouraged me when I was at my lowest, and humbled me by flaunting your superior mastery of the English language when I was at my highest. You are my world, and I truly could not have done this without you. I love you.

Dedication

This thesis is dedicated to my nephew Thomas, you inspire me to strive for a better future. Tom, I wish for you to grow up in a less privacy intrusive world.

I also dedicate this thesis to Dylan Robert Thorpe, I miss you every day and am sorry you couldn't read this. I know you would have liked it. May the force be with you buddy.

Acronyms

API - Application programming interface
BBC – British Broadcasting Corporation
CA- Cambridge Analytica
CBC – Canadian Broadcasting Corporation
DCMS - The Digital, Culture, Media and Sport Committee
EFF - Electronic Freedom Foundation
ETHI- The House of Commons Standing Committee on Access to Information, Privacy and Ethics
FTC – Federal Trade Commission
ICO – Information Commissioner's Office of the United Kingdom
and Electronic Documents Act
NDA – Non-Disclosure Agreement
NSA – National Security Agency
SCL – Strategic Communications Laboratories
SNS - Social Networking Sites
PII – Personally Identifiable Information

Introduction

Cambridge Analytica's (CA) illegal data collection began in 2013 when Dr. Aleksandr Kogan harvested data from 87 million Facebook users.[1] In December 2015, the collection became a global story when *The Guardian* published an article about the Ted Cruz campaign's use of data derived from Facebook to target voters.[2] As time passed, the story transformed into a privacy conflict.[3] Three years on, something feels different about CA. The popular reaction has been different, with a level of societal outrage that had not been achieved in previous privacy scandals.[4]

CA did not follow the typical contours of a privacy conflict as explored by scholars such as Bennett.[5] Usually, these stories appear in the technology section of newspapers, or if the scandal is big enough, briefly on the front-page. Eventually, however, the technical language associated with such issues is hard to translate into a catchy headline, and the media loses interest in pursuing the story. This time, the story remained a relative fixture in the news for almost two years. People, en masse, demanded Facebook adjust its privacy settings to appease a now more privacy-conscious population. When it failed to do so adequately, 25% of their US users deleted the Facebook

---

[1] Sumpter, David. 'My Interview with Aleksandr Kogan: What Cambridge Analytica Were Trying to Do and Why Their…'. Medium, 22 April 2018. https://medium.com/@Soccermatics/my-interview-with-aleksander-kogan-what-cambridge-analytica-were-trying-to-do-and-why-their-f869ef65d945.

[2] Davis, Harry. 'Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users | US News'. The Guardian, 11 December 2015. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[3] Gilbert, David. 'Cambridge Analytica Bragged about Using Fake News, Bribes, and Ukrainian Women to Influence Elections'. Vice News (blog), 19 March 2018. https://news.vice.com/en_ca/article/bjp87a/cambridge-analytica-bragged-about-using-fake-news-bribes-and-ukranian-hookers-to-influence-elections.

[4] Steiger, Stefan, Wolf J. Schünemann, and Katharina Dimmroth. 'Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany'. Media and Communication 5, no. 1 (22 March 2017): 7–16. https://doi.org/10.17645/mac.v5i1.814.

[5] Colin Bennett, *Privacy Advocates: Resisting the Spread of Surveillance* (The MIT Press, 2008).

application from their phones.[6] Politicians around the world wrote reports about the importance of data privacy; multiple regulatory agencies launched investigations, and the ICO in the UK raided CA offices to assert the message that "data crimes are real crimes."[7]

From a privacy perspective, the reaction to this event was unprecedented. The scope of the conflict demonstrated that privacy was no longer a national affair but a global issue. The world of data-brokers, an obscure industry, was thrust into the spotlight as people realized that their personal information could be captured, profiled, and sold to political parties in a process Bennett refers to as voter surveillance.[8] Voter surveillance is the use of surveillance to engage with, show ads to, and potentially manipulate voters. It relies on a variety of actors, methods, and technologies, and has remained largely unchallenged in broader public discourses. Voter surveillance is different than other forms of surveillance. Its purpose is to enhance and direct democratic participation in a time where trust in democratic institutions and partisanship is declining.[9] Thus, regulators must weigh the benefits of voter surveillance against their responsibility to protect privacy.

One of the data regulators responsible for investigating the CA conflict was the Office of Information and Privacy Commissioner of British Columbia. From May to

---

[6] Bhattacharjee, Monojoy. 'Facebook Loses over 25% of Its App Users in US: Pew Research'. What's New in Publishing | Digital Publishing News, 7 September 2018. https://whatsnewinpublishing.com/2018/09/facebook-loses-over-25-of-its-app-users-in-us-pew-research/.

[7] Cadwalladr, Carole. "Elizabeth Denham: 'Data Crimes Are Real Crimes'." The Guardian. July 15, 2018. Accessed November 13, 2018. https://www.theguardian.com/uk-news/2018/jul/15/elizabeth-denham-data-protection-information-commissioner-facebook-cambridge-analytica.

[8] Colin J. Bennett, 'Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications', *Surveillance & Society* 13, no. 3/4 (26 October 2015): 370–84, https://doi.org/10.24908/ss.v13i3/4.5373.

[9] Colin Bennett, 'The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies', *First Monday* 18, no. 8 (25 July 2013), https://doi.org/10.5210/fm.v18i8.4789.

September of 2018, I had the opportunity to assist this office in collecting evidence for their investigation into Cambridge Analytica, AggregateIQ, and Facebook. A non-disclosure agreement (NDA) prohibits me from discussing much of my work for the office. However, one body of evidence that is not restricted by an NDA is the testimonial evidence collected by the ETHI Committee in Canada, the DCSM Fake News Committee in the UK, and the Senate Judiciary Hearings in the US. Over the five months that I worked in this office, I, among others, collated this evidence. These testimonies provide the main body of empirical evidence, upon which the arguments in this thesis are based.

The Research Question

This thesis asks, what were the conditions that elevated the CA conflict into a sustained and global political issue? Data protection authorities (DPAs) and privacy commissioners around the world responded to condemn the Cambridge Analytica conflict. But was this a conflict about privacy and, if so, in what ways was it framed as such?

Method

To understand the conditions that assisted in garnering widespread public and political attention, I engaged in an intrinsic case study analysis of CA. John Gerring defines a case study as "an intensive study of a single unit for the purpose of understanding a larger class of (similar) units."[10] In this thesis, the CA conflict represents a deviant public reaction to privacy conflicts. This case study is built on an analysis of primary sources, comprised of evidence collected by the various national inquiries into

[10] John Gerring, 'What Is a Case Study and What Is It Good For?', *The American Political Science Review* 98, no. 2 (2004): 342.

CA. These inquiries resulted in an extensive collection of evidence that includes testimony by industry insiders, privacy scholars, advocates, and legislators. Specifically, it includes testimony by: Alexander Nix, the former CEO of Cambridge Analytica; Alexandr Kogan, the researcher who collected the Facebook data; whistleblowers Chris Wylie, Brittany Kaiser, and Sandy Parakilas; contractors such as Chris Vickery; and academics such as Eitan Hersh, and Emma Briant. Concurrent with these testimonies, I supplement this research with secondary sources by journalists such as Carole Cadwalladr, who was publishing new reports that, at times, contradicted witness testimony. Additionally academic sources about voter analytics and news articles about CA prior to and during the 2016 US election provide contexts and insight into CA's work. These sources of data assisted me in exploring the broad sociopolitical underpinnings and reactions to the CA controversy.

Justification

Understanding the CA conflict is necessary for three reasons. First, the global response to this conflict is an anomaly, dominating headlines around the world as it has. The dynamics of this conflict have defied the typical contours of privacy scandals and demand further analysis.

Second, CA exemplifies the dangers of unregulated data-driven elections. As campaigns have become increasingly reliant on the use of voter-analytics, CA is an example of a company breaking the law to provide new data to the ecosystem of electoral campaigns. Privacy and surveillance scholarship have been late to recognize the threat of voter surveillance to the democratic system. CA exemplifies the consequences of this oversight.

Third, because the public reaction to CA was so anomalous, it is essential to understand the elements that elevated this conflict to the top of global headlines. Privacy conflicts of the past have provided a useful blueprint for fostering broader support. However, the privacy advocates' use of international media, though not a new tool for activists, was striking in how effectively it harnessed social outrage around a privacy issue. It could provide a useful blueprint for future privacy activism.

Organization

Chapter one is a review of the surveillance, privacy, and political marketing literatures. By examining these fields, I will demonstrate that privacy violations and surveillance erode democracy. This literature does not adequately explore these ideas in the context of voter surveillance. Conversely, the political marketing literature focuses extensively on the ways personal data is utilized in an electoral context, but dedicates limited resources to exploring the privacy implications. Scholarship in this field argues that privacy is a universal concept that is deemed essential within almost all societies. Political parties have a responsibility to explore the wants and desires of their constituents, but must balance this responsibility with respect for privacy norms. Ultimately this chapter demonstrates that the literature does not adequately address the extent to which voter surveillance is, or is not, acceptable, or the subsequent outrage over CA.

Chapter Two situates CA into the context of US voter surveillance, arguing that CA was a tipping point in the public tolerance of voter surveillance. It is necessary to understand the dynamics of the US influence industry, a wide network composed of "digital and political strategists and consultants, technology services providers, data

brokers and platforms." These actors utilize various digital tools for the purposes of altering the opinions and decisions of people.[11] Understanding this wider industry will demonstrate that the practices of CA are substantially similar to those observed in the voter analytics industry as a whole. Thus, the popular reaction must stem from elsewhere. Finally, I explore the rise of the alt-right and its connections to CA. I argue that these groups' connections significantly contributed to increased public awareness of voter-surveillance practices.

Chapter Three argues that a decade of nearly unlimited data collection by Facebook has eroded concepts of privacy. Here, I rely on witness testimony to describe what data CA harvested and how they used it. I will also explore the politicization of Facebook data over the last decade. I demonstrate how CA was able to take advantage of two well-known and documented problems that existed within Facebook: the lack of privacy safeguards and the company's desire for economic growth. Exploring Facebook's practices over the past decade will demonstrate that CA was dealing with a company who resisted oversight, lacked accountability for their customer's data, and actively pursued using this data to impact democratic change. Ultimately, this chapter concludes that the prevalence of real privacy violations by Facebook primed users to react so strongly to the percieved privacy violation of psychographics.

Chapter Four explores the actors surrounding CA and how they amplified the public reaction by framing the narrative of the conflict. Individuals such as Chris Vickery, Brittany Kaiser, Chris Wylie, and Carole Cadwalladr all played an essential role

[11] Varoon Bashyakarla et al., 'Personal Data:Political Persuasion Inside the Influence Industry. How It Works.', Data and Politics Team (Tactical Technology Collective, March 2019), https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf. 5

in allowing this story to defy the contours of a typical data-scandal. Though there were many more people who assisted in elevating this story, these actors played a central role in highlighting the conflict. I will begin this chapter by reviewing the literature on privacy activism and will then analyze the testimonies of these individuals to understand how these actors framed the CA conflict.

In my conclusion, I demonstrate that the CA conflict cultivated broad and sustained outrage because of a convergence of the underlying structural conditions explored throughout this thesis. I will then demonstrate how the conflict challenges privacy protection and the various roles privacy plays in a democratic society.

The CA conflict appears to have intensified public demand for politicians to change their relationship with voter data. Regulator reports such as *Democracy Disrupted* by the ICO,[12] the DCSM *Fake News Report,*[13] and the ETHI *Interim Report on Cambridge Analytica*[14] support this conclusion. All of these reports either recommended or ordered that political parties' data collection must be regulated. Despite broad public support, political parties remain resistant to regulation. So did the CA conflict change our understanding of and concern about voter surveillance?

---

[12] Elizabeth Denham, 'Democracy Disrupted?: Personal Information and Political Influence' (Information Commissioner's Office, 11 July 2018), https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf.

[13] Damien Colins, 'Disinformation and "Fake News": Interim Report', Session 2017-2019 (United Kingdom House of Commons: Digital, Culture, Media and Sport Committee, 24 July 2018), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

[14] Bob Zimmer, 'Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Demcoratic Process:' (The Standing Committee on Access to Information, Privacy and Ethics: Canadian House of Commons, June 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf.

Chapter 1: The Importance of Privacy

The Cambridge Analytica conflict raised awareness about the use of personal data to micro-target voters, and the process of tailoring advertisements to smaller and more selected groups of people to maximize the impact and effectiveness of the advertisement.[15] This practice has recently become synonymous with elections and is a crucial tool in voter surveillance. The past decade has seen a disturbingly common practice of over-collection of voter data in Canada, the US, and the UK. CA highlighted the potential privacy and democratic implications of over-collection by political parties and was the impetus for a critical dialogue about data use in elections.[16]

The purpose of this chapter is to explore what the privacy and surveillance literatures say about the use of data in an electoral context. We will first explore some definitions of privacy to assess their relevance to the use of personally identifiable information (PII) in elections. Next, we will explore the growth of the surveillance society, and chart the significant areas of debate by these scholars in their critiques of electoral surveillance, or the lack thereof. This chapter will demonstrate that the privacy and surveillance literature have shown the disruptive impact of surveillance on a democratic system, although it has inadequately explored these ideas in the context of democratic elections.[17] Conversely, the political marketing literature has focused

---

[15] Solon Barocas, 'The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process', in *Proceedings of the First Edition Workshop on Politics, Elections and Data*, PLEAD '12 (New York, NY, USA: ACM, 2012), 31–36, https://doi.org/10.1145/2389661.2389671.

[16] Andrew Rankin, 'All of Canada's Federal Political Parties Collecting "Vast Amount" of Personal Information', The Chronical Herald, 3 July 2019, http://www.thechronicleherald.ca/news/local/all-federal-political-parties-collecting-vast-amount-of-data-329496/.

[17] Voter Surveillance will be used in this thesis to refer to the collection, modeling, and use of voter data for the purposes of effecting political opinions and electoral decisions. The term is borrow from Bennett's (2013) work. Bennett, 'The Politics of Privacy and the Privacy of Politics'.

extensively on the ways data is utilized in an electoral context to mobilize voters, but it has dedicated limited resources to an exploration of the privacy implications.

Privacy: Control & Autonomy

Privacy is integral to modern societies, though it remains an ambiguous concept. The earliest notable western definition of privacy, the right to be left alone, was a legal definition proposed by Warren and Brandeis in 1890.[18] Scholars of the field, unsatisfied with the incompleteness of this definition, have since expanded on it. Much of the scholarship is rooted in the groundwork of Alan Westin, whose seminal work, *Privacy and Freedom*, defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[19] His analysis situated privacy as a right for individuals, groups, and institutions to exercise their autonomy over their personal information. Flaherty agrees with Westin, opting to use Westin's definition of privacy and his typologies to explore the exercising of privacy in Puritan society.[20]

Concurrently, other scholars such as Garfinkle, have expanded the scope of this definition to describe privacy as being about self-possession, autonomy, and integrity.[21] Rule defines privacy as "the exercise of an authentic option to withhold information on one's self."[22] These scholars define privacy as the measure of control individuals have over their own information, the intimacies of their identity, and control over who has

---

[18] David H. Flaherty, *Privacy in Colonial New England* (University Press of Virginia, 1972).
[19] Westin, Alan F. Privacy and Freedom. 1st ed. New York: Atheneum, 1967. 7
[20] Flaherty, *Privacy in Colonial New England*.
[21] Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, 1st ed (Beijing ; Cambridge: O'Reilly, 2000). 4
[22] James B. Rule, *Privacy in Peril* (Oxford, UK ; New York: Oxford University Press, 2007). 3

sensory access to the individual, a definition with which Gavison agrees.[23] The diversity of the concept of privacy means that privacy's performance, protection, and violation differ as significantly in reality as it does academically.

However, with minor analytic distinctions, these definitions all suggest a privacy violation occurs if someone's control or access to their information is compromised without their consent. [24] Consent is central to the concept of privacy, it acts as a mediator of both access to and control over one's privacy. Yet the scope of digital collection in the 21st century is challenging many of these definitions of privacy, as the scale, quality and invasiveness of PII collection have changed the relationship between people and their personal information. Current methods of consent focus on a user agreeing to a company's terms and conditions to use its service. This method of consent has been used for decades as a means of collecting personal information and allowed people to control access to their PII. However, the advent of the internet has altered the volume of terms and conditions to which people must agree.

As of 2008, the average daily internet user would have to spend 244 hours per year reading privacy policies to understand the terms and conditions they encounter, reducing the possibility of informed consent.[25] Many only give these terms and conditions a brief overview before unconditionally agreeing to them. Thus, this system challenges both the control and access components of privacy, a problem that was highlighted throughout the CA conflict. Nissenbaum argues that this method of obtaining

---

[23] Ferdinand Schoeman, 'Privacy: Philosophical Dimensions', *American Philosophical Quarterly* 21, no. 3 (1984): 199.
[24] Helen Fay Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, Calif: Stanford Law Books, 2010).
[25] Aleecia M Mcdonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies', n.d., 26.

consent is ineffective; she suggests that a contextually bound normative structure limiting what is or is not acceptable to collect is necessary.[26] Despite Nissenbaum's critiques, this form of consent has seen continued use in the US. Thus, privacy scholarship has seen renewed interest as our concepts of consent are constantly challenged by new technologies premised on the collection of PII, often without the knowledge of the data owner. Despite the prevalence of uninformed consent, privacy remains a value held by almost all people.

Privacy: Is it Timeless & Universal?

Privacy is essential for almost all societies, though its manifestation can shift based on age, time, culture, and context. Understanding the universal value of privacy will be helpful in assessing the global reactions to CA. Following the Second World War, Article 12 of the United Nations Declaration of Human Rights enshrined privacy into international law.[27] This resolution codified long-standing norms of privacy relations that existed in most societies, including societies that Western anthropologists viewed as not valueing privacy. Various contextual elements play a role in determining what constitutes privacy and, importantly, what constitutes its violation. Westin writes that in seemingly open societies, "kinship rules and interaction norms present individuals with a need to restrict the flow of information about themselves to others."[28] Rules regulate when individuals interact with women who are menstruating, where couples fornicate, admission to a ceremony, or communication during the grieving process. Similarly, an

---

[26] Nissenbaum, *Privacy in Context*.
[27] Christopher Anglim, Gretchen Nobahar, and Jane E Kirtley, *Privacy Rights in the Digital Age* (Amenia, UNITED STATES: Grey House Publishing, 2016), http://ebookcentral.proquest.com/lib/uvic/detail.action?docID=4454671. xxxiii
[28] Westin, *Privacy and Freedom*, 14

individual's desire to privacy can be affected by who they are with, what they are doing, what time of day it is, and who is observing.[29] Krasnova's research on cultural differences in the use of Facebook found that individuals from cultures that were high in uncertainty avoidance (UAI) were more likely to reduce their self-disclosure when faced with privacy concerns.[30] Westin stresses that "anthropological studies have shown that the individual in virtually every society engages in a continuing personal process by which he seeks privacy at some times and disclosure or companionship at other times."[31] Ultimately, it is the ability to choose between disclosure and non-disclosure of ones' information that is central to the concept of privacy.

People often believe that there is a generational divide in privacy values, in part due to the rise of social media. Marwick and Boyd suggest that rather than a lack of concern for privacy, teenagers have become more focused on networked rather than individualistic models of privacy, suggesting that they are attempting to navigate the difficulty of public disclosure in the age of social networking, without being fully open.[32] Likewise, David Lyon points out that the willingness to share personal information with peers often does not extend to a parent or teacher.[33] An individual's right to regulate access to themselves is what provides an individual with a sense of ease, such that scholars such as Altman point out that without this ability to withdraw into the self,

---

[29] Westin, 1968, 12

[30] Hanna Krasnova, Natasha F. Veltri, and Oliver Günther, 'Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus', *Business & Information Systems Engineering* 4, no. 3 (June 2012): 135, https://doi.org/10.1007/s12599-012-0216-6.

[31] Ibid. 13

[32] Alice E. Marwick and danah boyd, 'Networked Privacy: How Teenagers Negotiate Context in Social Media', *New Media & Society* 16, no. 7 (1 November 2014): 1052, https://doi.org/10.1177/1461444814543995.

[33] David Lyon, *Surveillance after Snowden* (Polity Press, 2015). 100

individuals will burn out and face mental fatigue.[34] Likewise, Flaherty's account of colonial New England demonstrates that in seemingly oppressive social structures, individuals will find ways to maintain their privacy.[35] Flaherty argues that even in a Puritan social structure, privacy remained a value that people utilized for their psychological well-being as often as possible.

When viewed together, these works emphasize a vital aspect of the privacy literature. Privacy serves a psychological benefit for all people, one that transcends culture, era, or age, though the manifestation of privacy may differ from person to person, or manifest differently from situation to situation.[36] However, not all violations of individual privacy are equal, and though no infringement is benign, some are irreparable.

Privacy: Types & Violations

Westin identifies four states of privacy, which will be essential for critiquing modern voter surveillance in my conclusion. *Solitude*, the purest state of privacy, describes instances when an individual has time alone (i.e., devoid of observation from others) for inner reflection. *Intimacy* relates to times when individuals can have close, relaxed or frank discussions and relations with others. *Anonymity* is the moment in which an individual may share their thoughts to a total stranger, who may provide feedback but does not or can not restrain or exert authority over the person.[37] *Reserve* Westin defines as a "creation of a psychological barrier against unwanted intrusion; it occurs when an

---

[34] Irwin Altman, 'Privacy: "A Conceptual Analysis"', *Environment and Behavior; Beverly Hills, Calif.* 8, no. 1 (1 March 1976): 24.
[35] Flaherty, David H. 1972. Privacy in colonial New England. Charlottesville: University Press of Virginia.
[36] Nissenbaum, *Privacy in Context.*
[37] Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967). 31-32

individual's need to limit communication about himself is protected by the willing discretion of those surrounding him."[38] A violation of reserve is a violation of the most sacred aspect of the individual, the 'inner circle' which metaphorically holds one's most intimate and private thoughts.[39]

Although there is plenty of academic literature on what the psychological impact of such violations could be if conducted by governments or corporations, there remains an inadequately analyzed gap in the implications of violations that arise in the name of the electoral process. Does surveillance in the electoral context change the nature of the privacy violation? Privacy scholarship by Westin, Flaherty, Garfinkle, Nissenbaum, Rule, and numerous other scholars fails to evaluate these questions adequately. Scanning through the indices of these works for the words *political parties, or elections* demonstrate these works do not touch on these concepts. Illustrations are universally offered from corporate and governmental contexts. Likewise, much of the literature on privacy fails to capture how privacy violations by political parties may differ from those of a corporate or governmental nature.

Privacy violations have occurred with increased frequency in the face of accelerating surveillance practices that have become ubiquitous with the modern state.[40] However, privacy violations are just one aspect of the broader field of surveillance literature, which focuses on identifying contextual elements and power relations that underlie the monitoring of individuals in modern societies.

---

[38] Westin. 1967, 32
[39] Ibid.
[40] Mark Andrejevic, 'Ubiquitous Surveillance', in *Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball, Kevin D. Haggerty, and David Lyon 1948, Book, Whole (New York;Abingdon, Oxon; Routledge, 2012), 91–99,.

Surveillance: Panopticon & Purpose

Privacy theorists have focused extensively on the forms that privacy violations can take, and the impact of such violations on the individual. Surveillance theorists expand the scope of this, and focus on why systems of surveillance are deemed necessary and the broader social implications of these practices. Yet, many of the social impacts of surveillance in the electoral context are under-explored. Despite this gap, many of the problems associated with surveillance were present during the CA conflict. Modern surveillance literature gets much of its inspiration from Foucault's evaluation of Bentham's Panopticon, which he viewed as a laboratory of power to alter behaviour and control individuals.[41] Surveillance studies arose in response to new and expanding means of surveillance and control, in terms of both technology and scope.[42] As such, Ericson and Haggerty argue that surveillance is an acute feature of modernity. As societies became more complex, surveillance became a necessary component to manage their complexities.[43]

Throughout the 20th century, the desire for order led to the creation of databases on citizens. As technology has advanced, available processing power and data-points have increased exponentially. A person may gain approval for a loan, insurance, or welfare based on information that was once considered superfluous. This *datafication* of individuals leads to the virtual disassemby and reassembly of individuals, creating what

---

[41] Michel Foucault and Alan Sheridan, *Discipline and Punish* (Vintage Books, 1995). 204

[42] Maša Galič, Tjerk Timan, and Bert-Jaap Koops, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation', *Philosophy & Technology* 30, no. 1 (1 March 2017): 9–37, https://doi.org/10.1007/s13347-016-0219-1.

[43] Richard V Ericson and Kevin D Haggerty, *The New Politics of Surveillance and Visibility*, Green College Thematic Lecture Series (Toronto; Buffalo: University of Toronto Press, 2006), 5.

Ericson and Haggerty refer to as *data-doubles*.[44] Though a data-double is not a replication of the individual, decisions are made about that person by governments, insurance companies, hospitals, and many other sectors of society as if they were.

A constant theme in surveillance literature is how these decisions often, and repeatedly disadvantage marginalized peoples. Lyon details how the NSA disproportionately violates the informational sovereignty of the global south.[45] Crosby and Monaghan describe the use of surveillance to enforce colonial norms in the face of the Idle No More movement in Canada, with the Canadian state referring to the non-violent protestors as *Aboriginal extremists* to justify their surveillance.[46] Garfinkle points out that CCTV use in the UK has been disproportionately used to watch young African American males.[47] Likewise, consumer surveillance is used increasingly to drive decisions about where stores should be located, often moving away from impoverished neighbourhoods that need them.[48] Surveillance has been used to affect people's ability to get a mortgage, bank loan, or insurance for reasons such as economics, race, sexual orientation, or religion.[49] Clearly, surveillance exacerbates marginalization, yet the ways in which this marginalization extends to surveillance in the electoral context is underexplored by the literature.

Gary Marx argues that the last decades have seen a disturbing surveillance creep, in which softer methods of surveillance are transplanting traditionally hard surveillance

---

[44] Ibid.
[45] Lyon, *Surveillance after Snowden*. 57
[46] Andrew Crosby and Jeffrey Monaghan, 'Settler Colonialism and the Policing of Idle No More', *Social Justice* 43, no. 2 (144) (2016): 37–57.
[47] Garfinkel, *Database Nation*.116
[48] David Lyon, 'Why Where You Are Matters: Mundane Mobilities, Transparent Technologies, and Digital Discrimination', in *Surveillance and Security*, accessed 22 January 2019, https://www-igi-global-com.ezproxy.library.uvic.ca/chapter/you-matters-mundane-mobilities-transparent/48353.
[49] Rule, *Privacy in Peril*.

methods utilized by states, such as arrest and detention. Softer surveillance tactics have increased what Marx refers to as *mandatory volunteerism*, in which individuals are expected to submit to an expansive surveillance apparatus to function as a member of society.[50] While some may mask their identity on a day-to-day basis via gloves, facemasks, or CCTV disrupting glasses, individuals are *expected* to willingly have their autonomy violated by the ever-expanding normalization of intrusive surveillance tools.

While individuals are facing the increased pressures of mandatory volunteerism, the rise of social media and personal cellphones has fundamentally altered societies' relationship with surveillance. As governments have become increasingly engaged with data collection on their citizenry, so too have corporate entities. Shoshana Zuboff has termed this phenomenon *Surveillance Capitalism*, which she describes as a new form of capitalism that "aims to predict and modify human behaviour as a means to produce revenue and market control."[51] This model of capitalism, as defined by Zuboff, is what privacy scholars like Schwartz hoped to prevent, because, "information processing coerces decision-making when it undermines an individual's ability to make choices about participation in social and political life."[52] Unlike previous forms of corporate surveillance, such as those used by credit reporting agencies or insurance companies, this form of surveillance is omnipresent, fueled by a business model that aims to addict people to their product and views the individual's personal information as capital.

---

[50] Gary Marx, 'Surveillance and Society', in *Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information* (New York: Routledge), 37–53, accessed 10 December 2018, http://web.mit.edu/gtmarx/www/softsurveillance.html.

[51] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', *Journal of Information Technology* 30, no. 1 (March 2015): 75, https://doi.org/10.1057/jit.2015.5.

[52] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace', *Vanderbilt Law Review* 52, no. 6 (1 November 1999): 17.

Businesses operating in the platform economy, [53] such as Google or Facebook excel at capturing personal information and are shameless about their violation of privacy norms. In 2009, Eric Schmidt, the Chairperson of Google stated: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time …"[54] Mark Zuckerberg, CEO of Facebook shared similar sentiments, in which he argued that privacy is detrimental to a better world, "If people share more, the world will become more open and connected. And a world that's more open and connected is a better world."[55] The consequences of such a business model on an individual's privacy are notable.

The processing of personal information by these companies is done to target personalized advertisements to users. These companies gain their value from *big data.* By processing large quantities of data, algorithms detect latent patterns which the company can then utilize for advertising. By increasing the addictiveness of their product, these companies increase the time spent using their products and thus increase the amount of data generated by users. The results of this increased stimuli mean that the average smartphone user checks their phone every 12 minutes.[56] The user analytics generated can include revealing information such as what products people look for, what people buy, and even what people may think. Zuboff describes the result of this process as *The Big*

---

[53] For a more indepth analysis of Platform economies look at John Bruner's *Platform Economies*
[54] Schmidt Quoted in Zuboff, 2015, 80
[55] Zuckerberg quoted in Michael Zimmer, 'Mark Zuckerberg's Theory of Privacy', Washington Post, 3 February 2014, https://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html.
[56] 'Communications Market Report' (Ofcom, 2 August 2018), https://www.ofcom.org.uk/__data/assets/pdf_file/0022/117256/CMR-2018-narrative-report.pdf.

*Other, "*It is a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit."[57] In the process of gathering PII, these companies are further contributing to and exacerbating the propagation of data-doubles. Citizens become "a data source capable of being parsed, scanned, assessed, and monetized by other, invasive interests."[58] Moreover, this entire process alters peoples' relationships with the world, as it is designed to modify and predict behaviour.

Reviewing the literature on surveillance demonstrates a critical trend. Technological advances are making surveillance of the population easier, but it is not merely because there is more data to collect. Citizens have become increasingly accepting of practices, such as tracking devices, wiretaps and satellite surveillance, that were once considered to be the most egregious forms of privacy violations.[59] Rather than allowing these practices because of security or personal safety, many of these social changes (e.g., Google continually tracking the movement of people who use their operating system) have been made for the sake of convenience.[60] This *participatory surveillance* was described by Whitaker as a decentralized and consensual panopticon, leading him to suggest that the new model of surveillance is a *participatory panopticon*.[61]

---

[57] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', *Journal of Information Technology* 30, no. 1 (March 2015): 82, https://doi.org/10.1057/jit.2015.5.

[58] Jacob Silverman, 'Privacy under Surveillance Capitalism', *Social Research: An International Quarterly* 84, no. 1 (19 May 2017): 149.

[59] Marx, 'Surveillance and Society'. 34

[60] Sarah Perez, 'Google's CEO Thinks Android Users Know How Much Their Phones Are Tracking Them', *TechCrunch* (blog), accessed 21 December 2018, http://social.techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them/.

[61] Whitaker, Reginald. The End of Privacy: How Total Surveillance is Becoming a Reality. New York: New Press, 1999. 139

Various agencies and corporations engage in surveillance practices. Agencies such as the NSA, FBI, CSIS, IRS, and CSE may have considerable power regarding the control of the surveillance state, but other actors such as municipalities, provincial governments, insurance companies, advertising agencies, internet service providers and indeed political parties, also contribute to a constant surveillance of the public. Collection of this information creates what Whitaker calls "a system of surveillance more pervasive than that imagined by Orwell."[62] Moreover, citizens no longer need to be suspected of a crime to be subject to legal surveillance. It has become a phenomenon that has seeped into nearly every aspect of daily life. Davies suggests the future of privacy is much less of an Orwellian *Big Brother* and much more like Aldus Huxley's *Brave New World.* [63] Daniel Solove argues that the implications of this are a Kafkaesque world where individuals, unaware of the scope of surveillance, have no meaningful way to control the process.[64] Together, these works demonstrate an important trend, surveillance has become ubiquitous, normalized, and accepted in much of modern society.[65]

Despite the extensive work detailing the expanding surveillance state, and the conditions that facilitated its rise, there is again little focus paid to surveillance in the electoral context. Theories of surveillance have tended to evaluate the system as it affects consumers and criminalized or marginalized peoples, but has failed to assess the impact of voter surveillance on the democratic system. Furthermore, large sections of the

---

[62] Whitaker, The End of Privacy, 140

[63] Simon Davies, '13. Spanners in the Works: How the Privacy Movement Is Adapting to the Challenge of Big Brother', in *Visions of Privacy*, ed. Colin J. Bennett and Rebecca Grant (Toronto: University of Toronto Press, 1999), https://doi.org/10.3138/9781442683105-015. 245

[64] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, Ex Machina (New York: New York University Press, 2004).

[65] Andrejevic, 'Ubiquitous Surveillance'.

surveillance literature have not evaluated the effects of discriminatory electoral targeting on democracy. Looking through the indices of some of the most prominent works on surveillance for the terms *micro-targeting, voter surveillance, voter list, elections, political parties, and political targeting* reveals there have been very limited analysis of these subjects. Gandy dedicates some time to critique the rise of early voter-targeting systems in the *Panoptic Sort.*[66] Rule mentions voter lists in passing.[67] *Protecting Privacy in Surveillance Societies* by Flaherty does take note of electoral registers in France, and *Surveillance After Snowden* mentions the potential negative impacts of targeted voter systems, but there has been a limited critique of their use. Many other prolific works in surveillance studies entirely neglect the subject, suggesting that overall, the nature and effects of electoral surveillance, by and for political actors, remain largely unexplored.

Surveillance, Privacy & A Democratic State

It is clear, however, that on a theoretical level, despite the ubiquity of modern surveillance, privacy is an essential component of the democratic process, such that the deprivation of an individual's privacy erodes the foundations of the democratic system. Surveillance undermines many aspects of privacy, broadly grouped as *Self-discovery, Accountability, Erosion, and Bias Enforcement,* necessary for a functioning democratic state.

---

[66] Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Critical Studies in Communication and in the Cultural Industries (Boulder, Colo: Westview, 1993), 89.

[67] James B. Rule, *Private Lives and Public Surveillance: Social Control in the Computer Age*, 1st Schocken ed (New York: Schocken Books, 1973), 145.

Self Discovery: The division between political and apolitical enhances the space for individuals to grow as citizens and critically engage with, and think about dissident ideas and concepts. This space is a necessary element of an engaged democratic society. Westin states that all democratic societies function with the belief in the uniqueness of the individual and that individuals, in turn, seek to protect the sacredness of their individuality.[68] "The democratic society relies on publicity as a control over government, and privacy as a shield for group and individual life."[69] The state has the responsibility of balancing the harm that can be caused by violating the privacy of the individual and protecting the functionality of society as a whole. Gavison further suggests that without independent thinking, an individual is unable to develop a moral autonomy, without which participation in a deliberative decision-making process is not possible.[70]

When individuals lack control of their information, it hinders their ability to grow.[71] Boehme-Neßler suggests that democracy thrives in a society that respects privacy. Individuals are free to find dissident information and hold dissident beliefs; without this privacy, the state slides into a despotic regime.[72] Nick Couldry likewise suggests that the growth of the surveillance state, in combination with the proliferation of big data analysis, has the potential to undermine the decision-making capacity of a democratic citizen.[73]

---

[68] Westin, 1967, 33
[69] Westin, *Privacy and Freedom*.
[70] Ruth Gavison, 'Privacy and the Limits of Law', *The Yale Law Journal* 89, no. 3 (1980): 450, https://doi.org/10.2307/795891.
[71] Volker Boehme-Neßler, 'Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection', *International Data Privacy Law* 6, no. 3 (1 August 2016): 222–29, https://doi.org/10.1093/idpl/ipw007.
[72] Boehme-Neßler, 2016. 227
[73] Nick Couldry, 'Surveillance-Democracy', *Journal of Information Technology & Politics* 14, no. 2 (3 April 2017): 182–88, https://doi.org/10.1080/19331681.2017.1309310.

Accountability: Wayland and Johnson suggest that surveillance undermines the accountability of a democratic system.[74] Democracy works through systems of checks and balances, but surveillance undermines this process by using PII to maximize power. Modern surveillance may range from being insidious to being comforting for many citizens, but the power-imbalance stemming from surveillance reduces government accountability. Haggerty argues "democratic societies are constituted, in part, by systems of accountability, systems in which individuals and institutions are held to standards of behaviour and expected to explain failures to conform to those standards."[75] Mass surveillance alters this dichotomy. When the state has intimate knowledge of what its citizens are doing, and does not share this transparency, democracy is in a precarious position. Gavison likewise agrees that privacy-imbalances exacerbates unequal power structures, which undermines the democratic rights of the citizen,[76] and thus undermines the democratic institution.

Erosion: Haggerty and Samatas suggest that the relationship between surveillance and democracy is one of erosion. They believe that surveillance erodes social norms, rights and freedoms, and trust in the institutions of power.[77] Despite these erosions, it is difficult to find a modern democracy that can escape the definition of a surveillance society. Though the contemporary surveillance state is not necessarily fascist, the mass collection of information and increased transparency does have the potential to erode a citizen's willingness to exercise their civic rights and engage in free speech out of fear of

---

[74] Kevin D. Haggerty and Minas Samatas, *Surveillance and Democracy* (London, UNITED KINGDOM: Taylor & Francis Group, 2010), http://ebookcentral.proquest.com/lib/uvic/detail.action?docID=537878. 21
[75] ibid 21
[76] Gavison, 1980. 426
[77] Haggerty and Samatas. 2010, 21

persecution.[78] Without protection against mass surveillance, a nation can quietly transform into an authoritarian state.[79]

Bias enforcement: Surveillance can also disrupt the democratic process by creating informational narrowcasting - the result of tailoring messages based on perceived trends revealed through data analytics. Sunstein also suggests that surveillance can disrupt the democratic process when the market principles of data analysis apply to democracy. Politicians or campaigns can recognize these trends and try to maximize their message by replicating popular patterns, resulting in policies, talking points, and news informed by a highly polarized segment of the population, tending towards the fringes.[80] This topic resonates with Zuboff's theory of surveillance capitalism; as SNS try to increase user's engagement with their platforms, they tailor information to improve ease of use and access. Google, Facebook and Twitter prioritize information based on what their algorithm has determined to be the most relevant to the user.[81] Eli Praiser explored the topic of filter bubbles extensively and suggested that SNS's such as Facebook have usurped the traditional role of the media. As a result, people are exposed to less information contrary to the SNS algorithm's definition of their opinions.[82] Bozdag believes that this algorithmic bias undermines the freedom of choice principle, and the

[78] ibid

[79] The total number of democratic states in the world has continued to rise, however the quality of these democratic states has been falling. Only 12% of countries surveyed by the Economist Intelligence Unit's Democracy Index constituted full democracies; 32.9% are flawed democracies, 23.4% are hybrid Regimes, and 31.7% are authoritarian regimes. Likewise Freedom House's Freedom in the world index marked 2017 as the 12th consequitive year of a global decline in freedom. From: Michael J. Abramowwitz, 'Freedom in the World 2018', Freedom House, 13 January 2018, https://freedomhouse.org/report/freedom-world/freedom-world-2018.

[80] Sunstein, Cass R. Republic.Com. Princeton, N.J: Princeton University Press, 2001.

[81] Eli Pariser, *The Filter Bubble* (Penguin Press, 2011).

[82] ibid.

deliberative decision-making process necessary in a liberal democracy.[83] This theory would suggest that people will become entrenched in their views, rendering a constructive political discourse unfeasible.

Privacy and thus protection against surveillance play an essential role in the democratic process. The failure to maintain institutions of good governance, such as political participation, political culture, civil liberties, and the sanctity of the electoral process will rapidly decay the efficacy of the democratic system.[84] Democracy thrives when the individual has sufficient privacy to formulate independent thinking and build conceptions of who they are as a person. [85] Without protection against over-bearing surveillance, citizens are less able to hold their institutions of government to account. Moreover, the increased polarization resulting from surveillance erodes public discourse.

Though these are pressing and concerning issues, scholars have generally viewed this as mainly a democratic issue, but not an electoral issue. Anti-surveillance arguments for the democratic importance of privacy fail to recognize the scope of PII collection and processing within the electoral process. The information collected from various forms of surveillance contribute data to the electoral ecosystem, and this information is used to target voters and distort their perception of political elites. Voter surveillance further complicates these critiques because political parties do require some degree of information to fulfil their functions in a democratic system.

---

[83] Engin Bozdag and Jeroen van den Hoven, 'Breaking the Filter Bubble: Democracy and Design', *Ethics and Information Technology* 17, no. 4 (1 December 2015): 249, https://doi.org/10.1007/s10676-015-9380-y.
[84] 'The Retreat of Global Democracy Stopped in 2018', *The Economist,* 8 January 2019, https://www.economist.com/graphic-detail/2019/01/08/the-retreat-of-global-democracy-stopped-in-2018.
[85] Westin, *Privacy and Freedom*. 24

Political Parties: Democratic Enhancements and Detriments

Political parties operate within a special status in our society as intermediaries between the public and the government. Sartori suggests seven primary functions of political parties including the ability to encourage electoral participation, introduce policy suggestions, and manage various cleavages within the electorate into a cohesive political block. [86] To accomplish these functions, parties must be well acquainted with the needs and desires of citizens. They would not be able to perform their functions without some information on the opinions and desires of the electorate.[87] However, the last decade has seen increased attention on this phenomenon, in part due to the rise of microtargeting. Though Delacourt points out that parties have been collecting databases on their citizens for decades.[88] Behavioural microtargeting arose as a technique used by marketing agencies who combined online activity with consumer habits to tailor advertising to individuals based on their modelled information.[89]

Parties have thus begun the process of "shopping for votes" by identifying citizens in key ridings and trying to win them over with granular messaging.[90] This process is facilitated by mass data collection based on the belief that doing so will result

[86] Giovanni Sartori, 'Party Types, Organisation and Functions', *West European Politics* 28, no. 1 (1 January 2005): 23, https://doi.org/10.1080/0140238042000334268.
[87] Bernard Caillaud and Jean Tirole, 'Parties as Political Intermediaries', *The Quarterly Journal of Economics* 117, no. 4 (November 2002): 1453–89.
[88] Delacourt, Susan, Shopping for Votes: How Politicians Choose Us and we Choose them. Madeira Park, BC: Douglas & McIntyre, 2013.
[89] Tom Dobber et al., 'Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques', *Internet Policy Review* Volume 6, no. Issue 4 (1 December 2017), https://doaj.org.
[90] Susan Delacourt, *Shopping for Votes: How Politicians Choose Us and We Choose Them*, Updated second edition (Madeira Park, BC, Canada: Douglas & McIntyre, 2016).

in more electoral wins.[9192] There is some credibility to this claim. Kreiss believes that advances in voter targeting may be responsible for the Democratic Party's success from 2004-2012. US practices are beginning to spread worldwide, as techniques created in the US for voter targeting find their way into other countries, resulting in a proliferation of 'slicing and dicing' the electorates in many countries around the world.

There has been an intellectual rift between analytical and experiential evidence regarding the efficacy of political campaign data. Murray and Scime found that data mining can predict vote preferences with 66% accuracy.[93] Yet others, such as Hersh, suggests that these methods are far less effective than this, and ultimately only contribute to creating a digital representation that has little in common with the human being they are meant to represent.[94] Baldwin-Phillipi describes this rift as the *Myth of Big data*, which exaggerates the capabilities of data analysis.[95] Despite that, in the US, these voter management systems continue to be built with limited regard for the privacy implications.[96] Largely anecdotal evidence has convinced industry insiders that micro-targeting is how to win elections.

As a result, the last decade has seen an increase in voter surveillance. Though comprehensive data-protection legislation limits the collection of PII by political parties

---

[91] Eitan D. Hersh, *Hacking the Electorate: How Campaigns Perceive Voters* (Cambridge: Cambridge University Press, 2015), https://doi.org/10.1017/CBO9781316212783.
[92] Ira Rubinstein, 'Voter Privacy in the Age of Big Data', *SSRN Electronic Journal*, 2014, https://doi.org/10.2139/ssrn.2447956.
[93] Gregg Murray and Anthony Scime, 'Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies', *Journal of Political Marketing* 9, no. 3 (July 2010): 143, https://doi.org/10.1080/15377857.2010.497732.
[94] Hersh, *Hacking the Electorate: How Campaigns Perceive Voters 2015*.
[95] Jessica Baldwin-Philippi, 'The Myths of Data-Driven Campaigning', *Political Communication* 34, no. 4 (2 October 2017): 627–33, https://doi.org/10.1080/10584609.2017.1372999.
[96] Rubinstein, 'Voter Privacy in the Age of Big Data'.897

in many countries, similar legislation does not exist federally in Canada or the US.[97] In the US, this lack of regulation has resulted in parties building massive databases on voters. Bennett has identified four trends common in voter surveillance in western democracies.[98] In addition to the rise of microtargeting, political parties have also moved from voter management databases to integrated voter management platforms; increasingly they rely on commercial brokerage firms for data; and have intensified the use of social media analysis.[99] Bennett argues that this process has numerous potential adverse effects on the democratic process, including undermining national cohesion and dividing the population. Rather than proposing a general framework of governance, political parties offer focus-group tested messaging to critical segments of the population in swing ridings.[100]

These systems of voter surveillance have primarily been examined from a political marketing perspective by scholars like Hersh, Dobber, or Kreiss. Other scholars such as Murray and Scime have engaged in debate outlining the merits of micro-targeting,[101] while others like Barocas have critiqued its ethics.[102] Journalists such as Issenberg or Delacourt have also conducted impressive work charting the voter surveillance ecosystem in the US and Canada while seeking to understand how politicians use these databases, and what they believe they will accomplish.[103] This

---

[97] "Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations," Canadian Journal of Law and Technology, Vol 16, No 2 (November 2018); 195-226

[98] Bennett, 'Trends in Voter Surveillance in Western Societies'.

[99] Bennett. Trends In Voter Surveillance, 372.

[100] Bennett, 'Trends in Voter Surveillance in Western Societies'. Trends In Voter Surveillance, 381

[101] Murray and Scime, 'Microtargeting and Electorate Segmentation'.

[102] Barocas, 'The Price of Precision'.

[103] Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns*, First paperback edition (New York: B/D/W/Y, Broadway Books, 2013).

overview demonstrates that there has been some analytical focus on micro-targeting and political party data use, but the literature has largely failed to analyze this through the lens of surveillance.

Conclusion

The erosion of democratic values posed by voter surveillance is an underexplored aspect of the privacy, surveillance, and political marketing literature. Privacy is a value that transcends borders and cultures, and there are many ways a violation of privacy can occur, though many of the definitions and categories hinge on the notions of either autonomy or control. However, voters have a limited understanding of the collection of their information and in many ways have limited control over their data.[104] Mass surveillance erodes the institutions of democracy, but political parties must collect some data to engage with, and mobilize the electorate. Thus, democracies around the world must decide how to balance the benefits of voter surveillance against the privacy rights of their constituents. The exploration of this issue is complicated because little of the literature exploring voter databases and the political data ecosystem focuses on the privacy implications of voter surveillance.

Voter surveillance, as conducted by CA, may undermine the institutions of a democratic society, and yet political parties also have a responsibility to understand and know voters. Many of the functions of a political party suggested by Sartori do require a degree of information about the electorate, but this chapter has also indicated that there is a surveillance creep in data collection by political parties, who are becoming increasingly

[104] Bennett, Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations," 4

reliant on personal information. Some tactics of voter surveillance, such as micro-targeting, have a potentially chilling effect on democratic engagement. Barocas noted that, "collecting information about core personal beliefs and associations—or trying to predict these facts—without the consent of voters is likely to have a chilling effect on both public involvement in explicitly political activities and those activities that have been revealed to be highly correlated with political commitments."[105] Bennett argues that voter surveillance is *Janus-faced*, in that it "requires us to analyze and judge its complex dynamics according to a different set of criteria than those used when we evaluate the security practices of the state, or the profit-driven consumer monitoring by the private sector."[106] The practice of voter surveillance had remained relatively unchallenged for decades before CA stirred public outrage. So what was it about this company that captured the public's attention in such a massive way?

[105] Barocas, 'The Price of Precision'. 34
[106] Bennett, 'Trends in Voter Surveillance in Western Societies', 383.

Chapter 2: America's Voter Analytics Industry

Understanding why CA was so contentious is only possible in the context of the electoral environment in which it was competing. Political parties have operated under the assumption that additional PII on their voters will provide electoral gains.[107] They are not alone in this belief, almost all sectors of modern surveillance societies believe that more data means improved targeting.[108] Regardless of its effectiveness, voter surveillance has increased, and it has become ubiquitous within recent US elections.[109] CA's tactics were thus not out of the norm, but a slight deviation from industry standards in the US.[110]

This chapter will detail the competitive nature of the voter analytics industry, and the surveillance capabilities that existed at the time CA entered the scene. Doing so will demonstrate that CA was one of many Republican-leaning firms, albeit an ethically dubious one, that arose to counter a perceived data deficit. This chapter argues that CA was not practicing novel voter surveillance or micro-targeting methods. Rather, Trump's connections to the new *Alt-right* movement helped draw attention to practices that had been built up over the last decade. Thus, CA became the embodiment of the larger set of problems associated with voter surveillance.

---

[107] Bennett, 'Trends in Voter Surveillance in Western Societies'.

[108] Mark Andrejevic, 'Ubiquitous Surveillance', in *Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball, Kevin D. Haggerty, and David Lyon 1948, Book, Whole (New York;Abingdon, Oxon; Routledge, 2012), 91–99,

[109] Bennett, 'Trends in Voter Surveillance in Western Societies'.

[110] However, I did not research Cambridge Analytica's allegedly illegal or immoral activities in other countries, the purpose of this chapter is only to examine CA's voter surveillance in the United States compared to that of its contemporaries.

Voter Surveillance in the United States

In 2012, the Republicans were disadvantaged by the Democratic party's data operation.[111] The Obama campaign's *Project Narwhale* and their revolutionary approach to using Facebook meant that their campaign had access to the most integrated political database in US politics, populated with the social relationships of almost every single US citizen.[112] During the 2012 election post-mortem, which Kreiss describes as "a collective process of meaning-making in which [the] party … strategically vie to define the reason for victories and losses," [113] the Republicans decided to pivot their electoral strategy to a data-reliant approach, something Kreiss points out the Republicans largely failed to do in 2008.

Their oversight resulted in the rushed creation of the 2012 database *Project Orca*, which fell short of the Republicans' expectations.[114] As a result, The Republicans' data operation was inferior to that of the Democratic party in the 2012 election. Narwhale was far from perfect, but it did allow the campaign to match data between databases, a revolution for the time.[115] The Obama campaign employed 28 staffers with technology or data analytics experience compared to Romney's one analyst.[116] Though Republicans did increase data-collection during Romney's 2012 campaign, his team failed to consolidate this information with robust data-analytics and modelling strategies. These factors

---

[111] Daniel Kreiss, *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*, Oxford Studies in Digital Politics (New York, NY: Oxford University Press, 2016).
[112] Sasha Issenberg, 'How the Obama Campaign's Top-Secret Project Narwhal Will Change the 2012 Race', Slate Magazine, 15 February 2012, https://slate.com/news-and-politics/2012/02/project-narwhal-how-a-top-secret-obama-campaign-program-could-change-the-2012-race.html.
[113] Kreiss, *Prototype Politics.* 15
[114] Brett LoGiurato, 'Mitt Romney Has A New Strategy To Dominate The Facebook Campaign Wars', Business Insider, June 18, 2012 https://www.businessinsider.com/mitt-romney-campaign-facebook-social-media-zac-moffatt-barack-obama-2012-6.
[115] Kreiss, *Prototype Politics.* 136
[116] Kreiss, *Prototype Politics,*, 11

propagated the narrative that Obama won because of better data, and invigorated an industry focused on creating effective data-integration systems for electoral use, though the campaign's innovative use of Facebook to micro-target voters further fostered this narrative.[117] The Democrats' possession of an integrated database created a perceived strategic disadvantage for the GOP, a problem cited by Alexander Nix, former CEO of Cambridge Analytica, during his testimony to the DCMS on February 27, 2018.[118]

The Republicans believed that PII was needed to effectively engage the electorate and propose issues that resonate with voters.[119] However, in an unregulated and high-stakes election, this data collection can quickly escalate. Nix argued that his company's use of data-analytics was no different from that which the Obama campaign utilized in 2012, "That is an entire industry that is moving in this direction. It is not Cambridge Analytica."[120] It was this perceived threat that led the Republicans to expand the scope of their data collection.

Political Marketing in the US

In the early 2000s, political parties did not have the resources to support the long-term investment necessary to stay up-to-date on data innovation, and so they outsourced their data storage, analysis, and modelling to third-party vendors.[121] Indeed, the system of US voter surveillance now entails numerous companies competing to win the business of

---

[117] An aspect of this conflict which Chapter 3 examines.

[118] Alexander Nix, 'Oral Evi dence: Fake News, HC 363', Pub. L. No. 363, § Digital, Culture, Media and Sport Committee, 1 (2018), Q658 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/79388.pdf.

[119] Sartori, 'Party Types, Organisation and Functions'.

[120] Nix, 'Oral Evidence: Fake News, HC 363', Q658.

[121] Sasha Issenberg and Joshua Green, 'Why the Trump Machine Is Built to Last Beyond the Election', Bloomberg, 27 October 2016, https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go.

political parties and candidates.[122] These companies quickly became partisan aligned, with firms like Catalist, Blue State Digital, and the Voter Action Network only providing assistance to the Democratic Party.[123] And other groups such as Target Victory, i360, Deep Root Analytics, and Outlaw Media aligned with the Republican Party.[124]

Voter Surveillance in the US is greatly assisted by the Help America Vote Act (HAVA), which requires every state to maintain up-to-date and precise voter files on their populations.[125] Data brokers enhance these files by combining them with an array of other consumer files, a process that the Federal Trade Commission (FTC) critiqued in 2014 for its lack of transparency and accountability. The FTC report studied nine brokers and found that many of these data brokers swapped data with each other, "accordingly, it would be virtually impossible for a consumer to determine how a data broker obtained his or her data."[126] Many of these data brokers are trading information about people with whom they have no relationship, a process made possible because most people do not read the privacy policies to which they agree. In this system, getting properly informed consent from voters and accountability from the brokers is nearly impossible. However, in the US, voter surveillance remains almost entirely devoid of legal oversight or regulation.

Barocas notes that *Aristotle*, one prominent data broker, "maintains and sells records on 157 million American voter files that contain each voter's registration data as

---

[122] Bennett, 'Trends in Voter Surveillance in Western Societies'. 371
[123] Ibid. 86
[124] Kreiss, *Prototype Politics*, 12.

[125] Barocas, 'The Price of Precision'. 32
[126] 'Data Brokers: A Call for Transparency and Accountability' (Federal Trade Comission, May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

well as their ethnicity, occupation, education, homeowner status, income level, whether they are catalogue shoppers, and whether they have a history of making charitable or political donations."[127] Though the specifics are unknown, there are between 300-900 points of data in every person's voter file, and more recently the proliferation of tracking cookies has made it possible to match roughly 80% of a voter's online activity with their offline data points. *Acxiom*, a major data broker who provided data to CA, claims to have a database that holds information on "age, race, sex, weight, height, marital status, education level, politics, buying habits, household health concerns, vacation dreams, etc., averaging around 1500 data points per person."[128] If there is a point of information that these brokers can collect, it is likely for sale.

Political marketing firms then buy this data and use it to target consumers and voters. One such company is *Blue State Digital*, founded by former staffers of the Howard Dean presidential campaign. After working on the 2008 and 2012 Obama campaigns, *Blue State Digital* branched out to offer services to non-profits and businesses that align with their progressive goals. They provide products that facilitate form-building, email and SMS optimization, voter management systems, data optimization, fundraising, and social media outreach.[129] *Catalist* offers voter PII on 240 million citizens, and includes information such as: household attributes, voting history, purchase history, civic group membership, census data, community group membership, investment history, geographic data, social media data, occupational information, and recreational

---

[127] Ibid.

[128] Leanne Roderick, 'Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry', *Critical Sociology* 40, no. 5 (1 September 2014): 730, https://doi.org/10.1177/0896920513501350.

[129] 'Community Mobilization and Fundraising Platform | BSD Tools |', Blue State Digital, accessed 9 May 2019, https://tools.bluestatedigital.com/.

interests. *Catalist* partners with numerous other progressive firms such as *NPG Van, BlueLabs, Periscope data, Civis Analytics, Action Kit, Voter Circle, and Political Data Inc*., to provide the most up-to-date and integrated voter profiles available to progressive candidates, businesses, and NGOs. *DSPolitical* enhances *Catalist* voter files by matching it with over 600 million browser cookies and mobile devices to identify voters online.[130] They also provide tracking of early voters to allow campaigns to target their messaging better, as seen in Figure 2.1 from *DSPolitical's* marketing material. [131]

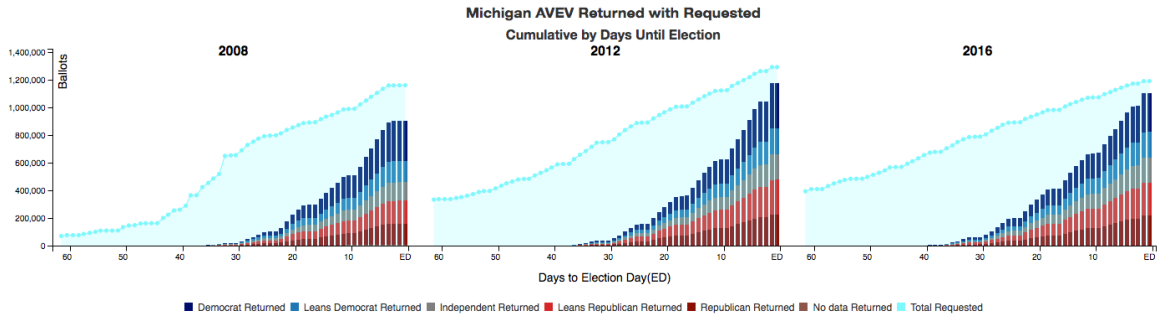

Figure 2.1: A figure representing *DSPolitical*'s ability to track early voting trends in Michigan.

The number of companies working specifically for the Democratic party meant tht the Democrats had an eight-year lead over the GOP in collecting, assembling and modelling private information to surveil and target voters. This advantage led the GOP to believe they needed to update their technological capabilities quickly. Two significant proprietors of enhanced voter files arose in the last decade to work with Republican candidates. One of them, *i360*, a Koch-brothers owned company, provides voter-profiles

[130] 'Reaching Voters', DSPolitical, accessed 9 May 2019, https://www.dspolitical.com/services/reaching-voters/.
[131] 'Reaching Voters'.

with innovative interfaces allowing for actionable data.[132] The *Database* page on their website boasts about their access to 199 million US voter files, 290 million consumer files, and up to 1800 points of data on every US citizen including categories of data such as: charitable donations, number of children, registration status, newspaper subscriptions, political donation history, gambling habits, social media usage, propensity to vote, interest in camping, investment history, persuadability, partisanship, content streaming habits, military service record, and religion. It also included medical information such as if the voter has arthreitis, osteoperosis, alzheimers, high blood pressure, allergies, asthma, high cholesterol, or bladder control issues.[133] The quality and quantity of PII offered in these databases is an alarming invasion of privacy, and yet remains unchallenged by the public.

The Republican National Committee (RNC) controls the second source of Republican data. We have some insight into the types of information the RNC collected in the 2016 election. In 2018, cyber risk researcher Chris Vickery discovered an unsecured *Amazon Web Services S3 bucket* containing 198 million voter files.[134] This breach was the second time that Vickery had found a Republican voter file. At the ETHI Committee on April 17, 2018, he revealed that between 2015 and 2017 the RNC had significantly enhanced their data.[135] In total, 99% of the US voting public's files were contained in this repository, and Vickery's analysis provides insight into the RNC's data operation. Vickery discovered that the RNC had modelled voter's opinions on issues such

---

[132] Allen, Mike, and Kenneth P. Vogel. "Inside the Koch Data Mine." POLITICO. December 08, 2014. Accessed February 05, 2019. https://www.politico.com/story/2014/12/koch-brothers-rnc-113359.

[133] 'The Database', i360, accessed 20 February 2019, https://www.i-360.com/the-database/.

[134] Dan O'Sullivan, 'The RNC Files: Inside the Largest US Voter Data Leak', UpGuard, 12 December 2018, https://www.upguard.com/breaches/the-rnc-files.

[135] Chris Vickery, 'Breach of Personal Information Involving Cambridge Analytica', Pub. L. No. 123, § Standing Committee on Access to Information, Privacy, and Ethics (2018). 0850

as: America first, cross partisan work, low taxes, exportation of jobs, support for Trump, healthcare, immigration, infrastructure investment, environmental protection, and optimism about the US' financial future. These opinions were modelled based on data categories such as a voter's: name, age, location, ethnicity, self reported demographic, state voter ID, gender, religion, what they post on Reddit, and if they are on the FTC do not call list.[136]

After *ORCA's* failure, Republican operatives worked to create an up-to-date, well-funded and integrated system. [137] The *i360* and RNC databases demonstrate that the US right-wing allocated significant energy and resources into populating and maintaining a massive voter surveillance operation on par with, if not surpassing, that of the Democratic Party.

This competitive and crowded field is the electoral context in which CA operated. Operatives were under the impression that more data equated with better electoral odds, and that digital solutions were how the Republicans would regain control in 2016.[138] Despite the scale of voter surveillance orchestrated by political parties, including the collection of sensitive medical information, the public remained largely unconcerned with, or more likely unaware of, this massive collection of personal data.

Cambridge Analytica: An Effective Sales Pitch

The electoral ecosystem in 2016 was crowded with numerous consultants and data-brokers each offering innovative "solutions" for electoral victory. At the beginning

[136] O'Sullivan, 'The RNC Files'.

[137] Kreiss, *Prototype Politics*. 165

[138] Ibid.

of the Republican primary, Ted Cruz had only a 40% name recognition, but with CA working for his campaign, he quickly rose to become the national Republican runner-up.[139] Nix stated that CA was unique in their field because of their use of psychographics, which he referred to as its "magic sauce,"[140] to target voters based on personality.[141]

In early 2016, reports arose about CA misrepresenting the efficacy of their product. Some Republican strategists suggested anonymously that CA did not effectively integrate into US politics and that they were unable to meet expectations. These complaints suggested that CA was competent at modelling and data analytics, but the company was more focused on sales and marketing than delivering a complete product.[142] CA's ineffectiveness prompted Ted Cruz's campaign to switch to another firm, *Targeted Victory*, to run advertising in the months leading up to the primary.[143] Moreover, after Trump's team hired CA, they determined that CA's data and models were less effective at targeting than the existing RNC systems.[144] [145]

Robert Mercer is one of the reasons that negative press about CA was largely absent within Republican circles in 2016. Mercer is a multi-billionaire who has quietly integrated himself into right-wing politics; in addition to running a successful hedge fund,

---

[139] Cambridge Analytica - The Power of Big Data and Psychographics. September 27, 2016. Accessed October 27, 2018. https://www.youtube.com/watch?v=n8Dd5aVXLCc.

[140] Nix term used to describe CA's psychographic profiles modelled using Facebook'likes' data.

[141] Cambridge Analytica - The Power of Big Data and Psychographics. September 27, 2016. Accessed October 27, 2018. https://www.youtube.com/watch?v=n8Dd5aVXLCc..

[142] Kate Kaye, 'In D.C., Cambridge Analytica Not Exactly Toast of the Town', Ad Age, 18 August 2016, https://adage.com/article/campaign-trail/cambridge-analytica-toast/305439/.

[143] Kaye.

[144] Nicholas Confessore and Danny Hakim, 'Data Firm Says "Secret Sauce" Aided Trump; Many Scoff', *The New York Times*, 20 January 2018, sec. U.S., https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html.

[145] Kate Kaye, 'How the Trump Camp's Data Inexperience Helped Propel His Win', AdAge, 14 December 2016, https://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/.

and moonlighting as a part-time deputy in New Mexico, Mercer is a financial backer for Breitbart News and CA.[146] Mercer's political power on the right is rivalled by the Koch brothers,[147] and it has been suggested that he stifled early criticisms of CA.[148] With the brand-power associated with Mercer, CA was able to oversell their product, over-promise clients, and exaggerate the strength of their *psychographics* without criticism from the Republican mainstream.[149] In his testimony to the DCMS, Chris Wylie suggested that the psychographic targeting was an incomplete product during the Cruz campaign.[150]

CA's data was an integration of numerous types of PII. During *Meeting 109* of the ETHI Committee, Wylie stated, "clients would sometimes provide the company with information so that they would help that modelling process. In other cases, there would be a contractual relationship directly with a company—a data vendor that sells consumer data…"[151] When Nix was on the stage of *The Concordia Summit,* his powerpoint listed numerous companies, indicating the sources of their data. CA purchased the bulk of its data from brokers such as *Data Trust, L2, Infogroup, Aristotle, Acxiom, Experian, Neilsen, MRI, Magellian Strategies,* and *RIK Data Solutions*.[152]

Additional information about CA's data comes from Dr. David Carroll. In 2016, Carroll officially requested his own PII from CA. This information included Carroll's

---

[146] Zachary Milder, 'Robert Mercer's Secret Adventure as a New Mexico Cop', *Bloomberg,* 28 March 2018, https://www.bloomberg.com/news/features/2018-03-28/robert-mercer-s-secret-adventure-as-a-new-mexico-cop.

[147] Who financed the creation of i360.

[148] Kaye,'In D.C., Cambridge Analytica Not Exactly Toast of the Town'

[149] ibid.

[150] Chris Wylie, 'Fake News', § Digital, Culture, Media and Sport Committee (2018), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81022.html. Q1406

[151] Christopher Wylie, 'Breach of Personal Information Involving Cambridge Analytica and Facebook', § Standing Committee on Access to Information, Privacy and Ethics (ETHI) (2018), 0955 https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-109/minutes.

[152] Alexander Nix, 'Cambridge Analytica - The Power of Big Data and Psychographics' (September 2016), https://www.youtube.com/watch?v=n8Dd5aVXLCc&t=192s.

perceived opinions on various issues. CA could use these models, derived from various sources of data to microtarget advertising to Carroll based on the issues they determined to be most important to him. Based on Carroll's file, CA could target him with information about the national debt, and likely avoid advertisements about the protection of gun rights. However, Carroll is listed as *very unlikely Republican*, so he likely would not be targeted with information about Republican candidates. Additional modelling about Carroll is depicted in Figure 2.2.[153]

National Debt Importance Rank [1-10]	10
Gun Rights Importance Rank [1-10]	3
Traditional Social and Moral Values Importance Rank [1-10]	9
Environment Importance Rank [1-10]	5
Education Importance Rank [1-10]	4
National Security Importance Rank [1-10]	7
Immigration Importance Rank [1-10]	8
Socially Progressive Civil Rights Importance Rank [1-10]	6
Jobs and Economy Importance Rank [1-10]	1
Healthcare Importance Rank [1-10]	2
Registered Partisanship	Very Unlikely Republican
Unregistered Partisanship	Very Unlikely Republican
2016 General Election Turnout Propensity	Very High

Figure 2.2: A sample Cambridge Analytica's modelling of Carroll's opinions

Cambridge Analytica: The Trump Card

In June of 2016, Clinton was outspending Trump in key battleground states, and the Trump team was rapidly depleting their resources with no access to *i360* or the RNC databases.[154] The Trump campaign hired CA following a substantial investment by Robert Mercer, a donation contingent on the hire. According to an internal CA document,

[153] David Carroll, 'Just Got My Data from Cambridge Analytica/SCL by Request. Yes, They Do Have Correct Voter and Personal Information about Me. More to Come.', Twitter, *David Carroll Twitter* (blog), 27 March 2017, https://twitter.com/profcarroll/status/846347516341837825?lang=en.

[154] Sophia Tesfaye, 'NRA Props up Trump's Flailing Campaign with Multi-Million Dollar Benghazi-Themed Ad Buy', Salon, 29 June 2016, https://www.salon.com/2016/06/29/nra_props_up_trumps_flailing_campaign_with_multi_million_dollar_benghazi_themed_ad_buy/.

the campaign's data was disorganized and lacked modelling, and included five firms that were conducting polling.[155] Brittany Kaiser, a former CA employee, described the Trump campaign's digital advertising and modelling as lacking.[156][157] It was also reported that the Trump campaign was not effectively utilizing email fundraising until June 21, 2016, and 60% of the emails sent were directed to the recipient's spam boxes rather than being opened.[158] A leaked power-point presentation of CA's Trump strategy demonstrates how the firm claimed to target people with tailored advertisements using Google, Snapchat, Twitter, Facebook, Email, and TV,[159] although the effectiveness of this targeting is not known.

In 2017, Molly Schweickert, Head of Digital at CA, claimed that CA conducted large-scale survey research in battleground states to understand the mood and concerns of voters.[160] CA would then try to extrapolate the findings from these surveys and model them on top of voter files. CA also analyzed data based on payments, web conversion rates, and Google web analytics.[161] Schweickert describes this practice as novel, although Barocas notes that modelling user data based on surveys was common in political campaigning during the 2012 election cycle and that, without such modelling, the data is

---

[155] Paul Lewis and Paul Hilder, 'Leaked: Cambridge Analytica's Blueprint for Trump Victory', *The Guardian*, 23 March 2018, sec. UK news, https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

[156] Lewis and Hilder.

[157] Though it is important to note that Brittany Kaiser worked in the capacity of sales, not data analysis, and this internal document was used for the purposes of pitching clients, thus there is a possibility this is less than accurate.

[158] Kate Kaye, 'Trump's First Fundraising Email Had a 60% Spam Rate', Ad Age, 23 June 2016, https://adage.com/article/campaign-trail/trump-s-fundraising-email-a-60-spam-rate/304673.

[159] It should be noted the same article states that a Trump campaign insider suggests that CA greatly over promoted their involvement in the campaign.

[160] Molly Schweickert, 'How Digital Advertising Worked for the US 2016 Presidential Campaign' (12 May 2017), https://www.youtube.com/watch?v=bB2BJjMNXpA.

[161] Molly Schweickert.

useless.[162] Likewise, Issenberg discusses how a similar process was used to identify Bush supporters in 2004,[163] suggesting the CA's innovation was more rhetoric than factual. CA modelled three universes of voters, including: *Online*, in which online behaviour was linked to voter profiles by matching PII with cookies, social ID, and devices if possible; *Geographic*, in which regions were microtargeted by matching voter files to postal codes and addresses; and *Demographic*, where voters were targeted based on characteristic data.[164] These universes would be standard for any campaign in the US. Online universes would be based on analytics collected from basic web cookies. These cookies help campaigns determine what is most effective in an advertisement and which demographic is most suseptable to the ad. Geographic universes can be developed using voter profiles made possible through HAVA, and Demographic universes are easily created based on data collected from data brokers. The commonality of these tactics should not distract from the egregious scale of surveillance necessary to build and populate these databases.

CA was a capable data modeller and had access to a remarkable amount of data, though many of the practices that they highlight had in fact been industry standard since the previous election cycle. It also appears that much of CA's touted capabilities were exaggerated. This exaggeration is likely propagated by people such as Nix, Kaiser, and Schweickert potentially misrepresenting CA's product for the sake of improved sales, contributing to what Baldwin-Philippi argues is the myth of data-driven campaigning.[165] Despite the disconnect between capabilities and hyperbole, much of the scrutiny on CA

[162] Barocas, 'The Price of Precision'. 32
[163] Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campmoaigns*, First paperback edition (New York: B/D/W/Y, Broadway Books, 2013). 140
[164] Molly Schweickert, 'How Digital Advertising Worked for the US 2016 Presidential Campaign'.
[165] Baldwin-Philippi, 'The Myths of Data-Driven Campaigning'.

arose because of their work during the 2016 election; in which the media accused them of manipulating voters into voting for Trump using psychological tricks.[166]

Emotional Advertising

CA inaccurately claimed to be revolutionary in its ability to target people based on their underlying emotional disposition. Mark Turnball, Managing Director of Cambridge Analytica, claimed to be responsible for developing the *Crooked Hillary* slogan.[167] Wylie also revealed that popular slogans like *build the wall,* and *drain the swamp*[168] were focus group-tested by CA as early as 2014.[169] Indeed, the Trump campaign and Nix both celebrated their use of emotions in campaigning to target voters. However, none of this appears to be based on psychographics. Brad Parscale argued that the Trump campaign ran almost exclusively emotionally affirmative advertising.

> If you look at all of our advertising it was about the emotional feel of what it meant if Donald Trump would win, how it would change your life, I believe people vote the same way they purchase, they vote with their emotions. [170]

The confidence of these individuals to claim their tactics as revolutionary is misplaced. The practice of emotional advertising has been a common method in political campaigning for some time - Obama's *Yes we can* campaign, and Trudeau's *Real Change Now* campaign both utilized this approach. Past campaigns have also used negative

---

[166] Carole Cadwalladr, '"I Made Steve Bannon's Psychological Warfare Tool": Meet the Data War Whistleblower', *The Guardian*, 18 March 2018, sec. News, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[167] Channel 4 News, *Cambridge Analytica: Undercover Secrets of Trump's Data Firm*, accessed 29 January 2019, https://www.youtube.com/watch?v=cy-9iciNF1A&t=16s.

[168] Ted Widmer, 'Draining the Swamp', 19 January 2017, https://www.newyorker.com/news/news-desk/draining-the-swamp.

[169] Cadwalladr, '"I Made Steve Bannon's Psychological Warfare Tool"'.

[170] 'Brad Parscale Digital Director Trump | User Clip | C-SPAN.Org', accessed 2 February 2019, https://www.c-span.org/video/?c4637517/brad-parscale-digital-director-trump.

emotions to stir voter support. In 2004, the Bush Campaign exploited the 9/11 footage for a promotional campaign video,[171] and *drain the swamp* was a slogan utilized during Reagan's campaigns in the 1980s.[172] Indeed, the field of political communication has understood the impact and efficacy of emotions in politics for a while.[173] As political strategist James Harding wrote, "the battle is ever more for hearts, not minds: America's winning and irresistible formula has been to repackage an intellectual argument inside an emotional appeal."[174] Emotional cues are commonly utilized by political parties as a heuristic to help engage voters, as was demonstrated in the 1950s when researchers realized that a high proportion of US voters lacked an understanding of policy issues or the institutions of their country, and were largely devoid of ideological coherence.[175] Thus, the utilization of emotions in advertising for both positive and negative purposes is neither novel nor revolutionary.

Cambridge Analytica: Questionable Tactics

Alexander Taylor, CA's Chief Data Officer, stated, "the campaign will focus their finite resources for things like persuasion and mobilization, and then they leave the air war… like the negative attack ads to affiliated groups."[176] Based on FEC filings, Williams and Gulati determined that super-PACs and other outside groups spent roughly

[171] Issenberg, *The Victory Lab*. 141
[172] Widmer, 'Draining the Swamp'.
[173] Eric Groenendyk, 'Current Emotion Research in Political Science: How Emotions Help Democracy Overcome Its Collective Action Problem', *Emotion Review* 3, no. 4 (October 2011): 456, https://doi.org/10.1177/1754073911410746.
[174] James Harding Quoted in Sasha Issenberg, 'Cruz-Connected Data Miner Aims to Get Inside U.S. Voters' Heads', Bloomberg, 12 November 2015, https://www.bloomberg.com/news/features/2015-11-12/is-the-republican-party-s-killer-data-app-for-real-.
[175] Groenendyk, 'Current Emotion Research in Political Science'. 456
[176] Channel 4 News, *Cambridge Analytica*.

$350 million on advertising for Trump, $153 million of which was for digital advertising.[177] Contrary to the claims of their leaked presentation, the work CA conducted on the official Trump campaign was limited to TV advertising, identifying 'persuadable' voters using survey research, and managing a $12 million advertising budget on behalf of Gilles-Parascale, Brad Parascale's company.[178] However, they also ran ads for *Make America Number One*, a super-PAC run by Rebekah Mercer and Steve Bannon, which spent ≈$5.7 million on CA services,[179] part of which went to *Stop Crooked Hillary*, a YouTube channel which uploaded 35 videos that collectively received 3,057,995 views.[180] These videos largely focused on portraying Clinton as corrupt, a threat to national security, or that she failed to pay female staff fairly. CA's advertising for this super-PAC won *Big Data Gold* at the *Advertising Research Foundations David Ogilvy Awards* for their identification of persuadable voters.[181] This campaign also posted multiple dark posts on Facebook that attacked Clinton's credibility and alleged that Clinton was a drug addict.[182]

During a 2016 interview, a senior campaign official stated that Trump's digital team was undertaking three separate voter suppression operations targeting African

---

[177] Christine B. Williams and Girish J. "Jeff" Gulati, 'Digital Advertising Expenditures in the 2016 Presidential Election', *Social Science Computer Review* 36, no. 4 (1 August 2018): 406–21, https://doi.org/10.1177/0894439317726751.

[178] Issie Lapowsky, 'What Did Cambridge Analytica Really Do for Trump's Campaign?', *Wired*, 26 October 2017, https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/.

[179] Heather Timmons, 'Cambridge Analytica's Biggest Customers', Quartz, 2018, https://www.theatlas.com/charts/SyHHFzJqM.

[180] 'Defeat Crooked Hillary', YouTube, 2016, https://www.youtube.com/channel/UCRvnu9aLecF_JM6D0E0ga-w.

[181] The Advertising Research Foundation, 'The Advertising Research Foundation Announces the Winners for The ARF David Ogilvy Awards', 21 March 2017, https://www.prnewswire.com/news-releases/the-advertising-research-foundation-announces-the-winners-for-the-arf-david-ogilvy-awards-300425825.html.

[182] Craig Silverman, 'Cambridge Analytica Says It Won The Election For Trump. Here's What They're Actually Talking About.', BuzzFeed News, 20 March 2018, https://www.buzzfeednews.com/article/craigsilverman/cambridge-analytica-says-they-won-the-election-for-trump.

American voters, young women, and idealistic white voters.[183] The strategy relied on targeting African Americans with ads based on Clinton's racially charged remarks about *super-predators*, in which she suggested African Americans were predisposed to violence. Information about Bill Clinton's sexual assault allegations was used to target women, while Clinton's stance on trade deals was used to target idealistic young voters.[184] In Hersh's testimony before the US Senate, he suggests that all of those characteristics would be relatively easy to access and target with basic datasets, and not reliant on psychographics. He also notes that mobilization and demobilization are much easier objectives to achieve than persuading undecided voters.[185]

Issenberg suggests that as the Trump campaign and CA ran out of identified persuadable voters, they tried to shrink Clinton's base, this was possibly accomplished using the Mercer Run super-PAC, a claim Parscale later denied.[186] This targeted demobilization could also help explain the sharp decline in Clinton's approval rating from 2008-2016, in some demographics noted by Elkin.[187] Wylie reported this tactic as well, "what I'm talking about is targeting particular groups of people with messages that will disengage, frustrate, or confuse them. That ultimately will, in some cases, inhibit or demotivate them enough to not participate in an election."[188] Wylie also confirmed that voter targeting was occurring based on racial lines. "I believe at the instigation of Steve

---

[183] Issenberg and Green, 'Why the Trump Machine Is Built to Last Beyond the Election'.
[184] Ibid
[185] Eitan Hersh, 'Written Testimony of Eitan Hersh', § HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY (2018), 4 https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Hersh%20Testimony1.pdf.
[186] Brad Parscale, The Frontline Interview: Brad Parscale, interview by James Jacoby, Video, 8 August 2018, https://www.pbs.org/wgbh/frontline/interview/brad-parscale/.
[187] Emily Elkin, 'The Five Types of Trump Voters', text/html, Voter Study Group (Democracy Fund, 11 June 2017), https://www.voterstudygroup.org/publications/2016-elections/the-five-types-trump-voters.
[188] Wylie, Breach of Personal Information Involving Cambridge Analytica and Facebook. 1000

Bannon and some of his colleagues in different packs—[Cambridge Analytica] was to create lists of predominantly African American voters and then look at what types of messaging would disengage them from politics further, which would then reduce the likelihood that they would vote…."[189] Racial targeting of this type was possible on Facebook in 2016, as race was a category available to campaigns.[190] This voter dissuasion is a possible contributing factor in explaining why African American voter turnout in 2016 was at the lowest point in 20 years.[191]

Though morally reprehensible, the US has a history of racially-based voter suppression.[192] Race as a category in micro-targeting is also a relatively common phenomenon in US politics, so that alone cannot account for the visceral reaction against CA.[193] Though such tactics are rarely referred to so openly, a mistake Issenberg believed was due to the amateur nature of the campaign, they are common.[194] However, this tactic alone also does not explain the reduced voter turnout; it is part of a broader pattern of racially motivated voter suppression occurring across the US in the 2016 election. There are records of voter suppression tactics such as gerrymandering,[195] tossing ballots,[196] and

---

[189] Wylie.

[190] Terry Parris Jr Julia Angwin, 'Facebook Lets Advertisers Exclude Users by Race', text/html, ProPublica, 28 October 2016, https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

[191] Mark Hugo Lopez and Jens Manuel Krogstad, 'Black Voter Turnout Fell in 2016 US Election', *Pew Research Center* (blog), 12 May 2017, http://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

[192] Tova Andrea Wang and Janice Nittoli, *The Politics of Voter Suppression: Defending and Expanding Americans' Right to Vote* (Ithaca, UNITED STATES: Cornell University Press, 2012),18 http://ebookcentral.proquest.com/lib/uvic/detail.action?docID=3138356.

[193] Julia Angwin, 'Facebook Lets Advertisers Exclude Users by Race'.

[194] Issenberg and Green, 'Why the Trump Machine Is Built to Last Beyond the Election'.

[195] Matt Ford, 'How Texas Republicans Got Away With a Racially Discriminatory Electoral Map', *The New Republic*, 25 June 2018, https://newrepublic.com/article/149357/texas-republicans-got-away-racially-discriminatory-electoral-map.

[196] Julie Ebenstein, 'We're Suing California Because It Threw Out More Than 45,000 Ballots in the 2016 Presidential Election Over Handwriting "Mismatches"', American Civil Liberties Union, 24 August 2017, https://www.aclu.org/blog/voting-rights/fighting-voter-suppression/were-suing-california-because-it-threw-out-more-45000.

arresting African American voters for voter fraud. [197] A racially charged discourse was pronounced throughout the entire Trump campaign, this rhetoric helped to bolster the rise of the alt-right movement, a movement with which many Trump insiders had connections.

Breitbart Doctrine

The Alt-Right is diffuse in its definition, though James T. Main suggests that the central themes of the movement focus around a rejection of contemporary liberal notions such as racial equality and feminism. Likewise, the movement embraces white racialism, anti-Americanism, and vitriolic rhetoric.[198] The group is supportive of the Trump presidency and were responsible for organizing the Charlottesville *Unite the Right* protest, which resulted in the murder of one anti-racist protestor.[199] Trump was slow to condemn the attack. Some members of this group are core-Trump voters such as Richard Spencer, a prominent leader in the movement, who has been filmed performing a Nazi 'Sieg-heil' while chanting "Heil Trump."[200] Likewise, David Duke, Grand Wizard of the Ku Klux Klan formally endorsed Trump for the presidency because he believed Trump would help white Americans take their country back.[201] The Klan's support of Trump is

---

[197] Jack Healy, 'Arrested, Jailed and Charged With a Felony. For Voting.', *The New York Times*, 10 August 2018, sec. U.S., https://www.nytimes.com/2018/08/02/us/arrested-voting-north-carolina.html.

[198] Thomas James Main, *The Rise of the Alt-Right* (Washington, D.C: Brookings Institution Press, 2018). 8

[199] Melissa Gomez, 'Charlottesville Car Attack Suspect Pleads Not Guilty to Federal Hate Crimes', *The New York Times*, 6 July 2018, sec. U.S., https://www.nytimes.com/2018/07/05/us/charlottesville-plea-hate-crimes.html.

[200] Robinson Meyer, 'YouTube Removed the "Hail, Trump" Video From Search - The Atlantic', The Atlantic, 20 March 2018, https://www.theatlantic.com/technology/archive/2018/03/youtube-removes-the-atlantics-hail-trump-video-from-search/555941/.

[201] Libby Nelson, '"Why We Voted for Donald Trump": David Duke Explains the White Supremacist Charlottesville Protests', Vox, 12 August 2017, https://www.vox.com/2017/8/12/16138358/charlottesville-protests-david-duke-kkk.

partially due to his dog-whistle rhetoric, such as the proposal to build a Southern-border wall, the idea for which originated at a Klan rally in 1924.[202]

Beyond the alt-right's support for the Trump campaign, there are also numerous concerning connections between CA and the alt-right ideology. Steve Bannon, former Vice-President of Cambridge Analytica, was also former head editor of Breitbart, a news organization he once referred to as the platform of the alt-right. Breitbart saw 64 million views per month, and 10.3 million were unique visitors from September 2016 – February 2018.[203] Under his stewardship, with funding from the Mercers, Breitbart became a staunchly right-wing, anti-immigrant, anti-Islamic publication. In 2016, he declared Breitbart to be the platform of the alt-right and threw the full support of the publication behind Trump.[204]

In his testimony to the ETHI Committee, *Meeting #109,* Chris Wylie stated that Bannon was attempting to enact the *Breitbart Doctrine,* premised on the notion that culture determines politics. "He was looking for a way of expanding his arsenal of tools to engage in what he would call [a] culture war."[205] In Wylie's understanding, Bannon's main objective of CA was to utilize a cultural shift to make Trump, and his rhetoric appear as a viable political option.[206] The roots of this theory are reminiscent of an alt-right philosophy of *meta-politic*s premised on the movement disseminating a new set of "cultural ideas, attitudes, and values in a society, which eventually leads to deeper

---

[202] Rebecca Onion, '"Build a Wall of Steel"', Slate Magazine, 17 January 2019, https://slate.com/news-and-politics/2019/01/second-kkk-anti-immigrant-trump-wall.html.
[203] Main, *The Rise of the Alt-Right.* 27
[204] Sarah Posner, 'How Donald Trump's Campaign Chief Created an Online Haven for White Nationalists', Mother Jones, 22 August 2016, https://www.motherjones.com/politics/2016/08/stephen-bannon-donald-trump-alt-right-breitbart-news/.
[205] Wylie, Breach of Personal Information Involving Cambridge Analytica and Facebook. 0920
[206] ibid

political change."[207] Since Trump's election, he has villainized numerous marginalized groups across the US, and likewise the FBI has reported a rise in hate crimes by as much as 17% in 2017.[208] Though it would be inaccurate to suggest that Trump is the direct cause of those crimes, the fact that he has refused to condemn them has emboldened white nationalists across the US.

Conclusions

Cambridge Analytica did not significantly deviate from standard voter surveillance practices in the US, but it did draw attention to those practices. The company's tactics are emblematic of larger problems in the US electoral system. CA entered a highly competitive ecosystem with the promise of better data and better targeting, though their ability to do so is highly contested. The hyperbole and smooth marketing that provided CA with clout in US elections also raised alarms about the role of micro-targeting in a democratic society. CA was one of many firms working on the 2016 election. They were responsible for TV advertising for Trump's official campaign, management of budgets, running ads for a super pac, and conducting survey research, none of which was a significant departure from methods used during the 2012 campaign of Barack Obama. Despite these facts, there was still a persistent narrative propagated through the media that CA was undermining the democratic system.[209]

CA caused outrage over their use of data-analysis and voter surveillance to identify political opponents and target them with advertising to dissuade their democratic

---

[207] Main, *The Rise of the Alt-Right.* 13
[208] John Eligon, 'Hate Crimes Increase for the Third Consecutive Year, F.B.I. Reports', *The New York Times*, 13 November 2018, sec. U.S., https://www.nytimes.com/2018/11/13/us/hate-crimes-fbi-2017.html.
[209] Denham, 'Democracy Disrupted?'

participation. This tactic stands as a stark contrast from the oft-purported narrative that political parties need access to this data to fulfill their role as political intermediaries. It also undermines the argument that a lack of access to this data will have a chilling effect on political participation.[210] The use of surveillance to marginalize groups is well documented in surveillance studies, though its impact on elections is less known. Barocas notes that micro-targeting creates hierarchical citizenship, which prioritizes voters in swing ridings over less critical ridings.[211] Using these same tactics to dissuade racial groups is a significant and abhorrent, yet logical extension of this marginalization. Racial disengagement is unfortunately all too common in US politics, as exemplified most poignantly by the number of African American voters turned away from polling booths during the 2000 election.[212] Yet CA and Trump's connection to the alt-right highlighted the egregiousness of these anti-democratic practices. This connection is the most crucial distinction between previous elections and the 2016 election.

CA's voter disengagement operations targeting African Americans, female voters, and idealistic white voters was an attempt to marginalize and silence enemies of the alt-right from participating in the democratic process, a realization of the worst fears of scholars of micro-targeting. Yet the attitudes that underpinned this rhetoric could be found in the RNC database discovered by Vickery, and not reliant on CA. Appetites for many of the more xenophobic policies proposed by the Trump campaign are hinted at in

---

[210] MIchael Fenwick, 'Breach of Personal Information Involving Cambridge Analytica and Facebook', § Standing Committee on Access to Information, Privacy and Ethics (2018), 1130 https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-123/evidence.

[211] Barocas, 'The Price of Precision'. 34

[212] Mireya Navarro and Somini Sengupta, 'Contesting the Vote: Black Voters; Arriving at Florida Voting Places, Some Blacks Found Frustration', *The New York Times*, 30 November 2000, sec. U.S., https://www.nytimes.com/2000/11/30/us/contesting-vote-black-voters-arriving-florida-voting-places-some-blacks-found.html.

the RNC's modelled opinions on immigration, the exportation of jobs, or America First.[213] The campaign can test the countries readiness for populist and white-supremacist attitudes and adjust rhetoric accordingly.

The election of a party so closely aligned with a movement like the alt-right demonstrates the dangers of these databases when operated without oversight. Yet, CA did not need psychographic profiles on their political opponents to craft and deliver messages; standard voter surveillance tactics ensured that this was more than achievable. Recognizing the sharp right-wing shift in the US forced voters to confront the realities of these databases. Yet the alt-right link does not explain how CA became a global conflict. What about this issue allowed CA to gain worldwide notoriety? To understand that, we must examine how Nix used Facebook data to enrich CA's data sets. CA's use of Facebook helped to expand the scope of this conflict beyond the US and demonstrate its global ramifications, but why?

[213] O'Sullivan, 'The RNC Files'.

Chapter 3: How the Data Flows

The CA conflict would not be possible without the capture and exploitation of Facebook data. Since CA, Facebook has been under a critical spotlight, shedding light on multiple alarming controversies.[214] Thus, to understand CA, it is necessary to understand how CA used Facebook to harvest the data of 87 million people, and examine the scope of personal information collected by Facebook and third-party app developers. CA capitalized on Faceboook's willingness to grant access to 'friend data' and used this data to try to build psychological profiles on US voters. CA's use of Facebook data fostered two central narratives about CA. One narrative argues that CA hacked Facebook,[215] the other argues that the Facebook hack helped CA hijack democracy.[216] This "hacking" helped to create a international outrage because of Facebook's global use and integration into the lives of billions of people. Furthermore, these 87 million people were not just US citizens, they were people around the world. The belief that such a platform could be hacked fostered alarm for many. This chapter will dispel both of those narratives and argue that reactions to CA data came from Facebook's resistance to regulation, rampant collection of personal information, and its continued erosion of, and blatant disregard for privacy principles. These factors ultimately contributed to the global outrage to CA.

---

[214] The ethnic cleansing of Myanmar and the use of Facebook to spread Russian propaganda are both important issues that have contributed greatly to the recent decrease of Facebook stock, however it is necessary to point out that these two issues came to light after Facebook came under scrutiny for their role in the Cambridge Analytica conflict.

[215] Adi Robertson, 'Netflix Documentary The Great Hack Turns the Cambridge Analytica Scandal into High Drama', The Verge, 30 January 2019, https://www.theverge.com/2019/1/30/18200049/the-great-hack-cambridge-analytica-netflix-documentary-film-review-sundance-2019.

[216] Carole Cadwalladr, 'The Great British Brexit Robbery: How Our Democracy Was Hijacked', *The Guardian*, 7 May 2017, sec. Technology, https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

Facebook and Privacy

Before it is possible to delve into the CA conflict, it is necessary to demonstrate how Facebook has weakened privacy norms over the past decade. Facebook's first privacy policy, enacted before surveillance capitalism had been articulated by Zuboff, promised not to share information without user approval, but Facebook users had little awareness of the possible value of their data.[217] To an individual unfamiliar with the Facebook platform, the network would appear to be antithetical to privacy, inasmuch as it was a peer-monitored information sharing platform. But much like Flaherty's Puritans who sought privacy in a Puritan surveillance society, these individuals had a degree of control over what information they chose to share and with whom they chose to share it. They could withdraw from the system when they wanted to receive privacy and could post the information they felt comfortable sharing. Though privacy settings allowed users to block specified individuals from seeing their account information, activity on the account was always fully visible to the company.

Internet ethics scholar Michael Zimmer believes that Zuckerberg, the CEO of Facebook, has an antagonistic relationship with privacy. By examining public statements from Zuckerberg, Zimmer discovered three main trends in how the founder of Facebook views privacy, such as the belief that information wants to be free, and the world will be a better place with more information; privacy is an obstacle to creating this better open world; and the belief that people do not care about privacy. "What people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what

[217] Zuboff, 'Big Other', March 2015.

they share and what they don't." [218] Collectively these comments indicate a lack of respect for the norms of privacy.[219]

Facebook's privacy control settings are useful for limiting other members' access to information, but there is no way for a member to control what information the platform collects. Facebook views itself as a public space,[220] but it is a surveilled public space. The platform situated itself as a mediator for everyday interactions and managing relationships. Facebook has achieved this integration into people's lives by designing the product to "consume as much of your time and conscious attention as possible."[221] The more time people spend on the platform and the more the platform mediates their lives, then the more of their personal data the platform collects. As Facebook expanded the public into the private through web analytics,[222] tracking a user's physical location,[223] and saving messages that users decide not to send, [224] they were engaging in what I define as *palter privacy,* a rhetorical device used to convince users that Facebook was concerned about protecting privacy while extracting as much information as possible from their users. The ability to withdraw from society temporarily is an aspect of privacy noted by

---

[218] Zuckerberg, Quoted Zimmer, 'Mark Zuckerberg's Theory of Privacy'.

[219] For a more detailed analysis of these trends please see: Michael Zimmer, 'Mark Zuckerberg's Theory of Privacy', 2014,

[220] Jacquelyn Burkell et al., 'Facebook: Public Space, or Private Space?', *Information, Communication & Society* 17, no. 8 (14 September 2014): 974–85, https://doi.org/10.1080/1369118X.2013.870591.

[221] Garett Sloane, 'Sean Parker Says Facebook Was Designed to Be Addictive', AdAge, 9 November 2017, https://adage.com/article/digital/sean-parker-worries-facebook-rotting-children-s-brains/311238.

[222] Paris Martineau, 'Facebook Is Tracking You on over 8.4 Million Websites', The Outline, accessed 10 January 2019, https://theoutline.com/post/4578/facebook-is-tracking-you-on-over-8-million-websites.

[223] Justin Pot, 'Facebook Is Tracking Your Phone's Location, Here's How to Review Your History', How-To Geek, accessed 10 January 2019, https://www.howtogeek.com/fyi/facebook-is-tracking-your-phones-location-heres-how-to-review-your-history/.

[224] Poppy Noor, '"The Fact That We Have Access to so Many Different Opinions Is Driving Us to Believe That We're in Information Bubbles" | The Psychologist', The British Psychological Society, June 2017, https://thepsychologist.bps.org.uk/volume-30/june-2017/fact-we-have-access-so-many-different-opinions-driving-us-believe-were.

Westin,[225] yet the degree of integration and encroachment of Facebook neuters the possibility of effective and full withdrawal while still being a member of the Facebook platform.[226] The transformation of the net into a fully public and trackable space means that for privacy to occur, individuals need to have full control over their data.

Through these methods of tracking users, Facebook became one of the most extensive private surveillance apparatuses in existence.[227] Over the past decade, they have worked to change the definition of privacy to expand the scope and quality of information people are comfortable sharing. The platform has become a socially integrated aspect of modern life, and though the argument of deleting Facebook is a viable solution, there are social and potentially economic problems that can arise for individuals from turning off Facebook. Facebook's integration resonates with a social version of Marx' theory of mandatory volunteerism, in which day-to-day participation in society hinges on the submission to surveillance.[228] Zuboff describes companies like Facebook as having, "skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces."[229] In the next section, I will examine how Facebook has resisted regulatory reactions to their underlying Graph API v1.0, but it is essential to remember that the scope of data collection by Facebook, their distaste for privacy regulation, and the ubiquity of the platform's global use help to explain why the reaction against CA was so severe.

---

[225] Westin, *Privacy and Freedom*, 7.
[226] Facebook's deployment of tracking cookies also means that it is building shadow profiles on non-users.
[227] Zuboff, 'Big Other', March 2015.
[228] Marx, 'Surveillance and Society'.
[229] Zuboff, 'Big Other', March 2015, 83.

Regulating Facebook

Facebook has been approached by multiple regulatory agencies over the last decade, demanding that they adjust their privacy settings and ensure they are upholding their responsibilities as data-holders. In 2007, Facebook made a change by allowing third-party app developers to use their API to develop applications. Facebook did this to improve cross-app integration on the platform.[230] Increased access also turned Facebook into a platform where programmers developed personalized content such as games, quizzes, and tools. To develop this content, the developers gained access to significant amounts of PII from app users and their friends. Though users could change their settings to limit permissions, thus making friend data inaccessible to an app, privacy settings were open by default meaning the majority of users did not limit permissions. Facebook's relationship with developers was mutually beneficial. Facebook's users increased their use of the platform because there was more to do, and app developers gained revenue. The same year that Facebook introduced the expanded third-party access, their privacy policy expanded the scope of people who could access a user's information on Facebook:

> Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.[231]

This change in 2007 has been the source of legal troubles with the Irish Data Commissioner, the Office of the Privacy Commissioner of Canada (OPC) and The Federal Trade Commission (FTC) in the US and many other regulators globally.

---

[230] Mark Zuckerberg, 'Facebook', 21 March 2018, https://www.facebook.com/facebook/posts/10157217558586729.

235. Zuckerberg. Opsahl, 2010.

Examining these cases will demonstrate both an irresponsible culture at Facebook that precipitated the CA conflict and the technical underpinnings of the platform that were used by Kogan.

In 2009, the OPC investigated multiple complaints by Canadians about Facebook. One of the issues that they addressed was Facebook withholding the purpose of collection. During the investigation, app developers were found to be consistently over-collecting information for purposes not essential to run the app. The OPC report noted that Facebook had no practical way to audit a developer's data collection.[232] To remedy this problem, the OPC recommended Facebook change their app settings to limit the seemingly unlimited collection of data by developers.[233] The OPC additionally recommended that Facebook inform users of the purpose of collection, and ensure that users expressly consent to that access. In response to the OPC report, Facebook declined to implement any of the recommended changes regarding the sharing of data with third-parties.[234] They responded to the OPC by stating:

> The phrase "seemingly unlimited and unmonitored access" offers an apparent endorsement of the view that there are no limits and no monitoring. This has been repeatedly shown to be completely false in presentations, and is shown to be false by other information presented throughout the Preliminary Report..[235]

Facebook went on to state that only 20-30% of Facebook users change their privacy settings from the default public setting.[236] Despite their denial of any error,

---

[232] Canada. Office of the Information & Privacy Commissioner for British Columbia. Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act. By Elizabeth Denham. Ottawa: Privacy Commissioner of Canada, 2009. 51

[233] Ibid.

[234] ibid

[235] Ibid 50

[236] Ibid. 66

Facebook adjusted its platform by introducing Graph API V 1.0 in April 2010, which promised to improve the level of control that users had over their privacy settings.[237]

Facebook's Graph API was developed based on *Graph Theory*, a formula used to describe the connection between objects.[238] From the platform's perspective, "every user on Facebook is represented as an object,"[239] and this allowed every action taken on Facebook to be coded and searchable. This objectification of the user allowed developers to request specific permissions based on an object ID, including personal information such as religion, political view, education history, posts that a person has liked, relationship status, photos, interests, groups, and work history. Like the previous iteration of the platform, developers could request permissions to the user's friend data, including the friend's photos, likes, posts, and location to build profiles on individuals who were not using the app.[240]

Two years after the 2009 OPC report, the FTC concluded an investigation into Facebook's privacy practices and ultimately charged Facebook on multiple counts. Five of these counts relate specifically to problems that would arise during the CA conflict, including deceptive privacy settings, ambiguous changes to Facebooks privacy settings to increase data shared with third parties, the sharing of personal information with advertisers in contravention of Facebook's privacy policy, and near unlimited collection

---

[237] Jonathan Albright, 'The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle', Medium, 21 March 2018, https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747.

[238] "Archive - Graph API - Documentation." Facebook for Developers. Accessed October 05, 2018. https://developers.facebook.com/docs/graph-api/changelog/archive.

[239] Facebook Developers. YouTube. June 20, 2013. Accessed October 05, 2018. https://www.youtube.com/watch?v=WteK95AppF4.

[240] Ibid.

of data by third-party apps.[241] These charges demonstrate that changes Facebook made to the API did little to protect the privacy of Facebook users, a problem that would re-occur during the CA conflict. In a settlement with the FTC, Facebook agreed to correct misleading language in its privacy policies and implement a privacy risk assessment (PRA) to identify all potential privacy risks that stem from their platform.

In 2011, the same year that the FTC charged Facebook, the Irish Data Protection Commissioner reported that many users are unaware that apps belong to third-party developers, and are not part of Facebook.[242] The report also noted that "a user can revoke the permission for an application via the applications permissions screen."[243] However, by Facebook's own admission only 20-30% of their users adjust their settings. The Commissioner was satisfied that app developers were limited from collecting information above and beyond the requested app permissions, though they felt that the privacy policies could be improved. The regulator also noted:

> In certain cases, reliance is placed on developer adherence to best practice or stated policy to ensure security of user data. This is not considered sufficient by this Office to assure users of the security of their data once they have third party apps enabled. We expect [Facebook] to take additional steps to prevent applications on a pro-active basis from accessing user information other than where the user has granted an appropriate permission.[244]

Facebook had no substantive means to keep track of the data flowing to third-party developers. This data was regulated by Facebook's Platform Policy which outlined that the data collected from a user could only be used to improve the Facebook

---

[241] Jon Leibowitz, J. Thomas Rosch, and Julie Brill, 'In the Matter of Facebook, Inc., a Corporation', Complaint (United States of America: Federal Trade Comission, n.d.), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

[242] Ireland. Data Protection Commissioner. Report of the Audit on Facebook Ireland by the Irish Data Protection Commissioner. By Gary Davis. 2011

[243] Ibid. 92

[244] Ibid. 93

experience and that the developer had to delete the information when it was requested. In 2018 Sandy Parakilas, former-Platform Operations Manager testified before the DCMS Committee to explain Facebook's app developer oversight process:

> Once the data passed from Facebook servers to the developer, Facebook lost insight into what was being done with the data and lost control over the data. To prevent abuse of the data once developers had it, Facebook created a set of platform policies—rules, essentially—that forbade certain kinds of activity, for example selling data or passing data to an ad network or a data broker. However, Facebook had very few ways of either discovering abuse once data had been passed or enforcing on abuse once it was discovered. [245]

CA's use of Facebook data stems from the failure to enforce regulations on Facebook. CA did not hack Facebook. Other apps used Facebook in the same way as CA's app, but CA did violate Facebook's Platform Policy by using the data for purposes other than enhancing user experience. Three regulators in three years approached Facebook about, among other things, their oversharing of information with third-party apps, and their lack of safeguards to secure or protect their user's data. Despite these calls for regulation, the company failed to mitigate the problems associated with third-party access. The company had positioned itself for rapid growth and development at the expense of its customers' privacy.

Once developers extracted the data, Facebook had limited powers of enforcement. Part of the issue associated with the use of Facebook data is what Chris Vickery referred to as its 'stickiness.'[246] Once Facebook has transferred the data to the third-party developer, Facebook is "basically reliant on [the developer's] word" that the data's use

[245] Fake News Inquiry: Testimony before the Committee on Digital, Culture, Media and Sport, HC 363 (2018) (Statement of Sandy Parakilas, former-Platform Operations Manager of Facebook) Q1188

[246] Fake News Inquiry: Testimony before the Committee on Digital, Culture, Media and Sport, HC 363 (2018) (Statement of Chris Vickery Director, Cyber Risk Research, UpGuard) Q2534

was privacy-compliant,[247] concerns that had been raised by the OPC in 2009. Despite API V1.0's success at bringing in new developers to design apps specific to Facebook, the social networking site found that users were uncomfortable with the amount of personal information that was collected by the apps.[248]

In 2014, Facebook announced a change to their Graph API to include granular permission settings, in which users could select what information an app could collect, and ended access to friend data. Facebook made the change when they became concerned that the openness of the platform may shrink their now more privacy-aware userbase. [249] Developers were given one year to prepare for the change, and by 2015, no app would have access to friend-data or extended permissions without explicit approval from users.[250] By April of 2015, Facebook closed API V1.0, though developers retained the data collected unless individuals requested data deletion.

Facebook: a Political Space

The potential power of this platform was demonstrated in 2013 when Facebook conducted a large-scale experiment on over 600 thousand Facebook users. Researchers manipulated the stories on the user's NewsFeed to test whether it could effect user's emotions. They were successful. Like previous privacy abuses, Facebook argued that users consented to participation in the experiment when they created their Facebook account. The research demonstrated that exposing the subject to negative content,

---

[247] Parakilas: Testimony on Fake News Q1190

[248] Josh Constantine, 'Facebook Is Shutting Down Its API For Giving Your Friends' Data To Apps', *TechCrunch* (blog), 28 April 2015, http://social.techcrunch.com/2015/04/28/facebook-api-shut-down/.

[249] ibid.

[250] This was later proven to be untrue when news broke that Facebook had been whitelisting companies to maintain access to this information.

resulted in them creating negative posts, but the inverse was true as well.[251] Facebook showed advertisers that they could affect their users' real-world behaviour without a user's awareness of emotional manipulation.[252] Undoubtedly the experiment is ethically dubious, but it demonstrated both the scope of monitoring possible through Facebook and Facebook's impact on individual emotions, although this was not the first time the platform was used to experiment with social influence.

In the 2012 US election, Facebook was utilized by the Obama campaign in a way that revolutionized the politicization of Facebook data. By taking advantage of the Graph API v1.0's friend settings, the *Obama for America* app gained access to the entire friend network of the one million people who downloaded the app.[253] By gaining access to the friend networks of all of the app users, the Obama campaign had access to almost all of Facebook's US social network,[254] a prospect according to Carol Davidson, who worked on Obama's 2012 campaign, that contributed to Facebook shutting down the Graph API.[255] The Obama campaign needed to solve a problem of voter outreach to young voters, a notoriously difficult demographic to reach. The Facebook feature allowed the Obama campaign to personalize messages which encouraged their supporters to solicit friends specificly identified by the campaign. Teddy Goff, the Obama campaign's digital

---

[251] Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, 'Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks', *Proceedings of the National Academy of Sciences* 111, no. 24 (17 June 2014): 8788–90, https://doi.org/10.1073/pnas.1320040111.

[252] Shoshana Zuboff, Surveillance Capitalism Is Eroding Democracy Recode Decode, Hosted By Kara Swisher podcast, Podcast, 20 February 2019, https://player.fm/series/recode-decode-hosted-by-kara-swisher-88572/shoshana-zuboff-surveillance-capitalism-is-eroding-democracy.

[253] Ed Pilkington and Amanda Michel, 'Obama, Facebook and the Power of Friendship: The 2012 Data Election', *The Guardian*, 17 February 2012, sec. US news, https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election.

[254] The main difference between the *ObamaforAmerica App* and the Kogan app was that Kogan sold the data to Cambridge Analytica, and thus violated Facebook's terms and conditions.

[255] Carol Davidsen, 'You Are Not a Target' (4 June 2015), https://www.youtube.com/watch?v=LGiiQUMaShw.

director, described the strategy as necessary because "people don't trust campaigns. They don't even trust media organizations. Who do they trust? Their friends."[256] The Obama team maintained ownership of this data after the election, providing the Democratic party with the advantage of knowing the digital relationships (circa 2012) of practically every US citizen on Facebook.[257]

The Graph API was not available during the 2016 election. Therefore political parties could not replicate the Obama campaign's methods. However, Facebook did develop an extensive political consultancy operation, with different departments for Republicans and Democrats. The platform offered embedded consultants to work with the campaign to ensure they were getting optimal results from Facebook.[258] Since its successes in the US, Facebook now offers embedded campaign workers in elections around the world. By 2014, political campaigns in the US were trying to optimize their advertising by studying social media sites to ensure their advertising practices were consistent with changes to Facebook's algorithms.[259] Thus, Facebook has become a pivotal resource in modern electoral campaigns.

Facebook also eased the ability to target based on demographics. So much so, that it became untenable to create personalized content for all the demographics available. One former Obama-staffer opined that the data now outpaced their targeting capabilities.

> So ideally you would have a track for women, a track for Hispanics, and a track for Hispanic women, track for African American women, and so on, and then you would break it down to age groups, then break it down by interests, or realistically

[256] Michael Scherer, 'Friended: How the Obama Campaign Connected with Young Voters', *Time*, 20 November 2012, http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/.
[257] Carol Davidsen, 'You Are Not a Target'.
[258] Parscale, The Frontline Interview.
[259] Kreiss, *Prototype Politics.* 200

> by behaviour… But you will never have enough content creators… our ability to target has moved beyond our ability to create content.[260]

The campaign chooses a demographic they wished to target, then they use Facebook in multiple ways. They can upload a list of supporters directly to Facebook, or use the *look-a-like* feature, which scans Facebook for people who share characteristics with already identified supporters. Alternatively, campaigns can select attributes that their analytics identified as being coorelated with supporters. An example of attributes Facebook offers is demonstrated in Figure 3.1.[261]

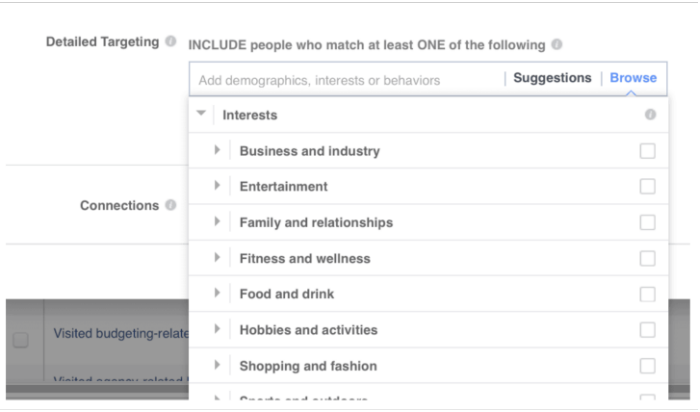

Figure 3.2: An example of categories Facebook makes available to advertisers

Facebook argues that they are a public space, like a digital town square. They have integrated themselves into almost every aspect of people's lives and produce revenue by selling access to this data. They are an intrusive surveillance apparatus that has eroded norms of almost every privacy principle and have been chastised by regulators for this reason. The introduction of political parties to Facebook means that the surveillance that has long been the standard practice for Facebook has transcended into

---

[260] ibid. 201

[261] 'The Beginner's Guide to Facebook Audiences and Targeting', *AdEspresso* (blog), accessed 7 June 2019, https://adespresso.com/guides/facebook-ads-beginner/demographic-targeting/.

the sphere of the political.[262] The Cambridge Analytica conflict occurred in this context. CA was dealing with a company resistant to regulatory oversight, with little accountability to their customer's data, and an interest in utilizing their vast quantity of data to impact democratic change.

Cambridge Analytica: The "Magic Sauce"

Alexander Nix stated that CA created a long-form quantitative instrument to probe the underlying psychology of the voting public. This instrument was developed based on the OCEAN (Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) psychological profile - psychologists refer to these traits as the big five personality traits. The model was developed in the 1980s by McCrea and Costa to categorize all factors involved in developing a personality.[263] In the model, an individual is assessed based on a multiple-choice exam, the answers to which are then scored and modelled to display the degrees of each of these traits in an individual. This method is considered scientifically valid and accepted in the psychology community. There are multiple variations of this personality model; however, each of the models tends to formulate into five broad personality groupings.[264]

In the mid-2000s, Facebook collaborated with numerous researchers to analyze the impact and relationships people had with Facebook. One such organization was the Cambridge Psychometrics Centre. Two of these researchers, Michal Kosinski, and David

---

[262] Though I do not personaly believe Facebook data should be considered public information.

[263] Robert R. McCrae and Paul T. Costa, 'Comparison of EPI and Psychoticism Scales with Measures of the Five-Factor Model of Personality', *Personality and Individual Differences* 6, no. 5 (January 1985): 587–97, https://doi.org/10.1016/0191-8869(85)90008-X.

[264] John M. Digman, 'Personality Structure: Emergence of the Five-Factor Model', *Annual Review of Psychology* 41 (1 January 1990): 432.

Stillwell developed an application called *MyPersonality* that provided users with 20 personality-scoring questions drawn from the International Personality Item Pool (IPIP) and additional questions about users personal lives. 58,466 volunteers completed the quiz and allowed researchers to analyze their Facebook data to reveal the connection between personality and Facebook likes. [265] The researchers analyzed criteria such as drug use, sexual orientation, and political views, as well as where the subjects were on the OCEAN personality ranking.[266] The study suggested that there are considerable benefits to utilizing this knowledge, though they are also quick to caution of its abuses, "because it can easily be applied to large numbers of people without obtaining their individual consent and without them noticing." [267]

CA believed they could use this research to effect political change. To accomplish this, they hired Dr. Alexandr Kogan to replicate this model. He did so by utilizing a quiz app that exploited the Graph API to collect friends' data, in a way that manifested the worst fears of regulators. Facebook never read the terms and conditions of Kogan's app, which stipulated that he would sell this information to third-parties. This oversite meant Kogan had access to the profiles of roughly 87 million people around the world.[268] Some of the information collected by Kogan's app includes the name, gender, birthday, location, email address, liked pages, posts, tagged photos, and messages of users, as well as the photos, page likes, gender, current city, and age of the user's friends.

---

[265] Michal Kosinski, David Stillwell, and Thore Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior', *Proceedings of the National Academy of Sciences* 110, no. 15 (9 April 2013): 5803, https://doi.org/10.1073/pnas.1218772110.
[266] Ibid.
[267] ibid. 5805
[268] Mike Schroepfer, 'Fake News', § DCMS (2018). 2144

This friend data was only accessible if the user's friends permissions setings allowed this data to be accessible .[269]

Cambridge Analytica: Not-so-magic sauce

When asked about the value of the Facebook data for political targeting, Kogan stated, "given what we know now, nothing. Literally, nothing."[270] Facebook was a useful source of data because roughly 70% of the US population had an account, so it was generally helpful to gather large N representative samples. However, this was contingent on having up-to-date data on a voting population.[271] This data was the source of CA's supposed competitive advantage over other companies. They claimed that this information underpinned their ability to micro-target based on psychographic profiles, although all evidence seems to indicate it did not work.

Kogan wrote that they were able to accurately predict all five personality scores for roughly 1% of the population. Furthermore, their models were more effective than randomly guessing, but less effective than guessing everyone has the same personality.[272] Though the data could be useful for recognizing trends in a population, it is unrealistic, and likely impossible, for this model to accurately predict an individual voter's personality. Eitan Hersh, in his written evidence to the Senate Judiciary Committee, remarked:

> While Mr. Wylie has used strong language about how his firm "weaponized" data, he has provided no specific information, such as results from validation studies or experiments measuring effectiveness of the firm's strategies… The fact

[269] Elizabeth Denham, 'Investigation into the Use of Data Analytics in Political Campaigns', A report to Parliament (Information Commissioner's Office, 6 November 2018), https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf. p.30

[270] Alexander Kogan, 'Fake News, HC 363', § Digital, Culture, Media and Sport Committee (2018), Q2027, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/81931.pdf.

[271] Kogan, Fake News, HC 363. 2022

[272] Alexandr Kogan, 'Written Evidence: Fake News', Pub. L. No. FKN0077, § DCMS, 1 (2018). Q2022

> that no such evidence of the firm's effectiveness has been provided publicly makes me skeptical of his strong claims.[273]

Much of the evidence surrounding the use of *Facebook likes* to derive psychographics were based on previous research by people like Stillwell and Kosinski. Other than claims by CA, there appears to be no evidence that the firm effectively harnessed this. When Issenberg was invited to CA offices in 2015 to see his profile, he compared it to the results of his official OCEAN test and found that the personality score modelled by CA was wildly inaccurate.[274] The ineffectiveness of the psychographic profiles would explain why both the Cruz campaign and the Trump campaign decided to abandon using the CA data, as noted in Chapter 2.[275]

After the CA story broke, Nix also argued that they were unable to extrapolate the personality scores from Facebook data. In part, because CA only received a small amount of information on the 87 million people. Nix Stated: "The fact is the data that we received wasn't fit for purpose, and that was why we abandoned that data long before we deleted that data from our servers in accordance with Facebook's wishes."[276] Both Kogan and Nix would have good reason to deny the viability of the data, as that would reduce the severity of their privacy violation, but they were not the only ones who argued that the data was unviable. Eitan Hersh commented that if CA had been using up to date Facebook data, they would have made microtargeting more effective- but the data they used was from 2014.

---

[273] Hersh, Written Testimony of Eitan Hersh. 1
[274] Issenberg, 'Cruz-Connected Data Miner Aims to Get Inside U.S. Voters' Heads'.
[275] Andy Kroll, 'Cloak and Data: The Real Story behind Cambridge Analytica's Rise and Fall', *Mother Jones* (blog), May 2018, https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer/.
[276] Nix, Oral evidence: Fake News, HC 363. Q3312 – Q3332

> Whereas a person who supported Republicans last cycle is likely to support Republicans this cycle, a person who was persuadable yesterday might not be persuadable today. There is no one subset of the electorate that is all the time susceptible to persuasion. Depending on the exact message, messenger, and context, a person may be persuadable or not persuadable. This makes it difficult for campaigns and political parties to learn, election to election, or even day to day, about how to persuade voters. What worked last time may not work this time.[277]

Dr. David Sumpter, an applied mathematician, analyzed the data that CA was using and interviewed Kogan. From his analysis of CA's data, he realized, "that it couldn't convincingly determine whether a person was likely to be neurotic or not."[278] Furthermore, when he interviewed Kogan, Kogan described the impracticality of the method CA was utilizing, noting that the correlation rate between Facebook likes and personality was weak at roughly 0.3. This data was then combined with consumer and geographic data and used to try and target people with messaging. When commenting on why Nix had promoted the product so aggressively, Kogan said, "Nix has very little comprehension of what he is talking about,… He is trying to promote [the personality algorithm] because he has a strong financial incentive to tell a story about how Cambridge Analytica have a secret weapon."[279] This experiment exacerbated the already existent problem of data-doubles, which meant that faulty data profiles had been used to inform political messaging during the Cruz campaign.

Though psychographics for consumer and political purposes are of dubious utility, CA is far from the only company utilizing these tactics. Hamish Marshall, campaign manager for the Canadian Conservative Party's 2019 election bid, said

---

[277] Hersh, Written Testimony of Eitan Hersh. 5

[278] David Sumpter, 'My Interview with Aleksandr Kogan: What Cambridge Analytica Were Trying to Do and Why Their…', Medium, 22 April 2018, https://medium.com/@Soccermatics/my-interview-with-aleksander-kogan-what-cambridge-analytica-were-trying-to-do-and-why-their-f869ef65d945.

[279] Ibid.

"combining psychographic information, demographics about someone's psychology is extraordinarily useful, [although] it's not for the faint of heart."[280] Environics Analytics is another company that offers consumer data for companies in Canada, though their products are anonymized rather than personalized. Their product, Prizm5, offers targeting based on geographic, demographic, and psychographic traits for Canadian citizens, as well as a range of beliefs such as: racial fusion, sexism, multiculturalism, patriarchy, xenophobia, acceptance of violence, national pride, rejection of inequality, obedience to authority, need to escape, aversion to complexity, ecological fatalism, and technological anxiety.[281]

Despite the insidiousness of these categories, the effectiveness of psychographics changing political opinions is far from successfully demonstrated. There is strong evidence to indicate that political microtargeting is useful for fundraising and volunteer turn-out, though there is no evidence that this translates into votes. Instead, journalists tend to accept verbatim the claims of political campaigns, propagating what Baldwin-Phillipi refers to as myths of big data.[282] PII is collected, modelled, and stored to infer the disposition of voters, this is done despite the dubious efficacy of big data in elections.

Conclusion

Facebook's resistance to regulation, its continued erosion of and blatant disregard for privacy principles, the increased politicization of Facebook's data, and its world-wide

---

[280] 'Andrew Scheer's Campaign Manager Says He Builds Creepy Psychological Profiles of Voters Too', *PressProgress* (blog), 22 March 2018, https://pressprogress.ca/andrew-scheers-campaign-manager-says-he-builds-creepy-psychological-profiles-of-voters-too/.

[281] 'Psychographic Data | SocialValues Dataset | Environics Analytics', accessed 25 February 2019, https://www.environicsanalytics.com/en-ca/data/psychographic.

[282] Baldwin-Philippi, 'The Myths of Data-Driven Campaigning'.

userbase ultimately primed the global outrage to CA's use of data. This chapter demonstrated that Facebook has long had an antagonistic relationship with privacy, the result of which is Facebook's active efforts to normalize the oversharing of personal information and redefine the paradigm of privacy. Westin points out that every person is always engaged in an adjustment process in which they must navigate the desires for disclosure and communication with the hopes of privacy.[283] Facebook's resistance to regulators meant that, for six years, apps with virtually no oversight had near unlimited access to PII. The company has rapidly altered the division between private and public for economic gain. As a result, until 2015, Facebook was an open door for PII. They increased their integration into social life, and increased the addictiveness of their product by expanding the number of activities on Facebook.

The politicization of this space altered the nature of the privacy violation inherent in the platform. CA directed a spotlight onto both the power and value of PII collected from Facebook and the irresponsible business practices that were rampant at Facebook. The way CA claimed to use the data was invasive and deeply personal, creating a severe perceived privacy harm. Information thought to be innocuous and personal by voters was allegedly transformed into powerful political data. However, Facebook had staff embedded in the Trump campaign and has been using the platform for political purposes since 2012, so this alone is not a complete explanation.

The unregulated collection of data by third parties and the collection of friend data was public knowledge, as was demonstrated by the OPC report from 2009. Therefore, the one distinct difference between CA and Facebook's voter targeting is the

[283] Westin, *Privacy and Freedom*. 7

use of the term psychographic. It is relevant to note that psychographic data is used in both commercial and political targeting, as demonstrated by both Environics and Hamish Marshall's comments in 2017. Facebook has already shown considerable targeting abilities, as well as the ability to manipulate emotions using their platform. Indeed Nix and Kogan both stated that CA abandoned its approach to microtargeting because Facebook's in-house system was far more effective at targeting people based on their dispositions.[284] CA did not take an egregious step beyond what was already common, but its marketing suggested that it had created a brain-washing tool, something Wylie stated in his first public interview.[285]

Both the data and the context were crucial components of this conflict, but those elements were known for almost two years before this story reached peak popularity - the Guardian first reported that Cruz was using stolen Facebook data in 2015.[286] People did not pay attention to this issue until it was framed correctly and propelled forward by individual actors central to this story. So who was responsible for framing this issue, and how did they frame the issue in a way that resulted in global attention?

[284] Kogan, Written Evidence: Fake News.
[285] Cadwalladr, '"I Made Steve Bannon's Psychological Warfare Tool"'.
[286] Harry Davis, 'Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users | US News', The Guardian, 11 December 2015, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

Chapter 4: The Actors and Advocates

Privacy scandals need privacy advocates – individuals who are able to bring the issues to public and political attention. The actors who contributed to bringing the CA conflict to global public attention are numerous. An analysis of the motivations and testimony of each of these individuals would be prohibitively difficult for a project this size. I am therefore narrowing my attention only to those key actors who provided new insights and frames to this conflict. These individuals are: Chris Vickery, who discovered a code repository belonging to the SCL network; Carole Cadwalladr, of the Guardian/Observer, who was the most prominent journalist of this story; Emma Briant, of the University of Essex who interviewed vital members of the SCL network; as well as Chris Wylie, and Brittany Kaiser, who risked a considerable amount to expand knowledge about this story.[287]

I will begin this final chapter by giving a brief overview of privacy advocacy and explore some of the strategies and frames that they have used in the past. Next, I will introduce these actors and analyze their testimony to understand how they framed the CA conflict, and what they believed were appropriate responses. By comparing past strategies and categories of privacy advocates with this contemporary case, I ultimately conclude that the narrative of democratic erosion was the most prominent theme promoted by the actors and that the most prominent actors in this conflict were not traditional privacy advocates.

[287] Though there were countless prominent academics, researchers, industry insiders, who helped the world understand this issue better. Their contribution to understanding Cambridge Analytica is irreplaceable.

Privacy Advocates: An Overview

Though the modern privacy and surveillance scholarship has grown considerably since its advent in the 1960s, privacy advocates and their impact remain under-studied. Scholars such as Colin Bennett and Simon Davies have shed some light on the methods employed by privacy activists.[288] Their work has also informed the analysis of contemporary privacy activism, such as Till Wascher's research on the privacy campaigns following the Snowden revelations.[289] Davies notes that the network is fluid and diverse, and has taken many forms and utilized multiple methods to advance adhoc privacy concerns. He argues that in all countries that have had privacy challenges, privacy is "fuelled by issues of sovereignty, technophobia, power, and autonomy."[290]

At times these movements have managed to gain broad public recognition, such as the Dutch census resistance in the 1970s.[291] Comparable to the environmental movement, they can garner significant support, though usually for a short period. Privacy activism is normally discrete, such as destroying privacy-invasive CCTV cameras, or using privacy-enhancing technologies such as Duck Duck Go or Adblocker when surfing the internet. Formalized organizations such as the Electronic Freedom Frontier (EFF), Privacy International, the International Association of Privacy Professionals, Center for Democracy and Technology, the Tactical Technology Collective, and numerous others also work to highlight the dangers of surveillance and protect privacy.[292] Many of the

---

[288] Davies, '13. Spanners in the Works'. 244
[289] Till Wäscher, 'Framing Resistance Against Surveillance: Political Communication of Privacy Advocacy Groups in the "Stop Watching Us" and "The Day We Fight Back" Campaigns', *Digital Journalism* 5, no. 3 (16 March 2017): 368–85, https://doi.org/10.1080/21670811.2016.1254052.
[290] Davies, '13. Spanners in the Works'. 1999, 245
[291] Bennett, 2008. 135
[292] Colin Bennett, *Privacy Advocates*, 2008, xx-xxii .

most prominent advocates did not begin as privacy advocates, but rather as concerned citizens who, when necessary, came forward to comment on, and critique privacy-invasive practices.[293] These actors then help to frame the conflict into language that both help people understand the issues and provide solutions.

Privacy advocates have utilized numerous tactics and strategies to garner public awareness. Bennett uses Keck and Sikkink's typology of politics to organize past activism.[294] One such tactic is *Information politics*, in which advocates provide the public with access to information about an unknown privacy threat. Bennett mentions that this tactic works well when "there is a wrong that can be documented. Appeals are then made to the collective conscience of a society and of its political and business elites."[295] Though this tactic is useful, it is difficult for privacy advocates to utilize as the effects of privacy violations are often diffuse and, by the nature of the breach, individualistic and personal.[296]

There have been examples in the past of overcoming this issue, such as Robert Ellis Smith's *War Stories*, which serves as a reminder of the financial, reputational, or psychological harm that privacy violations can cause. He does so by detailing stories of US citizens who were the victim of privacy invasions.[297] Information politics can be difficult in privacy cases as advocates can tend to rely on technical terms, limiting the discussion to experts. To circumvent this problem, privacy advocates will try to frame the

---

[293] Colin Bennett, *Privacy Advocates*, 2008 , 63.
[294] Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders : Advocacy Networks in International Politics* (Cornell University Press, 1998), 16.
[295] Bennett, *Privacy Advocates*, 96.
[296] Ibid.
[297] Robert Ellis Smith, Eric Siegel, and James S Sulanowski, *War Stories: Accounts of Persons Victimized by Invasions of Privacy* (Providence, R.I.: Privacy Journal, 1993).

issue in the context of *value*. By identifying a specific value that is under threat, such as freedom, advocates can expand the discussion to the broader public.[298]

Additionally, privacy advocates may engage in *symbolic politics*, where rather than value-based judgements, they appeal to cultural images about which people have a familiarity and pre-formed opinions. Perhaps the most prominent example of this is the use of Orwell's *1984* to oppose draconian surveillance practices.[299] The Orwellian imagery has been a relative fixture in privacy advocacy for decades and featured prominently during the anti-NSA protests in 2013.[300]

Advocates may also utilize *accountability politics* in which they hold governments or corporations accountable to either legal or publicly-acknowledged privacy standards. Advocates may use legal jurisdictions in creative ways, as was the case when the Canadian OPC investigated Accusearch Inc., a US-based company that was collecting information on Canadians without their consent.[301] Max Schrems also used this approach when he used European privacy law to force Facebook to become privacy-compliant in Europe.[302]

The last tactic that Bennett lists is *leverage politics*, in which a bad actor is publicly condemned and advocates leverage an economic impact against the actor until they adjust their practices. Though this only works when advocates can withhold something of value from the actor. More frequently, privacy advocates resort to publicly shaming a bad actor until they adjust their behaviour.[303]

---

[298] Bennett, *Privacy Advocates*, 98.
[299] Bennett, 107.
[300] Wäscher, 'Framing Resistance Against Surveillance'.
[301] Bennett, *Privacy Advocates*, 115.
[302] Kashmir Hill, 'Max Schrems: The Austrian Thorn In Facebook's Side', Forbes, accessed 9 June 2019, https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/.
[303] Ibid. 123

Wascher's analysis into the anti-NSA protests found that four framing packages attracted media attention. Wascher describes these frames as *historical parallels, Orwellian totalitarianism*, *global dimensions*, and *celebrity activism*. He discovered that of these frames, the media adopted and replicated celebrity activism frames most readily, with 40% of media organizations mentioning Snowden specifically in their coverage of the protests, significantly higher coverage than any other framing device.[304] By utilizing the celebrity frame, activists are "framing resistance against surveillance as heroic acts of individual activists that should be seen as role models for collectively voicing dissent."[305] In part because "Edward Snowden not only acted as an icon and protest symbol but participated himself by interpreting his leaks in morally charged terms. Also, because of his ability to attract media coverage and generate quotable sound bites, Snowden is currently arguably the most valuable asset of the privacy advocacy network."[306] Adding a human face to the conflict is a crucial element of increasing attention to a privacy issue.

Bennett offers a useful typology to organize the various advocates involved in past privacy conflicts. Many typologies may overlap within an actor, and multiple actors may work on the same issue, but all of these individuals provide useful skills and knowledge for combating privacy violations. Table 4.1 provides a summary of Bennett's categories.

[304] Wäscher, 'Framing Resistance Against Surveillance'. 375
[305] ibid, 372.
[306] Ibid.

Category	Description
Advocate/Activists	Advocates ideologically motivated by the value of privacy. As such, they work through many methods and tactics to elevate attention to the value of privacy first and foremost. They can be grassroots or expert-led. They may focus on critiquing legislation or educating the public.[307]
Advocate/Researchers	Advocates who provide an empirical or theoretical grounding for critiques surrounding a privacy conflict. Their critiques can span numerous disciplines from sociology to mathematics.
Advocate/Consultant	Advocates who provide information or skills to improve privacy practices or awareness of possible privacy concerns.
Advocate/Technologist	Advocates who utilize their skills to develop privacy-enhancing technology such as cryptography.
Advocate/ Journalist	Advocates who utilize their skills as journalists to discover, document, and disseminate information about privacy issues.
Advocate/Artist	Advocates who utilize their artistic skills to develop imagery that challenges structures of surveillance. Their work can span guerilla installations, movies, songs, and visual media.

Table 4.2: Bennett's Typology of Privacy Advocates[308]

The types of advocates and effectiveness of their strategies will differ from case-to-case and, because of the diversity and lack of cohesion in privacy advocacy, there will be multiple overlapping strategies utilized at the same time. In the case of CA, numerous actors, many of whom were formal privacy groups, worked to highlight concerns about CA, although they were not on the front-line of this conflict. Groups such as the Electronic Freedom Frontier (EFF), Privacy International, the International Association of Privacy Professionals, Center for Democracy and Technology, and The Tactical Technology Collective were late to draw attention to CA's voter surveillance practices. A search of each of their websites using the term *Cambridge Analytica* found that almost all

[307] Bennett, *Privacy Advocates*. 74

[308] Bennett, 63–94.

articles they published on the topic appeared after the March 2018 Wylie article.[309] Only two of these organizations wrote articles about CA before 2018: the EFF wrote an article leading up to the 2016 election warning of the dangers of voter surveillance, citing CA as a threat;[310] and Privacy International wrote an article about CA's technical capacity in April 2017, in which they related the company's predictive capacity to other technologies.[311]

This delayed attention would suggest that the testimony and media coverage was largely responsible for fostering concern about CA. Many of those who testified were not privacy concerned until the CA case. Some were not strictly privacy advocates who were "animated by a fundamental belief that privacy is not only an important issue but one of defining questions of modern times," but all of them "have deep-seated worries about abuses of power by modern organizations using the latest technological tools."[312] Each of them utilized, some at personal risk, various means and tools to highlight their concerns about CA and voter surveillance.

Strategies and Framing

Carole Cadwadladr

Journalist-Advocates such as Carole Cadwalladr or Harry Davies, who first reported on CA's acquisition of Facebook data in 2015,[313] drew public attention to the

---

[309] Cadwalladr, '"I Made Steve Bannon's Psychological Warfare Tool"'.

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

[311] 'Cambridge Analytica Explained: Data and Elections', Privacy International, accessed 22 May 2019, http://privacyinternational.org/feature/975/cambridge-analytica-explained-data-and-elections.

[312] Bennett, *Privacy Advocates,* 94.

[313] Davis, 'Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users | US News'.

gap in privacy standards at Facebook. The initial response by Facebook was "misleading people or misusing their information is a direct violation of our policies and we will take swift action against companies that do."[314] When Cadwalladr followed up the article in 2017, she faced a legal threat from Facebook.[315]

Just as Snowden became the face of the NSA revelations, Wylie became the face associated with the Cambridge Analytica conflict. His bright pink hair was prominent on the cover of the *Observer* when he first declared his public condemnation of CA. There were numerous articles written about CA, many of which this thesis references. However, Cambridge Analytica as a search term peaked following the publishing of *I made Steve Bannon's psychological warfare tool,* with a stoic picture of Chris Wylie. The story was released one day before *Channel 4's* expose on Alexander Nix. Figure 4.2 is a graph demonstrating the popularity of the term *Cambridge* Analytica on Google. It shows that the Nix and Wylie stories fostered the highest popularity on Google.[316] [317] Though it should be noted that this data set is collected and modelled internally by Google in non-transparent ways. Thus, the graph is representative of Google's perception of interest in Cambridge Analytica, and does not necessarily accurately represent public opinions or interest. Despite these shortcomings, I am using this tool as a rough demonstration of public interest.

---

[314] Harry Davies, 'Facebook Told Me It Would Act Swiftly on Data Misuse – in 2015 | Harry Davies', *The Guardian*, 26 March 2018, sec. Opinion, https://www.theguardian.com/commentisfree/2018/mar/26/facebook-data-misuse-cambridge-analytica.

[315] Carole Cadwalladr, 'Cambridge Analytica a Year on: "A Lesson in Institutional Failure"', *The Guardian*, 17 March 2019, sec. UK news, https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie.

[316] Google trends provides an broad look at popularity. 100 represents the time where interest in a search term was at its highest popularity, the other numbers represent popularity compared against peak popularity.

[317] 'Google Trends', Google Trends- Cambridge Analytica, accessed 22 May 2019, https://trends.google.com/trends/explore?date=2017-01-02%202019-05-22&q=CAmbridge%20analytica.

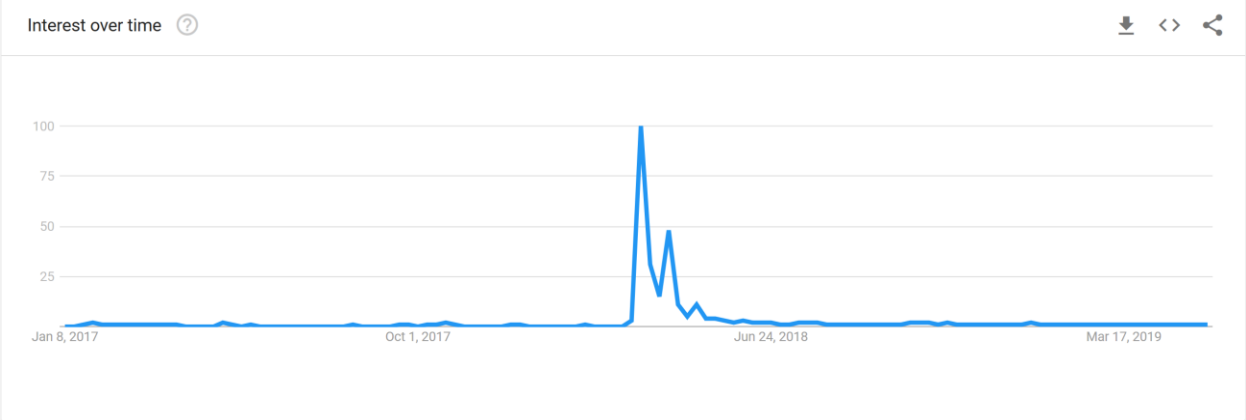

Figure 4.2: Google Trends graph of the serach term *Cambridge Analytica* January 2017 – March 2019

In that article, Wylie details the story of "how Facebook was hijacked, repurposed to become a theatre of war: how it became a launchpad for what seems to be an extraordinary attack on the US's democratic process."[318] The article was as much about Wylie as it was about CA, it detailed Wylie's education history, his dietary habits, his sexual orientation, and his mental health. The article then continues about Steve Bannon, the alt-right, psychological warfare, and "hacking Facebook." The expose by Channel 4 heightened this narrative by portraying Nix as a villain, willing to do anything to win an election for a client.[319] Figure 4.2 suggests that this coverage dwarfs the previous articles written on CA, but when I reframed the date window from January 2016 till March 16, 2018, two days before that article was released (as demonstrated in Figure 4.3) it puts the impact of the article into context.[320] Here we can see the first peak of interest in Cambridge Analytica was in December 2016 following a story by Das Magazin, which

[318] Cadwalladr, '"I Made Steve Bannon's Psychological Warfare Tool"'.
[319] Channel 4 News, *Cambridge Analytica*.

[320] Google Trends', Google Trends- Cambridge Analytica, accessed 22 May 2019, https://trends.google.com/trends/explore?date=2016-01-01%202018-03-16&geo=US&q=Cambridge%20Analytica

was then picked up and translated by Vice which accounted for the second spike in popularity.[321]

Table 4.3: Google Trends graph of search term Cambridge Analytica January 2016 - March 16, 2018

This article drew on interviews with Michael Kolinski, one of the data scientists who discovered the connection between Facebook likes and personality, to describe how the data could build personality profiles. It then makes connections between Cambridge Analytica, psych-ops, Brexit, Trump, Facebook data and voter-disengagement, and spends some time talking about electoral campaigning.[322] At roughly the same time as the German article, Cadwalladr wrote an article about white-supremacist gaming of search engines to suggest search terms like '*are jews evil'*; in this article, she made the connection between Breitbart, Steve Bannon, and CA's work in the US.[323]

The third spike in popularity was around May 7, 2017, when Cadwalladr published an article about Brexit, Trump, psychological warfare, Facebook data, and

[321] Von Hannes Grassenger and Mikael Krogerus, 'Ich habe nur gezeigt, dass es die Bombe gibt', *Das Magazin* (blog), 3 December 2016, https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/.

[322] Hannes Grassegger and Mikael Krogerus, 'The Data That Turned the World Upside Down', *Vice* (blog), 28 January 2017, https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.

[323] Carole Cadwalladr, 'Google, Democracy and the Truth about Internet Search', *The Observer*, 4 December 2016, sec. Technology, https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook.

CA.[324] This article used anonymous sources, and referred to CA as dystopian by using quotes such as: "psychological operations – the same methods the military use to effect mass sentiment change. It's what they mean by winning 'hearts and minds.' We were just doing it to win elections in the kind of developing countries that don't have many rules."[325] One section of her May 7 article demonstrates Cadwalladr's talent at blending in almost every core theme that Davies notes as necessary in privacy conflicts, such as issues of sovereignty, technophobia, power, and autonomy.

> There are three strands to this story. How the foundations of an authoritarian surveillance state are being laid in the US. How British democracy was subverted through a covert, far-reaching plan of coordination enabled by a US billionaire. And how we are in the midst of a massive land grab for power by billionaires via our data. Data which is being silently amassed, harvested and stored. Whoever owns this data owns the future.[326]

The last peak in Figure 4.3 came when The Guardian revealed that CA had exclusive contracts with Politico,[327] and the Daily Beast reported that CA had tried to contact Wikileaks.[328] Collectively, these articles cover most of the main elements that became central to this conflict, the psychographics, stolen Facebook data, shady connections, and Trump. However, it was not until the introduction of Wylie and Nix that broad public popularity sky-rocketed. Though governments and scholars already recognized CA as an issue, as the DCMS, and ETHI committees had already begun their inquiries into the CA conflict and Fake News.

---

[324] Cadwalladr, 'The Great British Brexit Robbery'.
[325] Ibid.
[326] Ibid.
[327] Stephanie Kirchgaessner, 'Cambridge Analytica Used Data from Facebook and Politico to Help Trump', *The Guardian*, 26 October 2017, sec. Technology, https://www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump.
[328] Betsy Woodruff, 'Trump Data Guru Alexander Nix: I Tried to Team Up With Julian Assange', *The Daily Beast*, 25 October 2017, sec. politics, https://www.thedailybeast.com/trump-data-guru-i-tried-to-team-up-with-julian-assange.

Chris Wylie

In the months that followed his story in the Guardian, Wylie worked with various governments to provide documentation of his time at CA. These documents included emails, reports, and contracts detailing the collection and modelling of Facebook data. His career as a political consultant began when he was a teenager working for the Canadian Liberal party as a volunteer, and later as a contractor.

Wylie portrayed CA as an egregious deviation from voter surveillance practices, such as those explored in Chapter 2. When asked by the Committee Chair at DCMS why he came forward with information regarding the company, he stated that a citizen has a responsibility to report illegal behaviour.[329] In his written evidence to the US Senate on May 16, 2018, Wylie wrote:

> American democracy matters. It matters not just to the American citizens who vote, organise, protest, run for office or to those who just speak their minds. American democracy matters to the world which so often looks to the United States for leadership in defending and promoting democratic ideals.[330]

Like Snowden, Wylie veils his revelations about CA in a moral critique. Wylie situates CA as a tool of war that is being used to undermine democracy. It is also important to note that in this testimony, he mentions that he did not work on the 2016 campaign, with his work in the US limited to the 2014 midterm election, meaning his knowledge the Trump campaign would be proximate at best.

> To be clear, the work of CA and SCL is not equivalent to traditional marketing, as has been claimed by some. This false equivalence is misleading. CA specialised in disinformation, spreading rumours, kompromat and propaganda. Using

---

[329] Wylie, Fake News. Q1276

[330] Chris Wylie, 'Written Statement to the United States Senate Committee on the Judiciary', § Committee on the Judiciary (2018), https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Wylie%20Testimony.pdf. 1

> machine learning algorithms, CA worked on moving these tactics beyond its operations in Africa or Asia and into American cyberspace.[331]

To Wylie, CA was something distinctly different from previous forms of electoral campaigning. Rather than focusing explicitly on voter surveillance, Wylie takes the opportunity to critique platform companies such as Facebook, suggesting that platforms are fostering a perception that privacy is an antiquated value. In doing so, Wylie's testimony evokes Marx' *mandatory volunteerism*.

> We should therefore be wary of any company that presents a false dichotomy between our privacy rights and living in a modern digitised society. Online platforms' terms and conditions present users with a false choice because using the Internet is no longer a choice.[332]

Wylie was a political operative before and after his time at CA, suggesting he may be sympathetic to the benefits of voter surveillance. Chapter 2 established that Wylie's framing of CA's role in the 2016 election as significantly deviant from the status quo is not accurate. Wylie argues that CA went a step too far, but is generally unapologetic about prior iterations of voter surveillance and does not regard these practices as part of the problem. Regarding what should be done to solve the problem, Wylie told the members of ETHI 109:

> One of the things that I think should be considered is more rules on transparency for targeting. Currently, if you as a politician go out and do a constituency event, the media might show up, there's an audience, your opponent might show up, and if you tell an untruth you can be called out on that, right? Or, if you say something and there's a different perspective, there is some kind of accountability mechanism there. That is the essence of the public forum.[333]

---

[331] Wylie. 'Written Statement to the United States Senate Committee on the Judiciary' 6
[332] Wylie, Written Statement to the United States Senate Committee on the Judiciary,15.

[333] Wylie, Breach of Personal Information Involving Cambridge Analytica and Facebook. ETHI 109. 1020

Wylie is specifically referencing the practice of dark-post micro-targeting, in which messaging is directed to voters in a digital format that is not public, this process is of dubious efficacy, but relies on campaigns having accurate PII. When speaking to the DCMS committee on March 27, 2018 Wylie stated, "There needs to be a wider discussion just in general about what is data protection …I do not think there is an either/or in terms of total restrictions on data and a free for all of data."[334] These two answers are useful suggestions that preserve the status quo with a strong focus on advertising transparency and minor limitations on political party data collection. This solution would allow politicians to continue to micro-target; it would preserve the electoral ecosystem, and do very little to curb the deployment of voter surveillance. Wylie also shifts the blame away from political parties and towards data platforms such as Facebook. His solution may force accountability in political parties for the messaging they deliver to their constituents, which may dissuade the more egregious examples of dog-whistle politics, such as those prominent in the Trump campaign.

Chris Vickery

Chris Vickery is a cyber-security researcher at UpGuard. His main task is to comb the internet locating unsecured databases. During his career, he has found databases belonging to the RNC, a database of 94.3 million Mexican voters,[335] 1.5 million unsecured medical files of US citizens,[336] and the leaked profiles of Hzone users, a dating

[334] Wylie, Fake News. Q1460

[335] Rafa Fernandez de Castro, 'A Massive Data Breach Exposed Personal Info for 93.4 Million Mexicans', Splinter, accessed 5 April 2019, https://splinternews.com/a-massive-data-breach-exposed-personal-info-for-93-4-mi-1793856429.

[336] Kate Knibbs, 'Error Exposes 1.5 Million People's Private Medical Records on Amazon Web Services [UPDATED]', Gizmodo, accessed 5 April 2019, https://gizmodo.com/security-hell-private-medical-data-of-over-1-5-million-1731548110.

app for people who are HIV positive.[337] He is exceptionally proficient at finding unsecured databases and then alerting companies of their privacy failings.

Vickery was invited to testify at DCMS and ETHI because he discovered an unsecured data bucket containing CA's voter data. He published his findings in four articles detailing the technical underpinnings of the company and how their Ripon platform organized CA's data models.[338] When speaking to the ETHI on April 17, 2018, Chris Vickery explained his perception of the CA conflict.

> I believe the matter before us is one of very great importance. Facebook is certainly one of the core elements involved, but I would urge all of you to keep an eye towards the very focused efforts of others who rely on Facebook as a pillar of their operations but not solely on Facebook; others who are tending to cause direct harm to what I believe is the institution of democracy itself as sort of an end goal of what they're working towards here. [339]

Like Wylie, Vickery situates the CA conflict as indicative of a threat to democracy. Between 2015- 2017, Vickery found exposed RNC data two times. Each time additional information had enriched the quality of the data. By commenting on the scale of data he has seen in political campaigns, Vickery suggested that the problem with CA is the scale of collection.

> You can have knocking on doors and gathering the phone number of one person at a time or whatever, but when that turns into more of a machine gun situation, whereby you are sending out thousands of surveys and emails and Facebook advertisements and everything and harvesting en masse the private details—or personal details, at least—of many, many thousands of times the people you could normally reach, that gets into the machine gun category, and that is dangerous.[340]

---

[337] 'Stolen Details of 3.3m Hello Kitty Fans – Including Kids – Published Online', *Naked Security* (blog), 10 January 2017, https://nakedsecurity.sophos.com/2017/01/10/stolen-details-of-3-3m-hello-kitty-fans-including-kids-published-online/.

[338] 'The Aggregate IQ Files, Part One: How a Political Engineering Firm Exposed Their Code Base', UpGuard, 18 February 2019, https://www.upguard.com/breaches/aggregate-iq-part-one.

[339] Vickery, DCMS - Q2504

[340] Chris Vickery, Breach of Personal Information Involving Cambridge Analytica. Breach of Personal Information Involving Cambridge Analytica. Meeting 99. 1005

Vickery's solution to the issue of over-collection by political parties is multifaceted, focusing on both strengthening existing privacy legislation and improving the mechanism of consent.

> We're more in the world in which, if the privacy laws are strengthened, there is a legitimate concern that the rules, or some would say restrictions, should not inhibit legitimate, responsible innovation. In answer to Mr. Baylis, I said that the value at stake for the most part is consent—control by individuals over their personal information.
> Part of the challenge is to have strong rules that generally ensure that consent is respected, but in the world of big data and artificial intelligence, it may be that there's a need for an exception to consent… I think a balanced piece of legislation would enhance consent, on one hand, but also needs to consider what we do as a country with proper business or social concerns—it may be in the health sector—that need to have information without necessarily the consent of the individual, for a true benefit for society.[341]

While Vickery has situated much of his criticisms towards platforms such as Facebook for their over collection and resistance to existing privacy legislation, he believes innovation via big data has a role in the future of technical developments. Thus, the challenge will be to balance these problems with the legitimate needs of political parties.

Dr. Emma Briant

Dr. Emma Briant is a media scholar who conducted interviews with key members of the SCL group and *Leave.EU*. She provided key information to the DCMS committee, which often contradicted witness testimony. She has also used her decade of interviews to write a book on the 2016 US election.[342] In her written evidence submitted to the US Senate Judiciary Committee, she provided a useful critique of many discussions around political party data use. Briant framed CA as a morally bankrupt company by using

[341] Chris Vickery. ETHI Committee 1010
[342] Which still has not come out at the time of writing.

quotes from key players such as Nigel Oakes, who provided an example of effective political advertising, "sometimes to attack the 'other' group, and know that you're gonna lose them, is going to reinforce or resonate your group."[343] Briant utilizes extensive comparisons between the tactics used by CA and Nazi propaganda. Indeed, most of the interviews Briant released showcase a moral critique of the company's targeting of minorities and situates it in a historical context.

Briant argues that knowledge about the audience improves the effectiveness of propaganda. Much of this information can come from platforms like Facebook.[344] People are largely unaware of the power of this information. Briant argues that social media has a debilitating effect of individualizing users, which has caused people to devalue the power of their data. User's are often unaware of how big data analysis can use innocuous data to infer intimate information. Through this, social media facilitates the normalization of privacy intrusions.

> The online architecture of social media encourage[s] the individual to focus on themselves, failing to see their data's significance within the collective, even as it becomes more and more compulsory to be 'connected' and surrender data.[345]

Organizations such as the Tactical Technology Collective have also argued that the individualization of privacy has undermined the progress of the privacy movement.[346]

---

[343] Nigel Oakes, quoted in Emma Briant, 'Three Explanatory Essays Giving Context and Analysis to Submitted Evidence', Written Evidence, 16 April 2018, FKN0071, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/88559.pdf. p4

[344] Briant.

[345] Emma Briant, 'Evidence for the US Senate Judiciary Committee on Cambridge Analytica and SCL Group', § US Sennate Judiciary Committee on Cambridge Analytica and SCL Group (2018), https://www.judiciary.senate.gov/imo/media/doc/Professor%20Emma%20L.%20Briant%20Report%20on%20Cambrige%20Analytica.pdf. 1

[346] Tactical Technology Collective and Becky Kazansky, 'FCJ-195 Privacy, Responsibility, and Human Rights Activism', *The Fibreculture Journal*, no. 26 (22 December 2015): 190–208, https://doi.org/10.15307/fcj.26.195.2015.

What heightened the prominence of CA was the global dimension and the sheer volume of people whose data was exposed. Through her decade-long study of SCL, Briant has concluded that the methods of distributing information and disinformation need improved regulation.

> Regulation is failing to keep up with the rapid progression of coordinated data-driven propaganda powered by AI and augmented with insights from neuroscience and psychology, this should raise alarm for us all.[347]

Briant began her investigation into SCL by looking at their anti-terrorism work. She has since witnessed SCL use these tactics, described as weapons of war, in elections. Briant suggests that technical developments in the influence industry are a threat to the future of democratic elections:

> Our data can reveal more about us than we wish to think about; the potentials for harm in some capabilities cannot be understated — machine learning can successfully identify markers of depression from our Instagram photos for instance…. as many declare #metoo, post-Weinstein, it is not unlikely that future campaigns could seek to combine these and similar data to exploit psychological wounds, mental health issues and trigger emotionally driven responses among vulnerable citizens.[348]

Briant's analysis is important. Though the technological capacity to target in these ways may not exist on a national scale, the industry will continue to push the development of these technologies. Briant argues the solution to the CA conflict is to improve regulation and transparency around micro-targeting, the algorithms that facilitate it, and personalized political messaging.

> It is also misleading to abstract the tools from how they were deployed – using our data is not in itself the problem, the issue is how it is being used, and this must be regulated with increased transparency at minimum. The Channel 4 expose

[347] Briant, 'Evidence for the US Senate Judiciary Committee on Cambridge Analytica and SCL Group'. 3
[348] Ibid. 2

> reveals Cambridge Analytica derived their power from a willingness to abuse it, targeting the vulnerable, hacking, and entrapping opponents. [349]

Briant's solution of improved transparency is simple though effective. It would cost the industry very little to improve transparency while potentially reducing many of the underlying issues such as voter dissuasion, and dog-whistle political messaging that were of prominence during the CA conflict. Though transparency does little to address the vast over collection of data Briant identified as problematic.

Brittany Kaiser

Brittany Kaiser was a Director of Business Development for Cambridge Analytica. During her time working for CA, she worked in the US, Mexico, and pitched Leave.EU, a pro-Brexit organization. On March 23, 2018, five days after Wylie's article, she was featured in the Guardian about her time working at CA. On April 17, 2018, Kaiser testified before the DCMS committee. Kaiser firmly situated CA as a privacy conflict, stating: "There's a much wider story that I think needs to be told about how people can protect themselves, and their own data."[350] Indeed, Kaiser spent much of her interview promoting data-autonomy. Since her time at CA, Kaiser went on to start the #Ownyourdata campaign to support data sovereignty.

In Kaiser's written evidence to the DCMS, she said:

> The elite have spent too many years using technology to take advantage of the people's openness and goodwill. I can no longer standby while the privileged abuse their power, intentionally or unintentionally.[351]

---

[349] ibid. 2

[350] Paul Lewis and Paul Hilder, 'Former Cambridge Analytica Exec Says She Wants Lies to Stop', *The Guardian*, 23 March 2018, sec. UK news, https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies.

[351] Brittany Kaiser, 'Written Testimony to the Fake News Inquiry', 17 April 2018, FKN0076, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Brittany%20Kaiser%20Parliamentary%20testimony%20FINAL.pdf. 1

Kaiser's statements provided insight into numerous aspects of CA's business operations, though she was surprised by, and unable to confirm many of the revelations regarding shady business dealings, blackmail, Russian connections, and extortion attributed to CA. Kaiser never had access to Facebook data and is not a data scientist, but she did provide insight into the working culture of electoral campaigning.

> It's important also to emphasise that during most of my time at Cambridge Analytica, the culture and assumptions of the firm and the wider data brokerage and ad tech industries within which it operated were a bit "Wild West," with citizens' data being scraped, resold and modelled willy-nilly.[352]

Kaiser's insights into the culture of the ad tech and data brokerage world provide evidentiary support to the belief that CA, rather than being a significant deviation, is much more aligned with the status quo in the US. In the concluding remarks of her written submission to the DCMS, Kaiser wrote:

> Governments, private companies and wealthy individuals have long had the opportunity to buy, license and collect our datasets. The past decade has seen a rampant rise of this data collection and modelling, targeting individuals to sell products, services and political ideology. I know this all too well, as a data rights campaigner and former employee of Cambridge Analytica.
> Privacy has become a myth, and tracking people's behavior has become an essential part of using social media and the internet itself; tools that were meant to free our minds and make us more connected, with faster access to information than ever before. Instead of connecting us, these tools have divided us. It's time to expose their abuses, so we can have an honest conversation about how we build a better way forward.[353]

Kaiser argues that the only way to reclaim power is to reclaim ownership over one's data, evoking definitions of privacy put forward by theorists like Westin, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what

---

[352] Ibid.. 5
[353] Ibid. 8

extent information about them is communicated to others."[354] Likewise, her proposed solution going forward is to restructure societies' relationship with technology to improve accountability over data. In her letter to the DCMS, Kaiser wrote:

> I launched the #OwnYourData campaign at the start of April, challenging Mark Zuckerberg to alter Facebook's terms of service to give users more rights over the use and monetisation of their own data. The petition I started for the campaign on Change.org now has 147,000 signatures.[355]

Data sovereignty would grant financial control over personal information. Though I believe that this solution is ripe with challenges, implementing a system of selling access to personal information protects individuals who are in a position to turn down the financial incentives to disclose. Yet this system does nothing to protect those who are in economically precarious situations, further exacerbating marginalization. This solution also does not introduce any of the regulatory oversight that the voter surveillance industry desperately requires.

A Bad Actor

I am ending this section by profiling Alexander Nix. There were two predominant frames that Nix used that helped form the CA conflict, a revolutionary psychological manipulation tool and a small political consultancy firm. [356] As far back as 2014, Nix crafted the message around his product as a groundbreaking innovation in political communication. During the 2016 presidential election, Nix framed his work on the Trump campaign as pivotal. At the end of his Concordia Summit presentation, he stated: "of the two candidates left in this election, one of them is using these technologies. And it

---

[354] Westin, Alan F. Privacy and Freedom. 1st ed. New York: Atheneum, 1967. 7

[355] 'Brittany Kaiser, Written Testimony to the Fake News Inquiry', 17 April 2018, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Brittany%20Kaiser%20Parliamentary%20testimony%20FINAL.pdf. 1

[356] Nix' testimony at DCSM was a pivotal inspiration for this thesis.

is going to be very interesting to see how they impact the next seven weeks."[357] In private meetings, Nix continued to propagate the message that his firm was directly responsible for the pin-point accuracy of persuading voters and spreading misinformation in crucial ridings.[358]

During the March 19th, 2018, *Channel 4* expose, Nix alluded to illegal activities such as hiring sex-workers to create compromising materials on political opponents, blackmail, and distributing anonymous propaganda on the internet to undermine the credibility of political opponents.[359] These comments were crutial for the popularity of the conflict and presented Nix as a villain. Of Nix' reamarks, Brittany Kaiser commented that Nix had a reputation for saying anything to convince a client to hire his firm.[360] Regardless of their authenticity, these remarks contributed to the myth of Cambridge Analytica.[361]

The second narrative that Nix presented was that his company was a humble ad agency. Following his Channel 4 expose, Nix agreed to testify before the DCMS committee. "By speaking with such exaggeration and hyperbole, I did not represent the company properly, I did not represent what we do as a company or as individuals, and that there was a significant impact from doing that."[362] Further, he situates his company as a minor deviation from other firms.

> That is an entire industry that is moving in this direction. It is not Cambridge Analytica. All we have simply done is look at the industry—the advertising industry—and at what is going on in the political industry, and we have taken the best practices and in a very short [period] of time we have replicated them and, I

[357] Nix, 'Cambridge Analytica - The Power of Big Data and Psychographics'.n 10:30
[358] Channel 4 News, *Cambridge Analytica*.
[359] Ibid.
[360] Lewis and Hilder, 'Former Cambridge Analytica Exec Says She Wants Lies to Stop'.
[361] Baldwin-Philippi, 'The Myths of Data-Driven Campaigning'.
[362] Nix, Oral evidence: Fake News, HC 363. Q3218

> would like to say, improved on some of these techniques and methodologies and served them up to a different political party in order to help them have an equal chance of competing in a free and fair democracy.[363]

These two narratives of democratic erosion and business as normal were prominent throughout the CA conflict. Nix' first narrative brought attention to an entire industry that, save academics and activists, had been under the radar of public discourse. By switching to the second narrative, that he was speaking in hyperbole and the company was not novel, he invited a deeper look at the larger issues of voter surveillance. If CA was indicative of standard practices, then the entire voter surveillance industry needed a deeper interrogation.

Conclusion

CA was unique as a privacy conflict with traditional privacy actors such as the EFF, who had been at the forefront of these issues in the past, being relegated to a supporting role, while the bulk of the discussion was fixated on new voices in the privacy debate. This emergence of new voices seems to indicate that the dangers of voter surveillance were largely under-the-radar of these traditional advocates prior to CA. Instead, numerous actors who are difficult to categorize as privacy advocates, or indeed would not identify themselves as advocates at all, were left to fill this vacuum. Almost all of these actors engaged in symbolic politics to draw on people's anti-elitist, anti-globalist, and technophobic attitudes - issues Davies notes are present in all major privacy conflicts.[364]

---

[363] Nix. Q658
[364] Davies, '13. Spanners in the Works'.

The CA conflict also highlighted the changing nature of digital consent, an issue many actors pointed to. Wylie argued that utilization of the internet is not an option, it is a necessity in modern society. Vickery argued for a contextually derived system of consent, remnisent of Nissenbaum's contextual integrity, in which concepts of privacy evolves with new social, moral, and political norms.[365] Thus companies must create more reasonable terms and conditions which limit whole-scale collection of PII. For Kaiser, this involved data ownership in an effort to seize the means of production in the surveillance capitalist system. Yet many of these actor's proposed solutions to the broader issues of voter surveillance were not privacy focused. Wylie, for example, argued in favour of improved transparency, rather than a limitation of data collection. Moreover, the main grievance of these actors, and the tone of the testimony was rarely focused on CA's privacy intrusion via Facebook data. Rather, these advocates focused on the far-reaching democratic implications of the CA conflict.

Each of these actors pointed to the conclusion that CA was a bad actor, and that it is a threat to democracy, although they disagree on how to fix the issue or what aspects of the case were the most egregious. Many of the problems addressed by the actors can be explored through a privacy lens, however the frequent emphasis of democracy's fragility demonstrates that privacy was not the central concern of many of these testimonies. Briant's evocation of Nazi imagery emphasized the historical parallels of this issue, and likewise, Cadwalladr's writing framed the CA conflict as a military style attack on democracy. The democratic problems of voter surveillance is an issue that politicians may not be ready to adequately address.

---

[365] Nissenbaum, *Privacy in Context*, 231.

Elected officials who are the beneficiaries of voter surveillance conducted all of these hearings. Politician's demand for an electoral advantage has been the driving force for increasingly granular data collection about voters. Despite this, these politicians are responsible for implementing regulations on these practices, with which they are seemingly out of touch. Following Zuckerberg's testimony before the US Senate, the media described the encounter as more akin to Zuckerberg explaining how to use Facebook than to a day of reckoning for the company.[366] A misunderstanding of voter surveillance technologies informed many of the questions asked by committee members.

Kreiss has argued that the technical sophistication of campaigns have left politicians unaware of the practices that are deployed to get them elected. Often campaigns bring in young political novices to dictate data-driven campaign tactics, leaving politicians alienated from, and thus unable to gauge the scope and potential detriments of voter surveillance.[367] This gap of knowledge left a huge space for privacy advocates and opponents of voter surveillance to dictate the direction of this discussion.

However, in response to the recommendations from the ETHI committee that the Canadian government expand the powers of the Privacy Commissioner and amend PIPEDA, the government decided to force political parties to publish privacy policies, but declined to extend privacy legislation to the parties.[368] The decision to not regulate political parties is not only antithetical to the recommendations made by ETHI, but it is

---

[366] Stewart, Emily, 'Lawmakers Seem Confused about What Facebook Does — and How to Fix It', Vox, 10 April 2018, https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations.

[367] Kreiss, *Prototype Politics*, 207.

[368] Chandler, Olivia · 'Privacy Commissioner, Chief Electoral Officer Issue Privacy Guidelines for Federal Political Parties | CBC News', 2 April 2019, https://www.cbc.ca/news/politics/powerandpolitics/politics-privacy-data-elections-canada-1.5080523.

also contrary to the advice by the Privacy Commissioner of Canada, the Privacy Commissioner of British Columbia, Elections Canada, the Information Commissioner of the United Kingdom, and every academic advocate who spoke on the matter at ETHI.

The impact of these testimonies is clear. On May 18, 2018, CA filed for bankruptcy,[369] and Facebook lost $130 billion as their user-base shrunk.[370] Unfortunately, the failure to regulate voter surveillance in Canada and the US means that its destabilizing effects are likely to continue. But the accomplishments of these individuals provide useful information on how to bring abuses to the public arena in the future. As the impacts of privacy violations and surveillance diffuse further into society, and impact more people, non-traditional actors and frames of democratic threat may be of increasing importance to the privacy movement.

[369] Eli Watkins and Joe Sutton, 'Cambridge Analytica Files for Bankruptcy', CNN, 18 May 2018, https://www.cnn.com/2018/05/18/politics/cambridge-analytica-bankruptcy/index.html.

[370] Jessica Guynn, 'Facebook Just Shed $130 Billion in Two Hours, Mark Zuckerberg Lost $16.8 Billion', USA TODAY, 25 July 2018, https://www.usatoday.com/story/tech/2018/07/25/facebook-catches-cambridge-analytica-chill-user-growth-slows/837683002/.

Conclusion: A Privacy Conflict?

The goal of this thesis was to analyze the underlying conditions that fueled public reactions to the Cambridge Analytica conflict and to understand its framing as a privacy issue. For over a decade, voter surveillance has remained under-challenged in the broader public discourse. Though there is some recent literature documenting voter surveillance, and some limited literature pointing to the privacy issues with which it is associated, the public in many democracies has remained largely uninformed and unconcerned. The multi-national inquiry into the practices of voter surveillance demonstrates that CA was a turning point. Why? Three interconnected structural conditions underlie the CA conflict: surveillance capitalism; an unregulated voter analytics industry; and the rise of the alt-right in the United States. A convergence of these forces allowed the CA conflict to erupt, which was then utilized by a network of actors to argue that Cambridge Analytica presented an alarming threat to democracy.

Chapter One demonstrated that on a theoretical level, privacy is an essential component of the democratic process, such that the deprivation of an individual's privacy erodes the foundations of the democratic system. I organized the democratic impacts of surveillance as *Self-discovery, Accountability, Erosion, and Bias Enforcement.* These categories are based on analyses of government and corporate surveillance, and yet these analyses have not yet been extended to a critique of voter surveillance. This final section will demonstrate that each of these categories of democratic impact were demonstrated during the CA conflict.

Surveillance Capitalism

Surveillance capitalism drove two components of the CA conflict, Facebook's encroachment of private spheres and the rise of the data brokerage industry. Zuboff describes the model of extraction in surveillance capitalism as continuously expanding into "legally and socially undefended territory until resistance is encountered."[371] Thus, Facebook adjusted their systems as was necessary to keep their userbase and regulators satisfied, while they continued data extraction largely unabated. The language of Facebook's privacy policies was found to be misleading by the OPC, the FTC, the Irish Data Commissioner, and other regulators. Once the issue of third-party access had been pointed out, Facebook waited years to fix the problem. Despite this regulatory rebuke, Facebook's profitability and userbase continued to grow.

Facebook was able to accomplish this scale of data collection in part because people have become inundated by an unreasonable burden of terms and conditions. The scale of contractual obligations in a technologically connected society speaks to Marx's theory of mandatory volunteerism.[372] Individuals must choose between refusing access to often necessary services, spending 244 hours per year reading terms and conditions,[373] or accepting the terms unread.

This scale of collection challenges concepts of consent and of privacy as a form of individual control. Facebook argued that individuals consented to Facebook's far

[371] Zuboff, 'Big Other', March 2015, 79.

[372] Marx, 'Surveillance and Society'.

[373] Mcdonald and Cranor, 'The Cost of Reading Privacy Policies'.

reaching data collection, but this consent was uninformed. This practice is common in surveillance capitalism, as the data collected by CA was also collected with the "consent" of users.[374] The introduction of algorithmic sorting via big data means that people no longer have control of "when, how, and to what extent information about them is communicated."[375] An algorithm processes seemingly trivial information, such as what music a person likes, and predicts consumer behaviour or political leanings. This process has increasingly eroded the power of individuals to meaningfully have, what Rule calls an "authentic option" to withhold information.[376] This information has financially benefitted many sectors of society, and the lessons learned from surveillance capitalism have translated into the political realm as well.

Unregulated Voter Analytics

Voter analytics have been enhanced greatly by the advent of surveillance capitalism. This process has directly contributed to the volume of information that political parties collect in an unregulated political market. Political data brokers like *Aristotle, the RNC, and i360* are collecting, processing, and analyzing vast quantities of incredibly detailed personal information about voters in the US. Much of this data is of a higher quality than that of CA.[377] Voters in the US have almost every detail of their lives assessed and modelled, albeit not accurately, on the assumption that information derived from algorithms may reveal and predict political behaviour. Thus, CA attempted to

[374] In Canada, Facebook users have received some justice for their data misuse as the OPC has found that Facebook and the *Thisisyourdigitallife* app did not obtain meaningful consent from their users. However no such standard exists in the US.[374]

[375] Westin, Alan F. Privacy and Freedom. 1st ed. New York: Atheneum, 1967. 7

[376] Rule, *Privacy in Peril.* 3

[377] Kroll, 'Cloak and Data'.

distinguish itself from its contemporaries by providing a relatively new product, psychographics, to an already saturated market.

Advertising to people based on their personality profiles is one of the few markets where PII had yet to see successful use in a Presidential election. And CA was certainly the most well known psychographic modeler. Despite their failure to effectively exploit these psychological profiles, CA brought practices that had been ongoing for over a decade to the forefront of an international discussion. They did so because CA's practices highlighted the risks of voter surveillance. Before the CA conflict, voters were unaware of the scope of the voter analytics industry, and as such, had no meaningful way to control the process.[378]

Barocas warned that such practices might have a chilling effect on democracy as people opt out of voting. [379] In the CA conflict, declining voter participation does not appear to be the case, as the 2018 midterm was the highest voter turnout since 1914. [380] But CA did demonstrate that unregulated political party data use contributes to other aspects of democratic erosion that surveillance scholars have predicted. Haggerty and Samatas argued that surveillance inherently erodes democracy as social norms, rights, freedoms, and trust in the institutions of power are all decayed.[381] Bennett, for instance, suggests that voter surveillance might undermine the national consensus by focusing voters on single-issue politics as politicians "shop for votes."[382] As the populous became

---

[378] Solove, *The Digital Person*.
[379] Barocas, 'The Price of Precision'.
[380] Ella Nilsen, 'The 2018 Midterms Had the Highest Turnout since before World War I', Vox, 10 December 2018, https://www.vox.com/policy-and-politics/2018/12/10/18130492/2018-voter-turnout-political-engagement-trump.

[381] Haggerty and Samatas, *Surveillance and Democracy*.
[382] Delacourt, *Shopping for Votes*.

increasingly informed by *polarized information*, politicians were able to optimize their popularity by pandering to the narrowest concerns that the voters expressed.[383]

These political messages were simplistic, emotional heuristics that were light on policy suggestions. Moreover, the messages skewed towards far-right white supremacist rhetoric - Trump's *Drain the swamp* and *Build the Wall* was a clear demonstration of these data-driven simplistic talking points. *Drain the swamp* became a popular rallying cry for Trump, but it was also disingenuous, a slogan meticulously focus-tested by CA years before they had worked for the Trump campaign. The results of which have eroded the quality of public discourse in the US.

Rise of the Alt-Right

Bias Enforcement has grown out of the lack of diverse information that people either gain access to, or choose to access, and this has undermined *Self-Discovery.* Boehme-Neßler argued that without access to dissident information, people are unable to grow intellectually and actively participate in a democratic process.[384] Surveillance capitalism's need to keep people engaged has resulted in increasingly polarized and extreme content delivered to people across numerous media. The result is an increase in the extremist rhetoric and beliefs that have become common in US politics. A recent story about the inability of a Twitter algorithm to distinguish white supremacist rhetoric from that of Republican politicians exemplifies this.[385] Though voter profiling and

---

[383] Sunstein, Cass R. Republic.Com. Princeton, N.J: Princeton University Press, 2001.
[384] Boehme-Neßler, 2016. 227
[385] Grace Panetta, 'Twitter Reportedly Won't Use an Algorithm to Crack down on White Supremacists Because Some GOP Politicians Could End up Getting Barred Too', Business Insider, accessed 21 June 2019, https://www.businessinsider.com/twitter-algorithm-crackdown-white-supremacy-gop-politicians-report-2019-4.

surveillance capitalism are not the sole cause for the rise of modern populism, these two factors have exacerbated the problem.

Cambridge Analytica garnered a lot of attention due to perceptions that it was a tool of politically empowering the fringe right-wing. Their funding and ownership had worked to elevate the alt-right for years and, following Trump's win, many alt-right beliefs have translated into policy with a disproportionately negative impact on marginalized peoples, including the separation of migrant families at the border.

The company's targeting of racial minorities exacerbated this perception and is exemplary of an underexplored aspect of voter surveillance, malicious use. Barocas noted that micro-targeting has the risk of marginalizing non-sympathetic voters who may be ignored by politicians.[386] Cambridge Analytica took this a step further and attempted to persuade non-sympathetic individuals not to vote, a tactic used alongside other racially motivated voter suppression activities.

The CA Conflict and the Invasion of "Privacy"

Many journalists drew attention to these structural issues, but they did not have the impact of the *psychological warfare* article. The Wylie article was the most effective at garnering attention because it introduced a human element to the conflict. Conversely, Nix was portrayed as an elitist villain of the story. Wylie used his moment of fame to deliver one concise and central message: Cambridge Analytica stole your personal information and is using it to threaten democracy. Candid interviews with Nix, and the companies connections to figures of the alt-right seemingly confirmed Wylie's claim. As a result, the public began to interrogate a variety of issues that they had, by and large,

[386] Barocas, 'The Price of Precision', 33.

ignored. Wylie and others helped to turn CA into the clear manifestation of the importance of privacy and the power of surveillance.

Surveillance capitalism and unregulated voter surveillance have fundamentally challenged our rights to informational privacy. When Alan Westin wrote *Privacy and Freedom* in 1963, he identified four states of privacy: *Solitude, Intimacy, Anonymity, and Reserve.*[387] Each of these categories is challenged by technology that played a prominent role in the CA conflict.

Solitude is defined as a state wherein an individual has a moment alone, away from jarring stimuli and left with their thoughts, they are in a complete state of privacy. Without solitude, an individual is deprived of quiet reflection. This time for reflection is necessary for personal growth and gives a person time to organize their thoughts and form opinions away from the influence of others.[388] However, the ability to achieve such peace is antithetical to the demands of surveillance capitalism, every moment an individual is unplugged from their device is a moment that data is not collected and profiled, or where they are free from advertising. An alert from your cellphone may tell you that your friend has posted something on Facebook, or you may receive a call, or work might send an email. The average person checks their phone every 12 minutes, and every year smartphone addiction is worsening.[389] Achieving true solitude is possible in the modern world, but it is becoming increasingly rare. The consequences of this on a democratic system are apparent; individuals have less time to critically examine policies or candidates and this hinders the development of the moral autonomy necessary for

[387] Westin, *Privacy and Freedom*, 31.

[388] Gavison, 'Privacy and the Limits of Law', 445.

[389] 'Communications Market Report'.

deliberative decision making.[390] The result of this can be a less informed, and more biased electorate.

Intimacy is a moment when an individual is in a small group and can achieve a "close, relaxed, and frank relationship."[391] Intimacy is still present today. However, modern intimacy is different from that which Westin envisioned. Increasingly intimacy is being mediated through third-parties such as Facebook. Indeed, Facebook has actively integrated itself into this role as a mediator of socialization and has sold access to this information for a considerable profit.[392] This information has also been used to leverage political participation. In the CA conflict, Facebook-mediated friendships facilitated Kogan's extraction of large quantities of information which was then used to model personality scores. Moreover, in 2012, the Obama campaign exploited knowledge of these friendships to increase voter participation; as noted above, "people don't trust campaigns. They don't even trust media organizations. Who do they trust? Their friends."[393] The use of our friendships for political or economic gain harkens to democratic erosion, as this exploitation of intimacy undermines the accountability of, and trust in the democratic process. Intimacy is essential for inter-personal growth and increasing trust and community.[394] An erosion of community further erodes the stability of the institutions of democracy.

---

[390] Gavison, 'Privacy and the Limits of Law', 450.

[391] Ibid. 31

[392] Alex Hern, 'Facebook Shared Private User Messages with Netflix and Spotify', *The Guardian*, 19 December 2018, sec. Technology, https://www.theguardian.com/technology/2018/dec/19/facebook-shared-user-data-private-messages-netflix-spotify-amazon-microsoft-sony.

[393] Scherer, 'Friended'.

[394] Westin, *Privacy and Freedom*, 38.

Westin describes *Anonymity* as a person's ability to be in public but unknown. "Unless he is a well-known celebrity, he does not expect to be personally identified."[395] Anonymity allows an individual to merge into the situational landscape. However, Westin notes that "knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom."[396] Westin argues one benefit of anonymity is the ability to critique ideas and governments without fear of persecution.[397] The importance of *anonymity* is most apparent on Facebook, which argues that they are a public space, and yet they monitor everything on their website and model that information for profit. However, Facebook tracking also goes beyond its website. Tracking cookies and web analytics, much like the kind utilized by CA, link IP addresses to online activity, thus ensuring digital monitoring is occurring in almost all times online.

Anonymity is also an essential component of the secret ballot. It provides individuals with the ability to express their political preferences without fear of persecution. Databases like those held by i360, or the data that Carroll received from CA demonstrates that this may be an antiquated concept in the age of voter surveillance. Now political parties can know when voters last voted, and which candidate they supported, an issue Rubinstein takes note of as well.[398] A lack of anonymity online and while voting further erodes the accountability of a democracy. A lack of accountability between political parties and their population means that parties can know who their opponents are and where to find them. The Trump campaign demonstrated the democratic consequences

---

[395] Westin, *Privacy and Freedom*.31

[396] Ibid.

[397] Ibid.32

[398] Rubinstein, 'Voter Privacy in the Age of Big Data', 906.

of such a privacy violation when they attempted to dissuade political opponents from voting.

Reserve is the most intimate aspect of a person's privacy. It is the psychological barrier against unwanted intrusion; psychographic profiles were a threat to this last refuge of privacy, still untainted by big data. [399] "Even in the most intimate relations, communication of self to others is always incomplete and is based on the need to hold back some parts of one's self as either too personal and sacred or too shameful and profane to express."[400] For the sake of convenience and addiction, *solitude* was interrupted by the platform economy, *intimacy* was managed by it, and *anonymity* made near impossible because of it. Until now, *reserve*, the inner-most barrier and the most private aspect of a person had remained untouched.

When CA finally gained widespread attention, people had become so accustomed to privacy intrusions in their daily life that there was little they had left as private. But their inner thoughts, their personality, their decision-making capacity, had remained private and personal things, and it was the last vestige of informational privacy that had yet remained untouched by surveillance. People believed that CA successfully used Facebook data to manipulate them, and they were justifiably angry about it. This was the spark that elevated the CA conflict, which tapped into a collective outrage fueled by an ever-expanding surveillance apparatus constantly seeking new sources of personal information.

Was this just a privacy conflict?

---

[399] Westin, *Privacy and Freedom*.31
[400][400] Ibid.

The analysis above suggests that this conflict could be read as a privacy conflict. But does that tell the whole story? The answer to this is yes and no. Many aspects of the CA conflict stem from privacy violations. Data regulators treated this as a privacy conflict, and many of the proposed solutions recommend increasing transparency and implementing restrictions on political party data use.[401] But data regulators are limited by the nature of the laws they are tasked to enforce. The role of data regulators is to protect data and privacy, not to serve as stewards of democratic stability. Thus, as the harms of voter surveillance expanded beyond mere privacy violations, these regulators were extended beyond the scope of their mandate. Data-regulators did an excellent job at filling the legislative gap, and in the case of CA they demonstrated that data crimes are real crimes, and will be treated as such. But they are still constrained by the nature of the laws they are meant to enforce, and these laws are insufficient to deal with the democratic harms of voter surveillance. Thus, this conflict has forced a discussion about the changing nature of privacy in an age of voter surveillance.

Bennett notes that part of the issue with privacy movements is the acute and personal nature of privacy violations.[402] Briant noted this in her testimony as well. This meant that previous privacy conflicts were very personal experiences, making it difficult to popularize outrage. Individuals would suffer the effects of privacy violations alone. They would feel the effects of having their identity stolen, or their banking information compromised, alone. The CA conflict was not just an invasion of personal privacy, it was a collective threat. The way actors framed this issue transcends the privacy implications

[401] Denham, 'Democracy Disrupted?'

[402] Bennett, *Privacy Advocates*. 96

of the conflict and reasserts something that has been argued extensively in the privacy and surveillance literature. The ICO report *Democracy Disrupted* warned *"*we are at risk of developing a system of voter surveillance by default. This could have a damaging long-term effect on the fabric of our democracy and political life."[403] The framing of CA as a threat to democracy meant that this was an issue that affects every aspect of democratic societies.

This framing was useful for fostering outrage about micro-targeting practices. But I am concerned that allocating too much focus on CA distracts from the wider structural issues that remain unaddressed. Political parties around the world have continued to use disturbingly detailed data from Facebook and other brokers as political tools. Bennett argues that voter surveillance is *Janus-faced*; as such, we must judge its complexities by a different set of criteria than surveillance by corporations or governments.[404] This thesis demonstrates that voter surveillance shares many of the same social problems associated with traditional surveillance structures such as bias enforcement, democratic erosion, and limiting self discovery and accountability; as such political parties must be judged in these contexts. CA's activities present a gap in the analysis - what happens when voter surveillance is used maliciously? CA demonstrates that the biggest risk voter surveillance poses is when actors wield it to strip away democratic rights. Yes, political parties do need data on their voters, but this thesis has detailed the undemocratic nature of unregulated voter surveillance. As such, this system, left unchecked, will only continue to erode the institutions of democracy.

[403] Denham, 'Democracy Disrupted?', 9.

[404] Bennett, 'Trends in Voter Surveillance in Western Societies', 14.

Bibliography

Abramowwitz, Michael J. ‘Freedom in the World 2018’. Freedom House, 13 January 2018. https://freedomhouse.org/report/freedom-world/freedom-world-2018.

Albright, Jonathan. ‘The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle’. Medium, 21 March 2018. https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747.

Altman, Irwin. ‘Privacy: “A Conceptual Analysis”’. *Environment and Behavior; Beverly Hills, Calif.* 8, no. 1 (1 March 1976): 7–30.

Andrejevic, Mark. ‘Ubiquitous Surveillance’. In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon 1948, 91–99. Book, Whole. New York;Abingdon, Oxon; Routledge, 2012. http://uvic.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwdV07C8IwED6sLoKDT9SqZBYUm_RhZ1EcXAR3SWsyVvD5971LYxWpYzIceZEv9-W-OwDB54vZz51AuC2EiCT6bsuYyu95gfZC6SVKxNqI1L7UZPDOCvGbOdEKT_7_zyDchEZz7qCrQ4KO_a5gXIgyQY_DytIDdP1E_EnBY9rhV-5PCzGbJlRJdtCCisra4OzkswPTIlyHEb9N72F21ux6vzwUFQvC_WLXPA6wC-5mfVhtZ2T3aDmZox0n70FDUiR7djOKt1MfWOBF0SnlqYil9BE9pFwowXWScJWkvvIH0CkzNSzvdqGOEM9z0mAENY2HWo3zWU7M-rwADxFz9Q.

‘Andrew Scheer’s Campaign Manager Says He Builds Creepy Psychological Profiles of Voters Too’. *PressProgress* (blog), 22 March 2018. https://pressprogress.ca/andrew-scheers-campaign-manager-says-he-builds-creepy-psychological-profiles-of-voters-too/.

Anglim, Christopher, Gretchen Nobahar, and Jane E Kirtley. *Privacy Rights in the Digital Age*. Amenia, UNITED STATES: Grey House Publishing, 2016. http://ebookcentral.proquest.com/lib/uvic/detail.action?docID=4454671.

Baldwin-Philippi, Jessica. ‘The Myths of Data-Driven Campaigning’. *Political Communication* 34, no. 4 (2 October 2017): 627–33. https://doi.org/10.1080/10584609.2017.1372999.

Barocas, Solon. ‘The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process’. In *Proceedings of the First Edition Workshop on Politics, Elections and Data*, 31–36. PLEAD ’12. New York, NY, USA: ACM, 2012. https://doi.org/10.1145/2389661.2389671.

Bashyakarla, Varoon, Stephanie Hankey, Amber Macintyre, Raquel Renno, and Gary Wright. ‘Personal Data:Political PersuasionInside the Influence Industry. How It Works.’ Data and Politics Team. Tactical Technology Collective, March 2019. https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf.

Bennett, Colin. *Privacy Advocates: Resisting the Spread of Surveillance*. The MIT Press, 2008.

Bennett, Colin. ‘The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies’. *First Monday* 18, no. 8 (25 July 2013). https://doi.org/10.5210/fm.v18i8.4789.

Bennett, Colin J. ‘Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications’. *Surveillance & Society* 13, no. 3/4 (26 October 2015): 370–84. https://doi.org/10.24908/ss.v13i3/4.5373.

Boehme-Neßler, Volker. ‘Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection’. *International Data Privacy Law* 6, no. 3 (1 August 2016): 222–29. https://doi.org/10.1093/idpl/ipw007.

Bozdag, Engin, and Jeroen van den Hoven. ‘Breaking the Filter Bubble: Democracy and Design’. *Ethics and Information Technology* 17, no. 4 (1 December 2015): 249. https://doi.org/10.1007/s10676-015-9380-y.

‘Brad Parscale Digital Director Trump | User Clip | C-SPAN.Org’. Accessed 2 February 2019. https://www.c-span.org/video/?c4637517/brad-parscale-digital-director-trump.

Briant, Emma. Evidence for the US Senate Judiciary Committee on Cambridge Analytica and SCL Group, § US Sennate Judiciary Committee on Cambridge Analytica and SCL Group (2018). https://www.judiciary.senate.gov/imo/media/doc/Professor%20Emma%20L.%20Briant%20Report%20on%20Cambrige%20Analytica.pdf.

Briant, Emma. Written Evidence. ‘Three Explanatory Essays Giving Context and Analysis to Submitted Evidence’. Written Evidence, 16 April 2018. FKN0071. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/written/88559.pdf.

Burkell, Jacquelyn, Alexandre Fortier, Lorraine (Lola) Yeung Cheryl Wong, and Jennifer Lynn Simpson. ‘Facebook: Public Space, or Private Space?’ *Information, Communication & Society* 17, no. 8 (14 September 2014): 974–85. https://doi.org/10.1080/1369118X.2013.870591.

Cadwalladr, Carole. ‘Cambridge Analytica a Year on: “A Lesson in Institutional Failure”’. *The Guardian*, 17 March 2019, sec. UK news. https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie.

Cadwalladr, Carole. ‘Google, Democracy and the Truth about Internet Search’. *The Observer*, 4 December 2016, sec. Technology. https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook.

Cadwalladr, Carole. ‘“I Made Steve Bannon’s Psychological Warfare Tool”: Meet the Data War Whistleblower’. *The Guardian*, 18 March 2018, sec. News. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Cadwalladr, Carole. ‘The Great British Brexit Robbery: How Our Democracy Was Hijacked’. *The Guardian*, 7 May 2017, sec. Technology. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

Caillaud, Bernard, and Jean Tirole. ‘Parties as Political Intermediaries’. *The Quarterly Jouranl of Economics* 117, no. 4 (November 2002): 1453–89.

‘Cambridge Analytica Explained: Data and Elections’. Privacy International. Accessed 22 May 2019. http://privacyinternational.org/feature/975/cambridge-analytica-explained-data-and-elections.

Carol Davidsen. ‘You Are Not a Target’. presented at the Imagine all the People: the future of civic tech, New York City, 4 June 2015. https://www.youtube.com/watch?v=LGiiQUMaShw.

Carroll, David. ‘Just Got My Data from Cambridge Analytica/SCL by Request. Yes, They Do Have Correct Voter and Personal Information about Me. More to Come.’ Twitter. *David Carroll Twitter* (blog), 27 March 2017. https://twitter.com/profcarroll/status/846347516341837825?lang=en.

Castro, Rafa Fernandez de. ‘A Massive Data Breach Exposed Personal Info for 93.4 Million Mexicans’. Splinter. Accessed 5 April 2019. https://splinternews.com/a-massive-data-breach-exposed-personal-info-for-93-4-mi-1793856429.

Ch, Olivia, ler · CBC News · Posted: Apr 01, and 2019 9:40 PM ET | Last Updated: April 2. ‘Privacy Commissioner, Chief Electoral Officer Issue Privacy Guidelines for Federal Political Parties | CBC News’. CBC, 2 April 2019. https://www.cbc.ca/news/politics/powerandpolitics/politics-privacy-data-elections-canada-1.5080523.

Channel 4 News. *Cambridge Analytica: Undercover Secrets of Trump’s Data Firm*. Accessed 29 January 2019. https://www.youtube.com/watch?v=cy-9iciNF1A&t=16s.

Chris Vickery. Breach of Personal Information Involving Cambridge Analytica, Pub. L. No. 123, § Standing Committee on Access to Information, Privacy, and Ethics (2018).

Colins, Damien. ‘Disinformation and “Fake News”: Interim Report’. Session 2017-2019. United Kingdom House of Commons: Digital, Culture, Media and Sport Committee, 24 July 2018. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

‘Communications Market Report’. Ofcom, 2 August 2018. https://www.ofcom.org.uk/__data/assets/pdf_file/0022/117256/CMR-2018-narrative-report.pdf.

‘Community Mobilization and Fundraising Platform | BSD Tools |’. Blue State Digital. Accessed 9 May 2019. https://tools.bluestatedigital.com/.

Confessore, Nicholas, and Danny Hakim. ‘Data Firm Says “Secret Sauce” Aided Trump; Many Scoff’. *The New York Times*, 20 January 2018, sec. U.S. https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html.

Constantine, Josh. ‘Facebook Is Shutting Down Its API For Giving Your Friends’ Data To Apps’. *TechCrunch* (blog), 28 April 2015. http://social.techcrunch.com/2015/04/28/facebook-api-shut-down/.

Couldry, Nick. ‘Surveillance-Democracy’. *Journal of Information Technology & Politics* 14, no. 2 (3 April 2017): 182–88. https://doi.org/10.1080/19331681.2017.1309310.

Crosby, Andrew, and Jeffrey Monaghan. ‘Settler Colonialism and the Policing of Idle No More’. *Social Justice* 43, no. 2 (144) (2016): 37–57.

‘Data Brokers: A Call for Transparency and Accountability’. Federal Trade Comission, May 2014. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-

transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Davies, Harry. 'Facebook Told Me It Would Act Swiftly on Data Misuse – in 2015 | Harry Davies'. *The Guardian*, 26 March 2018, sec. Opinion. https://www.theguardian.com/commentisfree/2018/mar/26/facebook-data-misuse-cambridge-analytica.

Davies, Simon. '13. Spanners in the Works: How the Privacy Movement Is Adapting to the Challenge of Big Brother'. In *Visions of Privacy*, edited by Colin J. Bennett and Rebecca Grant. Toronto: University of Toronto Press, 1999. https://doi.org/10.3138/9781442683105-015.

Davis, Harry. 'Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users | US News'. The Guardian, 11 December 2015. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

'Defeat Crooked Hillary'. YouTube, 2016. https://www.youtube.com/channel/UCRvnu9aLecF_JM6D0E0ga-w.

Delacourt, Susan. *Shopping for Votes: How Politicians Choose Us and We Choose Them*. Updated second edition. Madeira Park, BC, Canada: Douglas & McIntyre, 2016.

Denham, Elizabeth. 'Democracy Disrupted?: Personal Information and Political Influence'. Information Commissioner's Office, 11 July 2018. https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf.

Denham, Elizabeth. 'Investigation into the Use of Data Analytics in Political Campaigns'. A report to Parliament. Information Commissioner's Office, 6 November 2018. https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

Digman, John M. 'Personality Structure: Emergence of the Five-Factor Model'. *Annual Review of Psychology* 41 (1 January 1990): 417.

Dobber, Tom, Damian Trilling, Natali Helberger, and Claes H. de Vreese. 'Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques'. *Internet Policy Review* Volume 6, no. Issue 4 (1 December 2017). https://doaj.org.

Ebenstein, Julie. 'We're Suing California Because It Threw Out More Than 45,000 Ballots in the 2016 Presidential Election Over Handwriting "Mismatches"'. American Civil Liberties Union, 24 August 2017. https://www.aclu.org/blog/voting-rights/fighting-voter-suppression/were-suing-california-because-it-threw-out-more-45000.

Eligon, John. 'Hate Crimes Increase for the Third Consecutive Year, F.B.I. Reports'. *The New York Times*, 13 November 2018, sec. U.S. https://www.nytimes.com/2018/11/13/us/hate-crimes-fbi-2017.html.

Elkin, Emily. 'The Five Types of Trump Voters'. Text/html. Voter Study Group. Democracy Fund, 11 June 2017. https://www.voterstudygroup.org/publications/2016-elections/the-five-types-trump-voters.

Ericson, Richard V, and Kevin D Haggerty. *The New Politics of Surveillance and Visibility*. Green College Thematic Lecture Series. Toronto; Buffalo: University of Toronto Press, 2006. http://www.deslibris.ca/ID/418803.

Fenwick, MIchael. Breach of Personal Information Involving Cambridge Analytica and Facebook, § Standing Committee on Access to Information, Privacy and Ethics (2018). https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-123/evidence.

Flaherty, David H. *Privacy in Colonial New England*. University Press of Virginia, 1972.

Ford, Matt. 'How Texas Republicans Got Away With a Racially Discriminatory Electoral Map'. *The New Republic*, 25 June 2018. https://newrepublic.com/article/149357/texas-republicans-got-away-racially-discriminatory-electoral-map.

Foucault, Michel, and Alan Sheridan. *Discipline and Punish*. Vintage Books, 1995.

Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation'. *Philosophy & Technology* 30, no. 1 (1 March 2017): 9–37. https://doi.org/10.1007/s13347-016-0219-1.

Gandy, Oscar H. *The Panoptic Sort: A Political Economy of Personal Information*. Critical Studies in Communication and in the Cultural Industries. Boulder, Colo: Westview, 1993.

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century*. 1st ed. Beijing ; Cambridge: O'Reilly, 2000.

Gavison, Ruth. 'Privacy and the Limits of Law'. *The Yale Law Journal* 89, no. 3 (1980): 421–71. https://doi.org/10.2307/795891.

Gerring, John. 'What Is a Case Study and What Is It Good For?' *The American Political Science Review* 98, no. 2 (2004): 341–54.

Gomez, Melissa. 'Charlottesville Car Attack Suspect Pleads Not Guilty to Federal Hate Crimes'. *The New York Times*, 6 July 2018, sec. U.S. https://www.nytimes.com/2018/07/05/us/charlottesville-plea-hate-crimes.html.

'Google Trends'. Google Trends- Cambridge Analytica. Accessed 22 May 2019. https://trends.google.com/trends/explore?date=2017-01-02%202019-05-22&q=CAmbridge%20analytica.

Grassegger, Hannes, and Mikael Krogerus. 'The Data That Turned the World Upside Down'. *Vice* (blog), 28 January 2017. https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.

Groenendyk, Eric. 'Current Emotion Research in Political Science: How Emotions Help Democracy Overcome Its Collective Action Problem'. *Emotion Review* 3, no. 4 (October 2011): 455–63. https://doi.org/10.1177/1754073911410746.

Guynn, Jessica. 'Facebook Just Shed $130 Billion in Two Hours, Mark Zuckerberg Lost $16.8 Billion'. USA TODAY, 25 July 2018. https://www.usatoday.com/story/tech/2018/07/25/facebook-catches-cambridge-analytica-chill-user-growth-slows/837683002/.

Haggerty, Kevin D., and Minas Samatas. *Surveillance and Democracy*. London, UNITED KINGDOM: Taylor & Francis Group, 2010. http://ebookcentral.proquest.com/lib/uvic/detail.action?docID=537878.

Hannes Grassenger, Von, and Mikael Krogerus. ‘Ich habe nur gezeigt, dass es die Bombe gibt’. *Das Magazin* (blog), 3 December 2016. https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/.

Healy, Jack. ‘Arrested, Jailed and Charged With a Felony. For Voting.’ *The New York Times*, 10 August 2018, sec. U.S. https://www.nytimes.com/2018/08/02/us/arrested-voting-north-carolina.html.

Hern, Alex. ‘Facebook Shared Private User Messages with Netflix and Spotify’. *The Guardian*, 19 December 2018, sec. Technology. https://www.theguardian.com/technology/2018/dec/19/facebook-shared-user-data-private-messages-netflix-spotify-amazon-microsoft-sony.

Hersh, Eitan. Written Testimony of Eitan Hersh, § HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY (2018). https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Hersh%20Testimony1.pdf.

Hersh, Eitan D. *Hacking the Electorate: How Campaigns Perceive Voters*. Cambridge: Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781316212783.

Hill, Kashmir. ‘Max Schrems: The Austrian Thorn In Facebook’s Side’. Forbes. Accessed 9 June 2019. https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/.

Issenberg, Sasha. ‘Cruz-Connected Data Miner Aims to Get Inside U.S. Voters’ Heads’. Bloomberg, 12 November 2015. https://www.bloomberg.com/news/features/2015-11-12/is-the-republican-party-s-killer-data-app-for-real-.

Issenberg, Sasha. ‘How the Obama Campaign’s Top-Secret Project Narwhal Will Change the 2012 Race’. Slate Magazine, 15 February 2012. https://slate.com/news-and-politics/2012/02/project-narwhal-how-a-top-secret-obama-campaign-program-could-change-the-2012-race.html.

Issenberg, Sasha. *The Victory Lab: The Secret Science of Winning Campaigns*. First paperback edition. New York: B/D/W/Y, Broadway Books, 2013.

Issenberg, Sasha, and Joshua Green. ‘Why the Trump Machine Is Built to Last Beyond the Election’. Bloomberg, 27 October 2016. https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go.

Julia Angwin, Terry Parris Jr. ‘Facebook Lets Advertisers Exclude Users by Race’. Text/html. ProPublica, 28 October 2016. https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

Kaiser, Brittany. ‘Written Testimony to the Fake News Inquiry’, 17 April 2018. FKN0076. https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Brittany%20Kaiser%20Parliamentary%20testimony%20FINAL.pdf.

Kaye, Kate. ‘How the Trump Camp’s Data Inexperience Helped Propel His Win’. AdAge, 14 December 2016. https://adage.com/article/campaign-trail/trump-camp-s-inexperience-set-stage-rnc-data-win/307105/.

Kaye, Kate. ‘In D.C., Cambridge Analytica Not Exactly Toast of the Town’. Ad Age, 18 August 2016. https://adage.com/article/campaign-trail/cambridge-analytica-toast/305439/.

Kaye, Kate. ‘Trump’s First Fundraising Email Had a 60% Spam Rate’. Ad Age, 23 June 2016. https://adage.com/article/campaign-trail/trump-s-fundraising-email-a-60-spam-rate/304673.

Keck, Margaret E., and Kathryn Sikkink. *Activists Beyond Borders : Advocacy Networks in International Politics*. Cornell University Press, 1998.

Kirchgaessner, Stephanie. ‘Cambridge Analytica Used Data from Facebook and Politico to Help Trump’. *The Guardian*, 26 October 2017, sec. Technology. https://www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump.

Knibbs, Kate. ‘Error Exposes 1.5 Million People’s Private Medical Records on Amazon Web Services [UPDATED]’. Gizmodo. Accessed 5 April 2019. https://gizmodo.com/security-hell-private-medical-data-of-over-1-5-million-1731548110.

Kogan, Alexander. Fake News, HC 363, § Digital, Culture, Media and Sport Committee (2018). http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/81931.pdf.

Kogan, Alexandr. Written Evidence: Fake News, Pub. L. No. FKN0077, § DCMS, 1 (2018).

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

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. ‘Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks’. *Proceedings of the National Academy of Sciences* 111, no. 24 (17 June 2014): 8788–90. https://doi.org/10.1073/pnas.1320040111.

Krasnova, Hanna, Natasha F. Veltri, and Oliver Günther. ‘Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus’. *Business & Information Systems Engineering* 4, no. 3 (June 2012): 127–35. https://doi.org/10.1007/s12599-012-0216-6.

Kreiss, Daniel. *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy*. Oxford Studies in Digital Politics. New York, NY: Oxford University Press, 2016.

Kroll, Andy. ‘Cloak and Data: The Real Story behind Cambridge Analytica’s Rise and Fall’. *Mother Jones* (blog), May 2018. https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analytica-robert-mercer/.

Lapowsky, Issie. ‘What Did Cambridge Analytica Really Do for Trump’s Campaign?’ *Wired*, 26 October 2017. https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/.

Leibowitz, Jon, J. Thomas Rosch, and Julie Brill. 'In the Matter of Facebook, Inc., a Corporation'. Complaint. United States of America: Federal Trade Comission, n.d. https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

Lewis, Paul, and Paul Hilder. 'Former Cambridge Analytica Exec Says She Wants Lies to Stop'. *The Guardian*, 23 March 2018, sec. UK news. https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies.

Lewis, Paul, and Paul Hilder. 'Leaked: Cambridge Analytica's Blueprint for Trump Victory'. *The Guardian*, 23 March 2018, sec. UK news. https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

LoGiurato, Brett. 'Mitt Romney Has A New Strategy To Dominate The Facebook Campaign Wars'. Business Insider. Accessed 14 February 2019. https://www.businessinsider.com/mitt-romney-campaign-facebook-social-media-zac-moffatt-barack-obama-2012-6.

Lopez, Mark Hugo, and Jens Manuel Krogstad. 'Black Voter Turnout Fell in 2016 US Election'. *Pew Research Center* (blog), 12 May 2017. http://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

Lyon, David. *Surveillance after Snowden*. Polity Press, 2015.

Lyon, David. 'Why Where You Are Matters: Mundane Mobilities, Transparent Technologies, and Digital Discrimination'. In *Surveillance and Security*. Accessed 22 January 2019. https://www-igi-global-com.ezproxy.library.uvic.ca/chapter/you-matters-mundane-mobilities-transparent/48353.

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

Main, Thomas James. *The Rise of the Alt-Right*. Washington, D.C: Brookings Institution Press, 2018.

Martineau, Paris. 'Facebook Is Tracking You on over 8.4 Million Websites'. The Outline. Accessed 10 January 2019. https://theoutline.com/post/4578/facebook-is-tracking-you-on-over-8-million-websites.

Marwick, Alice E., and danah boyd. 'Networked Privacy: How Teenagers Negotiate Context in Social Media'. *New Media & Society* 16, no. 7 (1 November 2014): 1051–67. https://doi.org/10.1177/1461444814543995.

Marx, Gary. 'Surveillance and Society'. In *Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information*, 37–53. New York: Routledge. Accessed 10 December 2018. http://web.mit.edu/gtmarx/www/softsurveillance.html.

McCrae, Robert R., and Paul T. Costa. 'Comparison of EPI and Psychoticism Scales with Measures of the Five-Factor Model of Personality'. *Personality and Individual*

Differences 6, no. 5 (January 1985): 587–97. https://doi.org/10.1016/0191-8869(85)90008-X.

Mcdonald, Aleecia M, and Lorrie Faith Cranor. 'The Cost of Reading Privacy Policies', n.d., 26.

Meyer, Robinson. 'YouTube Removed the "Hail, Trump" Video From Search - The Atlantic'. The Atlantic, 20 March 2018. https://www.theatlantic.com/technology/archive/2018/03/youtube-removes-the-atlantics-hail-trump-video-from-search/555941/.

Milder, Zachary. 'Robert Mercer's Secret Adventure as a New Mexico Cop'. *Bloomberg*, 28 March 2018. https://www.bloomberg.com/news/features/2018-03-28/robert-mercer-s-secret-adventure-as-a-new-mexico-cop.

Molly Schweickert. 'How Digital Advertising Worked for the US 2016 Presidential Campaign'. D3con, 12 May 2017. https://www.youtube.com/watch?v=bB2BJjMNXpA.

Murray, Gregg, and Anthony Scime. 'Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies'. *Journal of Political Marketing* 9, no. 3 (July 2010): 143–66. https://doi.org/10.1080/15377857.2010.497732.

Navarro, Mireya, and Somini Sengupta. 'Contesting the Vote: Black Voters; Arriving at Florida Voting Places, Some Blacks Found Frustration'. *The New York Times*, 30 November 2000, sec. U.S. https://www.nytimes.com/2000/11/30/us/contesting-vote-black-voters-arriving-florida-voting-places-some-blacks-found.html.

Nelson, Libby. '"Why We Voted for Donald Trump": David Duke Explains the White Supremacist Charlottesville Protests'. Vox, 12 August 2017. https://www.vox.com/2017/8/12/16138358/charlottesville-protests-david-duke-kkk.

Nilsen, Ella. 'The 2018 Midterms Had the Highest Turnout since before World War I'. Vox, 10 December 2018. https://www.vox.com/policy-and-politics/2018/12/10/18130492/2018-voter-turnout-political-engagement-trump.

Nissenbaum, Helen Fay. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books, 2010.

Nix, Alexander. 'Cambridge Analytica - The Power of Big Data and Psychographics'. New York, September 2016. https://www.youtube.com/watch?v=n8Dd5aVXLCc&t=192s.

Nix, Alexander. Oral evidence: Fake News, HC 363, Pub. L. No. 363, § Digital, Culture, Media and Sport Committee, 1 (2018). http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/79388.pdf.

Noor, Poppy. '"The Fact That We Have Access to so Many Different Opinions Is Driving Us to Believe That We're in Information Bubbles" | The Psychologist'. The British Psychological Society, June 2017. https://thepsychologist.bps.org.uk/volume-30/june-2017/fact-we-have-access-so-many-different-opinions-driving-us-believe-were.

Onion, Rebecca. '"Build a Wall of Steel"'. Slate Magazine, 17 January 2019. https://slate.com/news-and-politics/2019/01/second-kkk-anti-immigrant-trump-wall.html.

O'Sullivan, Dan. 'The RNC Files: Inside the Largest US Voter Data Leak'. UpGuard, 12 December 2018. https://www.upguard.com/breaches/the-rnc-files.

Panetta, Grace. 'Twitter Reportedly Won't Use an Algorithm to Crack down on White Supremacists Because Some GOP Politicians Could End up Getting Barred Too'. Business Insider. Accessed 21 June 2019. https://www.businessinsider.com/twitter-algorithm-crackdown-white-supremacy-gop-politicians-report-2019-4.

Pariser, Eli. *The Filter Bubble*. Penguin Press, 2011.

Parscale, Brad. The Frontline Interview: Brad Parscale. Interview by James Jacoby. Video, 8 August 2018. https://www.pbs.org/wgbh/frontline/interview/brad-parscale/.

Perez, Sarah. 'Google's CEO Thinks Android Users Know How Much Their Phones Are Tracking Them'. *TechCrunch* (blog). Accessed 21 December 2018. http://social.techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them/.

Pilkington, Ed, and Amanda Michel. 'Obama, Facebook and the Power of Friendship: The 2012 Data Election'. *The Guardian*, 17 February 2012, sec. US news. https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election.

Posner, Sarah. 'How Donald Trump's Campaign Chief Created an Online Haven for White Nationalists'. Mother Jones, 22 August 2016. https://www.motherjones.com/politics/2016/08/stephen-bannon-donald-trump-alt-right-breitbart-news/.

Pot, Justin. 'Facebook Is Tracking Your Phone's Location, Here's How to Review Your History'. How-To Geek. Accessed 10 January 2019. https://www.howtogeek.com/fyi/facebook-is-tracking-your-phones-location-heres-how-to-review-your-history/.

'Psychographic Data | SocialValues Dataset | Environics Analytics'. Accessed 25 February 2019. https://www.environicsanalytics.com/en-ca/data/psychographic.

Rankin, Andrew. 'All of Canada's Federal Political Parties Collecting "Vast Amount" of Personal Information'. The Chronical Herald, 3 July 2019. http://www.thechronicleherald.ca/news/local/all-federal-political-parties-collecting-vast-amount-of-data-329496/.

'Reaching Voters'. DSPolitical. Accessed 9 May 2019. https://www.dspolitical.com/services/reaching-voters/.

Robertson, Adi. 'Netflix Documentary The Great Hack Turns the Cambridge Analytica Scandal into High Drama'. The Verge, 30 January 2019. https://www.theverge.com/2019/1/30/18200049/the-great-hack-cambridge-analytica-netflix-documentary-film-review-sundance-2019.

Roderick, Leanne. 'Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry'. *Critical Sociology* 40, no. 5 (1 September 2014): 729–46. https://doi.org/10.1177/0896920513501350.

Rubinstein, Ira. 'Voter Privacy in the Age of Big Data'. *SSRN Electronic Journal*, 2014. https://doi.org/10.2139/ssrn.2447956.

Rule, James B. *Privacy in Peril*. Oxford, UK ; New York: Oxford University Press, 2007.

Rule, James B. *Private Lives and Public Surveillance: Social Control in the Computer Age*. 1st Schocken ed. New York: Schocken Books, 1973.

Sartori, Giovanni. 'Party Types, Organisation and Functions'. *West European Politics* 28, no. 1 (1 January 2005): 5–32. https://doi.org/10.1080/0140238042000334268.

Scherer, Michael. 'Friended: How the Obama Campaign Connected with Young Voters'. *Time*, 20 November 2012. http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/.

Schoeman, Ferdinand. 'Privacy: Philosophical Dimensions'. *American Philosophical Quarterly* 21, no. 3 (1984): 199–213.

Schroepfer, Mike. Fake News, § DCMS (2018).

Schwartz, Paul M. 'Privacy and Democracy in Cyberspace'. *Vanderbilt Law Review* 52, no. 6 (1 November 1999): 1609.

Silverman, Craig. 'Cambridge Analytica Says It Won The Election For Trump. Here's What They're Actually Talking About.' BuzzFeed News, 20 March 2018. https://www.buzzfeednews.com/article/craigsilverman/cambridge-analytica-says-they-won-the-election-for-trump.

Silverman, Jacob. 'Privacy under Surveillance Capitalism'. *Social Research: An International Quarterly* 84, no. 1 (19 May 2017): 147–64.

Sloane, Garett. 'Sean Parker Says Facebook Was Designed to Be Addictive'. AdAge, 9 November 2017. https://adage.com/article/digital/sean-parker-worries-facebook-rotting-children-s-brains/311238.

Smith, Robert Ellis, Eric Siegel, and James S Sulanowski. *War Stories: Accounts of Persons Victimized by Invasions of Privacy*. Providence, R.I.: Privacy Journal, 1993.

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. Ex Machina. New York: New York University Press, 2004.

Stewart, Emily. 'Lawmakers Seem Confused about What Facebook Does — and How to Fix It'. Vox, 10 April 2018. https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations.

'Stolen Details of 3.3m Hello Kitty Fans – Including Kids – Published Online'. *Naked Security* (blog), 10 January 2017. https://nakedsecurity.sophos.com/2017/01/10/stolen-details-of-3-3m-hello-kitty-fans-including-kids-published-online/.

Sumpter, David. 'My Interview with Aleksandr Kogan: What Cambridge Analytica Were Trying to Do and Why Their…'. Medium, 22 April 2018. https://medium.com/@Soccermatics/my-interview-with-aleksander-kogan-what-cambridge-analytica-were-trying-to-do-and-why-their-f869ef65d945.

Tactical Technology Collective, and Becky Kazansky. 'FCJ-195 Privacy, Responsibility, and Human Rights Activism'. *The Fibreculture Journal*, no. 26 (22 December 2015): 190–208. https://doi.org/10.15307/fcj.26.195.2015.

Tesfaye, Sophia. 'NRA Props up Trump's Flailing Campaign with Multi-Million Dollar Benghazi-Themed Ad Buy'. Salon, 29 June 2016. https://www.salon.com/2016/06/29/nra_props_up_trumps_flailing_campaign_with_multi_million_dollar_benghazi_themed_ad_buy/.

The Advertising Research Foundation. 'The Advertising Research Foundation Announces the Winners for The ARF David Ogilvy Awards', 21 March 2017. https://www.prnewswire.com/news-releases/the-advertising-research-foundation-announces-the-winners-for-the-arf-david-ogilvy-awards-300425825.html.

'The Aggregate IQ Files, Part One: How a Political Engineering Firm Exposed Their Code Base'. UpGuard, 18 February 2019. https://www.upguard.com/breaches/aggregate-iq-part-one.

'The Beginner's Guide to Facebook Audiences and Targeting'. *AdEspresso* (blog). Accessed 7 June 2019. https://adespresso.com/guides/facebook-ads-beginner/demographic-targeting/.

'The Database'. i360. Accessed 20 February 2019. https://www.i-360.com/the-database/.

'The Retreat of Global Democracy Stopped in 2018'. *The Economist*, 8 January 2019. https://www.economist.com/graphic-detail/2019/01/08/the-retreat-of-global-democracy-stopped-in-2018.

Timmons, Heather. 'Cambridge Analytica's Biggest Customers'. Quartz, 2018. https://www.theatlas.com/charts/SyHHFzJqM.

Wang, Tova Andrea, and Janice Nittoli. *The Politics of Voter Suppression: Defending and Expanding Americans' Right to Vote*. Ithaca, UNITED STATES: Cornell University Press, 2012. http://ebookcentral.proquest.com/lib/uvic/detail.action?docID=3138356.

Wäscher, Till. 'Framing Resistance Against Surveillance: Political Communication of Privacy Advocacy Groups in the "Stop Watching Us" and "The Day We Fight Back" Campaigns'. *Digital Journalism* 5, no. 3 (16 March 2017): 368–85. https://doi.org/10.1080/21670811.2016.1254052.

Watkins, Eli, and Joe Sutton. 'Cambridge Analytica Files for Bankruptcy'. CNN, 18 May 2018. https://www.cnn.com/2018/05/18/politics/cambridge-analytica-bankruptcy/index.html.

Westin, Alan F. *Privacy and Freedom*. Atheneum, 1967.

Widmer, Ted. 'Draining the Swamp', 19 January 2017. https://www.newyorker.com/news/news-desk/draining-the-swamp.

Williams, Christine B., and Girish J. "Jeff" Gulati. 'Digital Advertising Expenditures in the 2016 Presidential Election'. *Social Science Computer Review* 36, no. 4 (1 August 2018): 406–21. https://doi.org/10.1177/0894439317726751.

Woodruff, Betsy. 'Trump Data Guru Alexander Nix: I Tried to Team Up With Julian Assange'. *The Daily Beast*, 25 October 2017, sec. politics. https://www.thedailybeast.com/trump-data-guru-i-tried-to-team-up-with-julian-assange.

Wylie, Chris. Fake News, § Digital, Culture, Media and Sport Committee (2018). http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81022.html.

Wylie, Chris. Written Statement to the United States Senate Committee on the Judiciary, § Committee on the Judiciary (2018). https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Wylie%20Testimony.pdf.

Wylie, Christopher. Breach of Personal Information Involving Cambridge Analytica and Facebook, § Standing Committee on Access to Information, Privacy and Ethics

(ETHI) (2018). https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-109/minutes.

Zimmer, Bob. 'Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Demcoratic Process:' The Standing Committee on Access to Information, Privacy and Ethics: Canadian House of Commons, June 2018. https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf.

Zimmer, Michael. 'Mark Zuckerberg's Theory of Privacy'. Washington Post, 3 February 2014. https://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html.

Zuboff, Shoshana. 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization'. *Journal of Information Technology* 30, no. 1 (March 2015): 75–89. https://doi.org/10.1057/jit.2015.5.

Zuboff, Shoshana. 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization'. *Journal of Information Technology* 30, no. 1 (March 2015): 75–89. https://doi.org/10.1057/jit.2015.5.

Zuboff, Shoshana. Surveillance Capitalism Is Eroding Democracy Recode Decode, Hosted By Kara Swisher podcast. Podcast, 20 February 2019. https://player.fm/series/recode-decode-hosted-by-kara-swisher-88572/shoshana-zuboff-surveillance-capitalism-is-eroding-democracy.

Zuckerberg, Mark. 'Facebook', 21 March 2018. https://www.facebook.com/facebook/posts/10157217558586729.