VOTER PRIVACY IN THE AGE OF BIG DATA

IRA S. RUBINSTEIN*

In the 2012 presidential election, the major candidates and political parties assembled extraordinarily detailed political dossiers on every American voter. These dossiers allowed them to target voters based on the likelihood of their registering to vote, supporting a candidate, donating to a campaign, or casting a ballot on Election Day. Despite this pervasive use of big data techniques, the privacy implications of data-driven campaigning have not been thoroughly explored, much less regulated. This Article suggests that political dossiers may be the largest unregulated assemblage of personal data in contemporary American life. It analyzes the main sources of voter data and the absence of privacy laws regulating the collection and use of such data. It also explores the potential privacy harms of voter microtargeting under the twin rubrics of information privacy (control over personal information) and political privacy (the personal sphere necessary for democratic deliberation and self-determination). This Article advocates a modest proposal for addressing these harms, which has two components. The first is a mandatory disclosure and disclaimer regime requiring political actors to be more transparent about their use of voter microtargeting and related campaign data practices. The second is the enactment of new federal privacy restrictions on commercial data brokers that would equally apply to firms providing data consulting services to political campaigns. This proposal is necessarily modest because it operates in the shadow of the First Amendment. The Article concludes by defending both components of the proposal against likely constitutional objections.

---

* Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law. For helpful comments, I thank Joseph Lorenzo Hall, Ronald Lee, Aleecia McDonald, William McGeveran, Peter Schuck, Joseph Turow, Felix Wu, Tal Zarsky, and workshop participants at the NYU Privacy Research Group and the Seventh Annual Privacy Law Scholars Conference. Thanks also to Ken Villa for outstanding research assistance.

INTRODUCTION

In *Franchise*, a 1955 short story by Isaac Asimov, an advanced computer holding "trillions of items" of information determines the outcome of the 2008 presidential election.[1] Every four years, the

1. Isaac Asimov, *Franchise*, *in* ELECTION DAY 2084: A SCIENCE FICTION ANTHOLOGY OF THE POLITICS OF THE FUTURE 11, 23 (Isaac Asimov & Martin H. Greenberg eds., 1984).

computer selects a single voter to represent the entire U.S. electorate.[2] It then asks this "Voter of the Year" a number of questions regarding his beliefs and preferences and feeds the answers into an attached "pattern-making" device, allowing the computer to apply a "top secret" method to pick the next president.[3] At the end of the story, Asimov observes that the sovereign citizens of this "Electronic Democracy" have once again exercised their "free, untrammeled franchise."[4]

Although just over 130 million Americans voted in the 2008 presidential election,[5] the last two presidential campaigns resemble Asimov's vision of predictive statistical analysis, harnessed to big data, playing a central role in determining electoral outcomes. Recent campaigns for major federal and state offices have become data-driven operations, with major parties, presidential campaign organizations, and a new breed of politically-oriented commercial data brokers (CDBs)[6] assembling extraordinarily detailed political dossiers on every American voter. Of course, there is nothing new about the collection and use of voter data in American political life.[7] But the twenty-first century version of political dossiers is vastly different from those of the past. Not only are modern political databases huge, with hundreds of millions of individual records, each of which has hundreds to thousands of data points, they also exploit powerful processors, ubiquitous network connections, cheap storage, and new abilities to mine data for meaningful voter patterns.[8] Moreover, political dossiers are strategically valuable in the sense that they permeate every aspect of modern campaigning, including efforts to mobilize supporters and donors, voter registration

2. *Id.*

3. *Id.* at 18, 21–22.

4. *Id.* at 24.

5. FED. ELECTION COMM'N, FEDERAL ELECTION 2008: ELECTION RESULTS FOR THE U.S. PRESIDENT, THE U.S. SENATE AND THE U.S. HOUSE OF REPRESENTATIVES 5 (July 2009), *available at* http://www.fec.gov/pubrec/fe2008/federalelections2008.pdf. Barack Obama defeated John McCain by a popular vote of 69,498,516 to 59,948,323. *See id.*

6. For a definition of commercial data brokers, see FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 3 (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter FTC DATA BROKERS REPORT] (defining data brokers as firms whose primary business is "collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it, for purposes such as marketing").

7. RASMUS KLEIS NIELSEN, GROUND WARS: PERSONALIZED COMMUNICATIONS IN POLITICAL CAMPAIGNS 159 (2012) (discussing Grover Cleveland's use of voter lists in 1892).

8. *See infra* Part I.A.4.

drives, campaign advertising, and get-out-the-vote efforts on Election Day.[9]

In short, modern campaigns rely on the analysis of large data sets in search of useful and unanticipated insights, an activity that is often summed up by the phrase "big data." An early and influential discussion characterizes big data in terms of the "three *v's*"—volume (the amount of data being created), variety (the range of data types and sources), and velocity (the speed at which data is generated and must be analyzed).[10] A more recent discussion identifies a fourth *v* as "the value derived from new insights and knowledge gained from applying advanced machine-learning and analytics to big data sets."[11]

When evaluated against the four *v's*, political dossiers certainly qualify as big data even if they are dwarfed in size by the gigantic datasets handled by Internet firms like Google or Facebook. Indeed, big data was one of the more prominent storylines before and after the 2012 election, capturing numerous headlines in newspapers, magazines, trade journals, and the blogosphere.[12] As a political data consultant recently stated:

---

9. *See infra* Part I.B.1.

10. *Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data*, GARTNER (June 27, 2011), http://www.gartner.com/newsroom/id/1731916.

11. Carolyn Nguyen et al., *A User-Centered Approach to the Data Dilemma: Context, Architecture, and Policy*, *in* DIGITAL ENLIGHTEN FORUM YEARBOOK 2013: THE VALUE OF PERSONAL DATA (Mireille Hildebrandt et al. eds., 2013).

12. *See, e.g.*, NATHAN ABSE, INTERNET ADVERTISING BUREAU (IAB): BIG DATA DELIVERS ON CAMPAIGN PROMISE: MICROTARGETED POLITICAL ADVERTISING IN ELECTION 2012, at 2 (2012) [hereinafter IAB REPORT]; RICHARD WOLFFE, THE MESSAGE: THE RESELLING OF PRESIDENT OBAMA 247 (2013); Lois Beckett, *Everything We Know (So Far) About Obama's Big Data Tactics*, PROPUBLICA (Nov. 29, 2012, 10:45 AM), http://www.propublica.org/article/everything-we-know-so-far-about-obamas-big-data-operation; Brett Bell, *Big Data Is a Big Factor in 2012*, CAMPAIGNS & ELECTIONS (Mar. 30, 2012), http://candeold.russellbrown.co.uk/email/magazine/canadian-edition/315777/big-data-is-a-big-factor-in-2012-by-brett-bell-.thtml; Micah Cohen, *From Campaign War Room to Big-Data Broom*, N.Y. TIMES (June 19, 2013, 10:56 PM), http://bits.blogs.nytimes.com/2013/06/19/from-campaign-war-room-to-big-data-broom/; Nicholas Confessore, *Groups Mobilize to Aid Democrats in '14 Data Arms Race*, N.Y. TIMES (Nov. 8, 2012), http://www.nytimes.com/2013/11/15/us/politics/groups-mobilize-to-aid-democrats.html?hp&_r=2&; Valentina Craft, *Winning the Elections with Big Data: Obama's Team of Newbies*, SILICON ANGLE, http://siliconangle.com/blog/2013/08/07/winning-the-elections-with-big-data-obamas-team-of-newbies-hpbigdata2013/ (last visited Oct. 8, 2014); Charles Duhigg, *Campaigns Mine Personal Lives to Get Out Vote*, N.Y. TIMES (Oct. 13, 2012), http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?ref=charlesduhigg&_r=0; Thomas B. Edsall, *Let the Nanotargeting Begin*, N.Y. TIMES (Apr. 15, 2012, 10:39 PM), http://campaignstops.blogs.nytimes.com/2012/04/15/let-the-nanotargeting-begin/; Sean Gallagher, *Built to Win: Deep Inside Obama's Campaign Tech*, ARS TECHNICA (Nov. 14, 2012, 10:15 AM), http://arstechnica.com/information-technology/2012/11/built-to-win-

> Political strategists buy consumer information from data brokers, mash it up with voter records and online behavior, then run the seemingly-mundane minutiae of modern life—most-visited websites [sic], which soda's in the fridge—through complicated algorithms and: pow! They know with 'amazing' accuracy not only if, but *why*, someone supports Barack Obama or Romney . . . .[13]

Although campaigns assemble political dossiers for targeting purposes, seeking to correlate the likelihood of individual voters casting a ballot and supporting a candidate with the observable patterns of every conceivable form of their offline and online behavior, the privacy implications of data-driven campaigning have received only limited

---

deep-inside-obamas-campaign-tech/; Sasha Issenberg, *How President Obama's Campaign Used Big Data to Rally Individual Voters*, MIT TECH. REV. (Dec. 16, 2012), http://www.technologyreview.com/featuredstory/508836/how-obama-used-big-data-to-rally-voters-part-1/ [hereinafter Issenberg, *Obama's Campaign*]; Sasha Issenberg, *Obama's White Whale*, SLATE (Feb. 15, 2012, 11:28 AM), http://www.slate.com/articles/news_and_politics/victory_lab/2012/02/project_narwhal_how_a_top_secret_obama_campaign_program_could_change_the_2012_race_.html [hereinafter Issenberg, *White Whale*]; Kate Kaye, *Big Data from Democratic Party Spawns Web Ad Targeting Firm*, CLICKZ (Mar. 30, 2012), http://www.clickz.com/clickz/news/2165034/democratic-party-spawns-web-targeting-firm; Steve Lohr, *The Obama Campaign's Technology Is a Force Multiplier*, N.Y. TIMES (Nov. 8, 2012, 7:25 PM), http://bits.blogs.nytimes.com/2012/11/08/the-obama-campaigns-technology-the-force-multiplier/?hpw; Alexis C. Madrigal, *When the Nerds Go Marching In*, ATLANTIC (Nov. 16, 2012, 7:00 AM), http://www.theatlantic.com/technology/archive/2012/11/when-the-nerds-go-marching-in/265325/; Robert L. Mitchell, *Campaign 2012: Mining for Voters*, COMPUTERWORLD (Oct. 29, 2012, 7:00 AM), http://www.computerworld.com/s/article/9232567/Campaign_2012_Mining_for_voters; Terrence McCoy, *The Creepiness Factor: How Obama and Romney Are Getting to Know You*, ATLANTIC (Apr. 10, 2012, 12:45 PM), http://www.theatlantic.com/politics/archive/2012/04/the-creepiness-factor-how-obama-and-romney-are-getting-to-know-you/255499/; Tim Murphy, *Inside the Obama Campaign's Hard Drive*, MOTHER JONES (Sept./Oct. 2012), http://www.motherjones.com/politics/2012/10/harper-reed-obama-campaign-microtargeting?page=2; David Parry, Op-Ed., *Big Data: What Happens When Elections Become Social Engineering Competitions*, TECHPRESIDENT (June 26, 2012), http://techpresident.com/news/22466/op-ed-big-data-what-happens-when-elections-become-social-engineering-competitions; Jim Rutenberg, *Data You Can Believe In: The Obama Campaign's Digital Masterminds Cash In*, N.Y. TIMES (June 20, 2013), http://www.nytimes.com/2013/06/23/magazine/the-obama-campaigns-digital-masterminds-cash-in.html?pagewanted=all&_r=2&; Michael Scherer, *Inside the Secret World of the Data Crunchers Who Helped Obama Win*, TIME (Nov. 7, 2012), http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-crunchers-who-helped-obama-win/#ixzz2jdOHLDBwin; Hayley Tsukayama, M*icrotargeting Has Growing Influence in Political Campaigns, Says Interactive Advertising Bureau*, WASH. POST (Feb. 26, 2013, 11:51 AM), http://www.washingtonpost.com/blogs/post-tech/post/microtargeting-has-growing-influence-in-political-campaigns-says-interactive-advertising-bureau/2013/02/26/32e0723e-8023-11e2-b99e-6baf4ebe42df_blog.html.

13. McCoy, *supra* note 12.

attention.[14] This Article seeks to remedy this oversight. Part I offers the first comprehensive analysis of the main sources of voter data and the absence of legal protections for these data and related data processing activities. Part II considers the privacy interests that individuals enjoy when they participate in elections, organizing the analysis under the rubrics of information privacy and political privacy. It asks two interrelated questions: first, does the relentless profiling and microtargeting of American voters invade their information privacy and, if so, what harm does it cause; and, second, do these activities undermine political privacy and, hence, the integrity of the electoral system? It also examines why political actors tend to minimize privacy concerns.

Next, Part III identifies a modest proposal for addressing the harms identified in Part II, consisting of (1) a mandatory disclosure and disclaimer regime requiring political actors to be more transparent about voter microtargeting and related campaign data practices and (2) new federal privacy restrictions on commercial data brokers and a complementary "Do Not Track" mechanism enabling individuals (who also happen to be voters) to decide whether and to what extent commercial firms may track or target their online activity. The Article concludes by asking whether even this modest proposal runs afoul of political speech rights guaranteed by the First Amendment. It makes two arguments. First, the Supreme Court is likely to uphold mandatory privacy disclosures and disclaimers by applying doctrines developed in the campaign finance cases to this new form of political transparency. Second, the Court will continue viewing commercial privacy regulations as constitutional under longstanding First Amendment doctrines, despite any incidental burdens they may impose on political actors, and notwithstanding its recent decision in *Sorrell v. IMS Health*,[15] which is readily distinguishable.

I. DATA-DRIVEN POLITICAL CAMPAIGNS

State election agencies collect and maintain voter data for obvious reasons. Accurate and up-to-date voter records make it possible to administer a democratic electoral system in which citizens who meet legal requirements have the right to cast a ballot in local, state, and

14. Earlier studies include Solon Barocas, *The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process*, *in* PROCEEDINGS OF THE 2012 ACM WORKSHOP ON POLITICS, ELECTIONS AND DATA 31, 34 (2012); Daniel Kreiss & Philip N. Howard, *New Challenges to Political Privacy: Lessons from the First U.S. Presidential Race in the Web 2.0 Era*, 4 INT'L J. COMM. 1032, 1039 (2010); Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data*, 64 STAN. L. REV. ONLINE 70, 71–72 (2012).

15. 131 S. Ct. 2653 (2011).

federal elections. Political actors require access to voter lists mainly to communicate with voters but also to ensure that all and only eligible voters cast a ballot.

Privacy law fundamentally concerns "personally identifiable information" (abbreviated as "PII" but also referred to as "personal data"), which means data that is or can be linked to a specific individual.[16] Although voter registration data clearly qualifies as PII, making it a fit subject for privacy regulation, most of this data also qualify as public records, implying that voter data must be open to inspection by the general public with limited exceptions.[17] The dual status of voter registration data as both public records and PII inevitably creates tension between transparency and privacy.

Earlier studies of voter privacy have mainly focused on a few discrete privacy issues regarding the appropriate limitations on the access, transfer, and use of voter registration records.[18] But voter data consists of far more than the basic information recorded in the voter rolls. As already stated, political actors assemble a vast array of PII into detailed dossiers on practically every American voter in order to target voters with individualized messages for purposes of both persuasion and mobilization (a process they refer to as "voter microtargeting") and for ongoing tactical, budgetary, and staffing decisions.[19] Most voters are ignorant of the steps taken to create these dossiers and know even less about related targeting practices. But they do object to targeted political ads, even though they have few if any controls over the personal data collected about them or its use in voter microtargeting.[20]

---

16. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 872–73 (4th ed. 2011). Most privacy laws distinguish PII (personal data) from non-PII (non-personal data). *Id.*

17. Many states protect vulnerable populations by redacting their information. *See infra* notes 30–31.

18. *See* U.S. PUB. POLICY COMM. OF THE ASS'N FOR COMPUTING MACHINERY (ACM), STATEWIDE DATABASES OF REGISTERED VOTERS: STUDY OF ACCURACY, PRIVACY, USABILITY, SECURITY, AND RELIABILITY ISSUES 30 (Feb. 2006), *available at* http://usacm.acm.org/images/documents/vrd_report2.pdf [hereinafter ACM REPORT]; NAT'L RESEARCH COUNCIL, IMPROVING STATE VOTER REGISTRATION DATABASES: FINAL REPORT 63–64 (2010), http://funderscommittee.org/files/ImprovingStateVoterRegistrationDatabases.pdf [hereinafter NRC REPORT]. *See generally* CAL. VOTER FOUND., VOTER PRIVACY IN THE DIGITAL AGE (June 9, 2004), *available at* http://www.calvoter.org/issues/votprivacy/pub/0504voterprivacy.pdf [hereinafter CVF REPORT].

19. DANIEL KREISS, TAKING OUR COUNTRY BACK: THE CRAFTING OF NETWORKED POLITICS FROM HOWARD DEAN TO BARACK OBAMA 23 (2012).

20. *See* Joseph Turow et al., *Americans Roundly Reject Tailored Political Advertising at a Time When Political Campaigns Are Embracing It*, ANNENBERG SCH. FOR COMM. (July 2012), http://www.asc.upenn.edu/news/Turow_Tailored_Political_Advertising.pdf. A recent survey found that "the vast majority of adult

This Part begins by analyzing four sources of voter data and then turns to the absence of applicable privacy regulation concerning its collection, use, and disclosure. The sources are state voter registration databases ("VRDs" or "voter rolls"), donor and "response" data, campaign web site data, and national voter files, whether maintained by the major parties or by private consulting firms. Next, this Part explores voter microtargeting: what it is, whether it is effective, and how much data it requires. These inquiries set the stage for identifying and analyzing in Part II a broad range of serious privacy violations and related harms associated with data-driven campaigning.

A. Voter Data and Regulatory Gaps

1. STATE VOTER REGISTRATION DATABASES

States gather a wide variety of data from voters on paper or online registration forms. According to a 2004 study, 48 of the 50 states (plus the District of Columbia)[21] require voters to submit name, address, and signature.[22] All but one of these jurisdictions also require date of birth, while a majority of them require phone number, gender, all or part of Social Security numbers (SSNs), and party affiliation.[23] Most states also keep track of voter history (when and how often someone votes but not for whom they vote).[24]

VRDs help confirm voter eligibility and facilitate election administration tasks.[25] They also play a central role in the U.S. political system by enabling candidates and others to communicate with voters for political purposes by mail, phone, email, and door-to-door canvassing.[26] Indeed, all 50 states permit the use of voter rolls for political purposes, while 22 of these jurisdictions allow unrestricted access to this data including for commercial purposes.[27] As a result, voter registration data is widely disseminated not only to parties, candidates, outside consultants, and advocacy groups for political purposes, but also to

---

Americans—86%—do not want political campaigns to tailor advertisements to their interests." *Id.*

21. CVF REPORT, *supra* note 18, at 13. Two states lack statewide registration systems: North Dakota (which has no registration requirement) and Wyoming (which conducts registration only at the county level). *Id.*

22. *Id.* at 3.

23. *Id.* Additionally, a handful of states seek optional information such as place of birth, driver's license number, and race. *Id.*

24. *Id.* at 35–36.

25. *See* NRC REPORT, *supra* note 18, at 63–64.

26. CVF REPORT, *supra* note 18, at 9–10.

27. *Id.* at 4.

commercial, academic, and news organizations.[28] In the past, political campaigns purchased voter registration data directly from their state or local election offices, but many campaigns currently acquire this data from their state or national party or buy it from a few giant political data vendors.[29]

Although VRDs collect and disseminate personal data for multiple purposes, most states engage in only token efforts to protect the privacy of voters. On the positive side, 29 of the 30 states that collect SSNs redact them from voter lists before distributing them for any secondary uses.[30] And, in a bare majority of states, officials who serve in sensitive public positions (such as police officers or judges) may remove their records from voter lists before they are distributed for secondary users, as may battered men or women.[31] But for the average voter concerned about the privacy (and security) of his or her registration data, more basic protections vary greatly and frequently are inadequate.

All modern privacy laws are premised on Fair Information Practices (FIPs), a set of basic principles setting forth rights and responsibilities in the collection and use of personal data.[32] The FIPs represent a common understanding of the principles that organizations should follow to provide individuals with appropriate controls over the collection, use, and disclosure of their personal data, safeguard this data against security threats, and establish accountability measures that give effect to these principles.[33] Unfortunately, most state voting laws fail to satisfy even these basic requirements. For example, they provide no notice or incomplete notice regarding the collection of SSNs, or required versus optional data fields, and offer few if any choices to citizens who may wish to redact certain information or limit secondary uses.[34] Even the relatively few states that have enacted general privacy laws regulating personal information held by state agencies offer only limited privacy protections for VRDs.[35]

There are several studies of the privacy issues associated with VRDs, and all of them recommend the adoption of the FIPs as a starting

---

28. *Id.* at 22–23, 25.

29. *See infra* Part I.A.4.

30. CVF REPORT, *supra* note 18, at 20.

31. *Id.* at 21.

32. SOLOVE & SCHWARTZ, *supra* note 16, at 699.

33. *See infra* notes 148–57 and accompanying text.

34. CVF REPORT, *supra* note 18, at 17–20.

35. *See* ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 31–34 (2013) (identifying 28 states with applicable laws on personal information maintained by a state agency). In states with strong privacy laws, the public interest in the disclosure of voter records generally outweighs privacy interests, which weakens privacy protections for such records.

point for enhancing voter privacy.[36] Specific recommendations include increased transparency, data minimization, more redaction of sensitive data, a prohibition on commercial use of voter data, and improved enforcement.[37] But even if the states embraced these reforms, an undeniable tension would remain between the privacy rights voters may desire and the data needs of election administrators, parties, candidates, and civil society.[38] This tension is exacerbated by the fact that most states treat voter registration data as public records, making them subject to open access laws, which generally mandate broad public access.[39]

Although one can readily imagine modest changes in state voter registration laws to address perceived privacy weaknesses, an outright prohibition on sharing voter lists for political purposes is out of the question. As noted above, a well-functioning democratic electoral system requires the use of voter rolls for a variety of legitimate purposes, and there are constitutional constraints on restricting the dissemination or use of voter lists in elections.[40] And yet it is a mistake to infer that privacy concerns are unimportant or impossible to accommodate.

2. DONOR AND "RESPONSE" DATA

The voter rolls contain data that allows parties and candidates to contact voters and form a preliminary idea of who they are and which candidates they might support in an upcoming election. During every election cycle, however, parties and candidates supplement this information with two rich and constantly renewed sources of political data: records of individual campaign contributions and information about individual voter attitudes gleaned from door-to-door canvassing, telephonic or e-mail surveys, and/or polls directed at select groups of the electorate (so-called "response" data).[41]

a. Donor Data

Federal campaign finance law requires candidates for federal office to report the names, addresses, and occupations of donors of $200 or

---

36. CVF REPORT, *supra* note 18, at 44–45; NRC REPORT, *supra* note 18, at 52–53; ACM REPORT, *supra* note 18, at 30.

37. CVF REPORT, *supra* note 18, at 44–45; NRC REPORT, *supra* note 18, at 52–53; ACM REPORT, *supra* note 18, at 30.

38. NRC REPORT, *supra* note 18, at 93.

39. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 127–39 (2004).

40. *See infra* Part III.B.

41. NIELSEN, *supra* note 7, at 142.

more.[42] Prior to the Internet, this data remained hidden thanks to "practical obscurity" (that is, the time and expense associated with visiting an election agency office in person and rummaging through paper files). The rise of the Internet has changed all this by making donor information readily available in electronic form.[43] The digital age makes it easy to learn about the political beliefs of friends, neighbors, and colleagues simply by using the donor lookup tools provided by the Federal Election Commission (FEC)[44] or various non-governmental organizations (NGOs).[45] Federal campaign finance law requires disclosure of donor data mainly to prevent corruption or the appearance of corruption but shows scant regard for the privacy implications of the compulsory disclosure of donor data.[46] Similarly, the Supreme Court recently held that signers of referendum petitions generally do not have a constitutional right to keep their identities private when state open government laws mandate disclosure.[47]

b. "Response" Data

Donor data reveals much about the political beliefs of individual contributors, but donors make up only a very small percentage of qualified voters.[48] To learn more about the attitudes of the overall voting population toward specific candidates and issues, political actors rely on canvassing and surveys. Volunteers go door-to-door or make phone calls to find out "whether individuals are registered to vote, what candidate they support and the degree to which they support them, and what issues matter to them."[49] This information is fed into campaign databases along

42. *See* Federal Election Campaign Act (FECA), Pub. L. No. 93-443, 88 Stat. 1263 (1974) (codified at 2 U.S.C. §§ 431–455 (2000)). The requirement to identify individuals by their name, address, occupation, and employer is found at 2 U.S.C. § 431(13)(A) (2012).

43. William McGeveran, *Mrs. McIntyre's Checkbook: Privacy Costs of Political Contribution Disclosure*, 6 U. PA. J. CONST. L. 1, 11–12 (2003).

44. *See* FED. ELECTION COMM'N, ELECTRONICALLY FILED INDEPENDENT EXPENDITURES, *available at* http://www.fec.gov/finance/disclosure/ie_reports.shtml (last visited Oct. 8, 2014).

45. *See Donor Lookup*, OPENSECRETS.ORG, http://www.opensecrets.org/indivs/ (last visited Oct. 8, 2014).

46. *See* McGeveran, *supra* note 43, at 8–24.

47. *See Doe v. Reed*, 561 U.S. 186, 202 (2010). I return to this topic in Part III.B, *infra*.

48. *See Donor Demographics*, OPENSECRETS.ORG, https://www.opensecrets.org/overview/donordemographics.php (last visited Oct. 8, 2014).

49. KREISS, *supra* note 19, at 104.

with supplementary field data gathered from large-scale surveys of voter attitudes.[50]

3. CAMPAIGN WEB SITES

In the last two presidential elections, campaign web sites have emerged as "the central hub of digital political messaging."[51] The Obama campaign's web site, as compared to the Romney campaign's, is as an obvious choice for a case study for two reasons: its success in using information and technology to outpace a better funded opponent[52] and, owing to this success, the greater availability of information about its web practices (including a very detailed privacy policy).[53]

The first thing to notice about the Obama campaign web site is that it functions like any commercial web site: visitors who navigate there may engage in various activities such as viewing published content and videos, e-mailing the candidate, signing a petition, completing a survey, donating money, or registering to receive a newsletter or e-mail alerts on breaking news.[54] Every such interaction is an opportunity for the campaign to collect and/or analyze personal data about voters.[55] Web-based voter data include required, volunteered, observed, and inferred data.[56]

---

50. *See* JONATHAN ALTER, THE CENTER HOLDS: OBAMA AND HIS ENEMIES 103–04 (2013) (noting that the Obama campaign placed 4,000 to 9,000 "ID calls" every night to voters in battleground states and that these calls allowed the campaign to build and update its voter models); *see also* SASHA ISSENBERG, THE VICTORY LAB: THE SECRET SCIENCE OF WINNING CAMPAIGNS 259 (2012).

51. Pew Research Ctr., *How the Presidential Candidates Use the Web and Social Media: Obama Leads but Neither Candidate Engages in Much Dialogue with Voters*, Pew Research Journalism Project (Aug. 15, 2012), http://www.journalism.org/2012/08/15/how-presidential-candidates-use-web-and-social-media/.

52. Jim Rutenberg, *Secret of the Obama Victory? Rerun Watchers, for One Thing*, N.Y. TIMES (Nov. 12, 2012), http://www.nytimes.com/2012/11/13/us/politics/obama-data-system-targeted-tv-viewers-for-support.html?ref=politics&_r=0 (describing this as "[o]ne of the biggest emerging stories" of the 2012 election).

53. *See infra* notes 100–05 and accompanying text.

54. OBAMA FOR AM., http://web.archive.org/web/20120824111653/http://www.barackobama.com/ (last visited Oct. 8, 2014) (retrieved from Internet Archive).

55. *See* GREG CONTI, GOOGLING SECURITY: HOW MUCH DOES GOOGLE KNOW ABOUT YOU? 16–18 (2009).

56. *See* WORLD ECONOMIC FORUM, RETHINKING PERSONAL DATA: STRENGTHENING TRUST 18 (May 2012), http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf ("Personal data can be volunteered, observed or inferred."). "Required" data is a fourth category added by the author.

a. Required Data

This includes the information any visitor must supply to create a registered user account (first and last name, zip code, e-mail, address and password) and thereby gain access to a host of web tools for online political engagement. These include tools for identifying local events and groups, contacting undecided voters who reside nearby, posting messages on the campaign blog, or volunteering for canvassing or registration drives.[57] Web site registration enhances existing voter files in two important ways. First, it allows the campaign to link voters in the physical world with their email address, thereby creating a very cheap and efficient channel of mass communication to known supporters; and, second, every user's ID and password becomes the basis for a unique identifier, which not only allows the web site to authenticate a user as the same person who previously signed in with a given identity, but also assists the campaign in developing and building profiles of the individual voters who use the site's services.[58]

b. Volunteered Data

This category is both descriptive and normative. On the one hand, it covers any information that supporters freely give to the campaign as they interact with fellow supporters or the wider public on campaign blogs, forums, or other interactive services, whether hosted on the Obama web site or by popular commercial services like Facebook, Google+, Twitter, or YouTube, where the campaign has dedicated Obama "pages" or "channels."[59] On the other hand, it encompasses any publicly available information, regardless of whether individuals deliberately shared it with the campaign. For example, the campaign might collect such data by hiring a consultant with expertise in "web scraping" (automated web data monitoring and extraction).[60] Not all publicly available data is voluntarily provided, however. Nor should campaigns assume that publicly available data is free of all privacy concerns.

---

57. The 2008 Obama campaign introduced a host of new social networking tools when it launched the "My.barackobama.com" web site. *See* Heather Havenstein, *Obama Still Dominates Web 2.0 World*, COMPUTERWORLD (Oct. 22, 2008, 1:00 AM), http://www.computerworld.com/article/2533697/web-apps/obama-still-dominates-in-web-2-0-world--internet-searches.html.

58. CONTI, *supra* note 55, at 78–81.

59. Pew Research Ctr., *supra* note 51.

60. *See generally* Joseph Bonneau et al., *Prying Data out of a Social Network*, *in* PROCEEDINGS OF THE 2009 INTERNATIONAL CONFERENCE ON ADVANCES IN SOCIAL NETWORK ANALYSIS AND MINING (2009), *available at* http://www.jbonneau.com/doc/BAS09-ASONAM-prying_sns_data.pdf.

c. Observed Data

This is a very broad category that includes (1) the data generated whenever a user's browser accesses the campaign web page such as the user's Internet protocol (IP) address (which may be analyzed to determine his or her physical location), the IP address of a referring web site (which may be analyzed to link the visitor's IP address with the search query, news article, or blog entries the visitor generated or looked at before navigating to the campaign web site), and (if the voter accesses the site from a mobile device), additional information such as the device's unique ID and geo-location information; (2) user's activities on the web site (including browsing patterns, which convey information about their goals and interests and may uniquely identify them); and (3) data associated with first- and third-party cookies and other tracking technologies used to help manage and deliver targeted ads.[61] The Obama web site privacy policy acknowledges the use of third-party network advertising cookies that "may automatically collect information about your visits to this and other web sites, your IP address, [and] your ISP" in order "to deliver advertising on other web sites targeted to your interests and to better understand the usage and visitation of our Sites and the other sites tracked by these third parties."[62]

d. Inferred Data

This term refers to "the output of data analysis, combination or mining, and it includes credit scores, predictions of preferences and purchase intent."[63] For present purposes, it covers any information computationally derived from required, volunteered, and/or observed data. At a minimum, the Obama campaign relied on inferred data in developing voter profiles (which enabled the campaign to deliver personalized web content,[64] targeted ads,[65] and personalized e-mail

61. *See* CONTI, *supra* note 55, at 65–72. First-party cookies are set (i.e., placed on the user's computer) by the web site the user is visiting and have various uses ranging from enabling web sites to recognize returning visitors or save their preferences to tracking their behavior for purposes of serving targeted web content or personalized ads. *See generally id.* at 72–76. Third-party cookies are set by a different entity with whom the user has no direct relationship, such as a network advertising service that invisibly tracks users across different web sites, often without the target's awareness or consent, making them far more worrisome from a privacy standpoint. *See generally id.*

62. *Privacy Policy*, OBAMA FOR AM. (Feb. 3, 2012), http://web.archive.org/web/20120920105413/http://www.barackobama.com/privacy-policy?source=footer-nav [hereinafter *Obama Privacy Policy*] (retrieved from Internet Archive).

63. *See* WORLD ECONOMIC FORUM, *supra* note 56, at 18.

64. The 2012 Obama Privacy Policy states that it uses "personal information collected through our Sites . . . to monitor and analyze site usage and trends, and to personalize and improve the Sites and our users' experiences on the Sites and with the

messages) and voter scores (which allowed the campaign to predict candidate support and voter turnout as part of its voter microtargeting operations).[66] It is less clear whether the campaign combined campaign web site data with voter files to develop these profiles or derive these scores.

Statistics on web site usage during the last two presidential elections indicate the size and scale of the Obama campaign's web operations. For example, in 2008, barackobama.com saw an unprecedented level of online activity, with reports indicating that 3 million donors made a total of 6.5 million online donations (adding up to more than $500 million); 13 million voters shared their e-mail addresses and the campaign sent more than more than 1 billion e-mails with about 7,000 different messages; 1 million people signed up for Obama's text-messaging program; and 2 million people created profiles on Obama's own social network (MyBO), which supporters used to plan 200,000 offline events, share about 400,000 blog posts, and create more than 35,000 volunteer groups.[67] In October 2012, the Obama web site attracted 8.6 million visitors (over three times more than the Romney web site) and collected observed and inferred data from every visitor as well as required and volunteered data from a large subset of them.[68]

4. STATE AND NATIONAL VOTER FILES

State VRDs, donor and response databases, and campaign web sites all raise a number of familiar privacy concerns. But they are only the starting point of modern efforts to collect, capture, purchase, match, combine, store, manage, analyze, and share voter data. All of this data only becomes truly useful for political campaigns as a result of three transformations. First, the foundational data in VRDs is *cleansed* (by matching it with a database of valid, up-to-date addresses and phone numbers); second, clean data is *supplemented* (by appending donor and response data, census data, polling results, and all sorts of consumer data

---

campaign, such as providing content, or features that match your profiles or interests." *Obama Privacy Policy*, *supra* note 62.

65. The Obama Privacy Policy also states that it uses such data "to serve ads, on this Site or other web sites or media, based on the information you provide and the actions you take." *Id.*

66. *See infra* Part I.B.

67. *See* Jose Antonio Vargas, *Obama Raised Half a Billion Online*, WASH. POST (Nov. 20, 2008, 8:00 PM), http://voices.washingtonpost.com/44/2008/11/obama-raised-half-a-billion-on.html.

68. *See* Larry Kim, *Who Will Win the Election Tomorrow? Obama by a Landslide*!*, WORDSTREAM (Nov. 5, 2012), http://www.wordstream.com/blog/ws/2012/11/05/who-will-win-the-election-tomorrow-obama-landslide.

acquired from CDBs); and, third, all of this data is *integrated* (combined with campaign web data and stored in databases in a convenient format for subsequent data processing and analysis).[69]

In years past, state parties took the lead in performing these tasks, but by the mid-nineties, the Republican National Committee (RNC) began working to create an integrated national voter file.[70] Launched in 2002 and called "Voter Vault,"[71] by 2004 it had data on "every one of the 168 million or so registered voters in the country, cross-indexed with phone numbers, addresses, voting history, income range and so on—up to as many as several hundred points of data on each voter."[72] By the 2004 election cycle, the Democrats had created their own national voter file called "DataMart."[73] In creating national voter files, both parties shared the common goal of using technology to improve the efficiency and effectiveness of their fund-raising and campaign operations. They invested millions of dollars in "state-of-the-art data warehouses, data mining software and Web-based user interfaces"[74] in the hopes of better identifying likely supporters and targeting them with more personalized messages. This technique is known as "voter microtargeting" and is discussed in detail below.[75]

Beginning with the 2004 election cycle, the major parties and candidates for high office also began relying on a new breed of political consulting firms for everything from their massive voter data files, to new digital tools and infrastructure, to their microtargeting and related online advertising services.[76] Many such firms work exclusively for one party or the other, although the oldest of them, called Aristotle, provides a comprehensive range of servicers on a non-partisan basis.[77] Political data firms compete on the size of their national voter files,[78] the

69. KREISS, *supra* note 19, at 108–09; NIELSEN, *supra* note 7, at 161.

70. Kreiss & Howard, *supra* note 14.

71. *Id.*

72. Jon Gertner, *The Very, Very Personal Is the Political*, N.Y. TIMES (Feb. 15, 2004), http://www.nytimes.com/2004/02/15/magazine/15VOTERS.html.

73. Elana Varon, *Election 2004: IT on the Campaign Trail*, CIO MAG. (June 1, 2004, 8:00 AM), http://www.cio.com/article/32314/Election_2004_IT_on_the_Campaign_Trail.

74. *Id.*; *see* ISSENBERG, *supra* note 50, at 131–36, 170–80; KREISS, *supra* note 19, at 107–13; NIELSEN, *supra* note 7, at 166–68.

75. *See infra* Part II.B.

76. *See* NIELSEN, *supra* note 7, at 141 (noting that voting microtargeting was "pursued on a large scale by the Bush campaign" in 2004 and that this work is "generally done by specialized outside consultants").

77. *See* ARISTOTLE, http://aristotle.com (last visited Oct. 8, 2014).

78. *See Products*, CATALIST, http://www.catalist.us/products (last visited Oct. 8, 2014) (offering a database with "more than 190 million voter records").

availability of specialized databases,[79] the number of data points available for voter profiling purposes,[80] and their dedication and loyalty to the digital needs of conservatives[81] versus progressives.[82]

In the 2012 election cycle, an emerging trend for these firms was the formation of new partnerships with online advertising firms that specialized in tracking people on the web. Their goal was to reach voters online at any web site they might visit with even more targeted political messages based on matching existing voter files with online, cookie-based profiles.[83] Consider the three-way partnership between Aristotle (a political data broker), Intermarkets (a digital ad firm), and Lotame (a data management and analytics firm).[84] Intermarkets took the lead role in matching its "cookie pool" (i.e., a database of active and targetable cookies) with Aristotle's political data in order to identify individuals with particular characteristics and send them targeted ads wherever they might show up on the web:

> The robust national voter data provided by Aristotle gives Intermarkets the ability to target digital ads . . . based on party affiliation and degree of voter activity in addition to information Aristotle appends to voter filer data such as demographic info on gender and household income levels, and psychographic information. Lotame is . . . building out larger

79. *See Premium Enhancements*, ARISTOTLE, http://aristotle.com/political-data/premium-enhancements/ (last visited Oct. 8, 2014) (offering a voter list with "over 5.4 million voters who hold hunting and fishing licenses, as well as individuals who subscribe to a wide array of magazine subscriptions including family, religious, financial, health, culinary and do-it-yourself publications").

80. *Under the Hood*, CAMPAIGNGRID, http://campaigngrid.com/under-the-hood/ (last visited Oct. 8, 2014) (offering "[a]dvanced segmentation along tens of thousands of data points to message to the right individuals at the right time with the right message").

81. *See, e.g.*, CAMPAIGNGRID, http://www.campaigngrid.com/news/online-political-advertising-gets-personal/ (last visited Oct. 14, 2014) (characterizing Campaign Grid as "a Republican advertising platform"); TARGETED VICTORY, http://www.targetedvictory.com/our-services (last visited Oct. 8, 2014); TARGETPOINT, http://www.targetpointconsulting.com (last visited Oct. 8, 2014). *See generally* Susan Lahey, *In The News: VoterTrove Helps Conservative Campaigns Move into the Age of Big Data*, VOTERTROVE (Feb. 12, 2014), http://votertrove.com/2014/02/12/in-the-news-voter-trove-helps-conservative-campaigns-move-into-the-age-of-big-data/.

82. *See, e.g.*, *Our Work*, BLUE ST. DIGITAL, http://www.bluestatedigital.com/our-work (last visited Oct. 8, 2014); *Products*, *supra* note 78.

83. *See* Kate Kaye, *Intermarkets Pairs with Lotame to Enhance Aristotle Data Relationship*, CLICKZ (July 23, 2012), http://www.clickz.com/clickz/news/2193317/intermarkets-pairs-with-lotame-to-enhance-aristotle-data-relationship.

84. *Id.*

> audiences to target by finding people who fulfill similar criteria to the original audience pool.[85]

A second emerging trend in 2012 was the decision by Obama's re-election team to bring in-house much of its data management and analytic operations. After campaign staff conducted a post-election assessment of their data needs, they realized that their voter files, consumer profiles, web logs, donor data, and field reports were kept in separate silos and were not well integrated.[86] As a result, the campaign did not know if a given donor was the same person who attended a rally or volunteered for door-to-door canvassing, what her demographic profile looked like, or what issues mattered to her.[87] They set out to fix this by creating a more integrated data infrastructure while at the same time developing in-house targeting and analytic capabilities.[88] To accomplish these ambitious goals, the Obama team recruited and hired over 50 statisticians, mathematicians, quantitative scientists, software developers, and data analysts from leading Internet firms such as Twitter, Google, Facebook, Microsoft, and Craigslist.[89] This group designed and built a new database infrastructure code named "Project Narwhal," which solved the silo problem by integrating databases and building programming interfaces to allow controlled access and data pulls,[90] with the strategic goal of fusing "the multiple identities of the engaged citizen—the online activist, the offline voter, the donor, the volunteer—into a single, unified political profile."[91] And, in much the same manner as a Silicon Valley start-up, this group also created a host of innovative campaign applications and tools.[92]

---

85. *Id.* Similarly, Catalist partnered with Collective to form DSPolitical, a new ad-targeting firm serving Democrats and progressive groups. *See* Kaye, *supra* note 12. i360, another political data broker, partnered with comScore, a digital marketing firm. *See comScore and i360 Team Up to Provide Digital Marketing Insights for Political Campaigns and Advocacy Groups*, I360 (Apr. 17, 2012), http://www.i-360.com/comscore-and-i360-team-up-to-provide-digital-marketing-insights-for-political-campaigns-and-advocacy-groups. For a general description of audience segmentation and how it works, see JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH 73–87 (2011).

86. *See* Issenberg, *White Whale*, *supra* note 12.

87. ISSENBERG, *supra* note 50, at 260–61.

88. *Id.* at 262–63.

89. *See, e.g.*, Gallagher, *supra* note 12; Madrigal, *supra* note 12.

90. Gallagher, *supra* note 12.

91. Issenberg, *White Whale*, *supra* note 12; *see also* Gallagher, *supra* note 12.

92. Gallagher, *supra* note 12.

5. ABSENCE OF LEGAL PROTECTIONS

Political databases hold records on almost 200 million eligible American voters.[93] Each record contains hundreds if not thousands of fields derived from voter rolls, donor and response data, campaign web data, and consumer and other data obtained from data brokers, all of which is combined into a giant assemblage made possible by fast computers, speedy network connections, cheap data storage, and ample financial and technical resources. Ubiquitous personal identifiers (name and address, telephone numbers, e-mail addresses, IP address, cookies, mobile device IDs, and other unique IDs) allow campaigns to link and integrate these diverse datasets, while data mining and sophisticated statistical techniques allow them to engage in highly strategic and cost-effective analysis and targeting.[94] Although the preceding Sections focus almost exclusively on the Obama campaign, the Romney campaign, the Democratic Party, the Republican Party, and a handful of "political data brokers" (PDBs),[95] each mount data operations of similar size, speed, and analytic sophistication. Given the volume, velocity, variety, and value of voter data, there is little doubt that American presidential campaigns have entered the world of big data.

And yet these huge data hybrids fall into a regulatory gap. State election laws, for example, favor the public disclosure of voter rolls for political and—in 22 states—commercial purposes, except for a few narrowly drafted provisions allowing for the redaction of SSNs and certain additional data for vulnerable citizens.[96] Otherwise, state VRDs do not go very far in adhering to the FIPs. Donor data is heavily regulated except for privacy purposes.[97] Response data is largely unregulated—the data falls beyond the scope of state mini-Privacy Acts, which only apply to data collected and maintained by state agencies.[98]

---

93. *See, e.g.*, *About Us*, CATALIST, http://www.catalist.us/about (last visited Oct. 8, 2014); *Voter Files*, ARISTOTLE, http://aristotle.com/campaigns/voter-data/ (last visited Oct. 8, 2014) ("Our national voter file contains over 190 million voter records . . . .").

94. *See* ISSENBERG, *supra* note 50, at 131–36, 170–80; KREISS, *supra* note 19, at 107–13; NIELSEN, *supra* note 7, at 166–68; Varon, *supra* note 73.

95. PDBs are simply CDBs that combine consumer records with voter lists, donor records, and online data collected directly from voters and resell this assemblage to political parties and campaigns. Meg Schwenzfeier, *Consumer Data Used by Political Campaigns*, PULITZER CENTER (Feb. 21, 2014), http://pulitzercenter.org/reporting/north-america-united-states-political-campaigns-consumer-data-privacy.

96. *See supra* Part I.A.1.

97. *See supra* note 46 and accompanying text.

98. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 605 (1995)

Response data also falls outside the scope of federal and state consumer privacy laws, which only apply to data collected by commercial entities.[99]

Campaign web data is also largely unregulated. To begin with, the FEC has no relevant rules on web site privacy practices, and many consider this agency dysfunctional in any case.[100] Although state election laws regulate false and deceptive campaign statements,[101] they are mostly silent on unfair or deceptive online campaign practices. And the consumer protection agencies that ordinarily handle online privacy issues operate under jurisdictional grants limited to "commercial" data and therefore have refrained from investigating the privacy practices of campaign web sites.[102] In the absence of government regulation, a limited form of self-regulation governs these web sites. Indeed, in recent election cycles, the major parties and leading candidates voluntarily posted privacy policies; however, the discretionary terms and conditions of the Romney and Obama policies diverge in interesting ways. For example, in 2012, the Romney web site's privacy policy was quite short and so vague as to be almost meaningless.[103] Obama's 2012 privacy policy went to the opposite extreme: at 2,574 words, it was as lengthy, complex, and mystifying as any major commercial privacy policy and relied on very similar language.[104] It is striking that the 2012 Obama Privacy Policy had many of the same provisions and characteristics that the White House and the Federal Trade Commission (FTC) have taken issue with in two recent reports on privacy reform.[105]

(explaining that most states lack "omnibus data protection laws" and have "scattered laws [that] provide only limited protections for personal information in the public sector").

99. The basic consumer protection statute enforced by the Federal Trade Commission (FTC) is § 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." 15 U.S.C. § 45(a)(1) (2012). State consumer protection laws, sometimes referred to as "mini-FTC Acts," also apply solely to commercial activity.

100. *See, e.g.*, David A. Graham, *This Is Why We Can't Have Nice Elections: The Dysfunctional FEC*, ATLANTIC (July 12, 2013, 8:45 AM), http://www.theatlantic.com/politics/archive/2013/07/this-is-why-we-cant-have-nice-elections-the-dysfunctional-fec/277639/.

101. *See generally* Richard L. Hasen, *A Constitutional Right to Lie in Campaigns and Elections?*, 74 MONT. L. REV. 53 (2013); William P. Marshall, *False Campaign Speech and the First Amendment*, 153 U. PA. L. REV. 285, 285, 288 (2004).

102. *See supra* note 99.

103. *See Privacy Policy*, MITT ROMNEY FOR PRESIDENT, http://web.archive.org/web/20120601000000*/http://MittRomney.com (last visited Oct. 8, 2014) [hereinafter *Romney Privacy Policy*] (retrieved from Internet Archive).

104. *See Obama Privacy Policy*, *supra* note 62.

105. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC REPORT]; THE

Finally, the jury is still out on the application of more comprehensive privacy laws to national voter files or the overall data operations of various political actors. There is evidence that campaigns take seriously a few selected privacy requirements such as the nondisclosure provisions in the Cable Act.[106] But other laws are largely irrelevant to political activity, either because they protect privacy only in specific sectors of the economy, using narrow definitions of personal data or covered entities,[107] or because they explicitly exempt political speech on First Amendment grounds.[108] State security breach laws apply to voter data only if the political actors in question meet the various definitions of covered entities.[109] If the U.S. were to enact an omnibus privacy law as recommended by the Obama Administration and the FTC, this might fill some of the regulatory gaps described above. In the absence of such laws, voter data may be the largest concentration of unregulated personal information in the U.S. today.

B. Voter Microtargeting

Historically, candidates in American political campaigns have always targeted specific messages to individual voters.[110] As a tactic, voter microtargeting is analogous to a ward captain walking the precinct and using his local knowledge to appeal to individual residents. And yet the application of sophisticated data-mining techniques to massive voter

---

WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 9–22 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter WHITE HOUSE REPORT].

106. Cable Communications Policy Act (Cable Act), 47 U.S.C. § 551(c)(1) (2012).

107. For a list of such statutes, see SOLOVE & SCHWARTZ, *supra* note 16, at 37–39.

108. *See, e.g.*, Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (imposing restrictions on "commercial electronic mail messages"); Telephone Consumer Protections Act (TCPA) of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991) (imposing restrictions on telephone solicitations and unsolicited ads of a commercial nature).

109. Under state breach notification laws, there is no single definition of "covered entity," although most definitions cover some combination of individuals, businesses, state agencies, or any person. For a chart comparing state breach notification laws in 46 states, see *State Data Security Breach Notification Laws*, MINTZ LEVIN (Aug. 1, 2014), http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

110. *See* D. SUNSHINE HILLYGUS & TODD G. SHIELDS, THE PERSUADABLE VOTER: WEDGE ISSUES IN PRESIDENTIAL CAMPAIGNS 155 (2008); KATE KENSKI ET AL., THE OBAMA VICTORY: HOW MEDIA, MONEY, AND MESSAGE SHAPED THE 2008 ELECTION 304–06 (2010).

data sets beginning with the 2000 election marks a new development, because contemporary microtargeting is "more precise, efficient, and individualized" than anything preceding it.[111] The following discussion highlights the privacy aspects of contemporary voter microtargeting.

1. WHAT IS VOTER MICROTARGETING?

Voter microtargeting is a relatively new form of political direct marketing in which political actors target personalized messages to individual voters by applying predictive modeling techniques to massive troves of voter data.[112] The goal of voter microtargeting is to activate the base, persuade undecided voters, and improve partisan turnout. It therefore represents a partial retreat from huge media buys for undifferentiated mass audiences ("broadcasting") in favor of tailoring messages to the "needs, wants, expectations, beliefs, preferences, and interests" of a target audience as determined by data analysis ("narrowcasting").[113]

How does predictive modeling work? First, an analytic team (with expertise in statistics) assembles a test group based on information contained in voter files (which include voter history and often party registration), appended consumer data (which provides insight into socioeconomic status such as age, gender, income, and race), and—most importantly—up-to-date response data (which reveals people's "partisan leanings, candidate sympathies, and issues of interest").[114] Second, the statistical experts apply sophisticated algorithms to the assembled data to discover hidden correlations or patterns linking personal characteristics with political beliefs.[115] For instance, in the 2004 presidential race, Democrats sought to identify "the libertarian white male in Cobb County, Georgia, who would swing their way if approached appropriately," while Republicans sought "the socially conservative African American on the South Side of Chicago who might vote for a Republican."[116] Once they determine these and other patterns, the experts

111. *See* HILLYGUS & SHIELDS, *supra* note 110; *see also* Mitchell, *supra* note 12.

112. Tim Taylor, *All Things to All People*, 13 GEO. PUB. POL'Y REV. 25, 28–29 (2007–08).

113. W. Lance Bennett & Jarol B. Manheim, *The One-Step Flow of Communication*, 608 ANNALS AM. ACAD. POL. & SOC. SCI. 213, 215–16 (2006); *see also* Michael S. Kang, *From Broadcasting to Narrowcasting: The Emerging Challenge for Campaign Finance Law*, 73 GEO. WASH. L. REV. 1070, 1090–92 (2005) (analyzing the implications of narrowcasting on political campaigns).

114. NIELSEN, *supra* note 7, at 142, 146; *see also* ALTER, *supra* note 50, at 104; Gertner, *supra* note 72.

115. Taylor, *supra* note 112, at 29.

116. Kang, *supra* note 113, at 1079; *see* NIELSEN, *supra* note 7, at 142.

build a model for predicting how other voters (outside the test group) are likely to behave when faced with a choice of specific candidates or ballot measures.[117] The third and final step is applying this model to the larger voting population and generating at least two scores for every voter: a "support score" ranking every registered voter in the U.S. on a scale 0 to 100 based on their likelihood of voting for one's candidate; and, a turnout score measuring the likelihood of voters going to the polls on election day.[118]

2. IS VOTER MICROTARGETING EFFECTIVE IN WINNING ELECTIONS?

Voter microtargeting now guides and informs every aspect of modern elections. Political actors have embraced voter microtargeting for three main reasons. First, it enables campaigns to allocate their field resources very efficiently.[119] Second, it creates "innovative ways of discovering and turning out new voters."[120] Third, it supports new ways of delivering individualized messages using both old media (traditional narrowcasting methods like direct mail, door-to-door canvassing, and phone calls) and new media (targeted e-mail, personalized phone calls,[121] and "targeted sharing"[122] via social networking services like Facebook).

Thus, voter microtargeting depends on very reliable predictions about voters' preferences, intentions, and beliefs. Political scientists who have examined various claims about the benefits of voter microtargeting have raised doubts about whether it actually works. To begin with, most of the relevant data is inaccessible or inadequate, making data-driven campaigning very difficult to study.[123] One analysis suggests that the effects of targeted messages are difficult to understand from observational studies due to selection bias and endogeneity.[124] Moreover, researchers have discovered countervailing trends. According to Hersh and Schaffner, voters rarely prefer "targeted pandering" to general

---

117. This model can be validated and refined by making predictions about a subgroup of voters (whose views are already known but were not relied on to create the model) and seeing how well the model performs in predicting their behavior. NIELSEN, *supra* note 7.

118. *See* KREISS, *supra* note 19, at 179.

119. *See* ISSENBERG, *supra* note 50, at 12; Gertner, *supra* note 72.

120. *See* Gertner, *supra* note 72.

121. *See infra* notes 185–89 and accompanying text.

122. *See infra* note 229.

123. David Karpf, *The Internet and American Political Campaigns*, 11 FORUM: J. OF APPLIED RES. CONTEMP. POLS. 413, 421 (2013).

124. *See* Kevin Arceneaux, *The Benefits of Experimental Methods for the Study of Campaign Effects*, 27 POL. COMM. 199, 202–04 (2010).

messages, and voters who are mistargeted may penalize candidates enough to erase the positive returns to targeting.[125]

Despite academic skepticism regarding the efficacy of voter microtargeting, political operatives believe in it whole hog. This seems largely the result of anecdotal evidence from campaign insiders and paid consultants who not only view voter microtargeting as highly effective[126] but also have assigned it a crucial role in determining the outcome of the past three presidential campaigns.[127]

In short, party leaders now believe that microtargeting not only works but that it also wins (or loses) elections. Indeed, Romney's recent defeat has persuaded Republicans to do whatever it takes to catch up to the Democrats.[128] On the other hand, non-partisan analysts worry that lack of access to voter databases may emerge as a barrier to entry for political newcomers or challengers, including Tea Party candidates.[129] For present purposes, the evidence concerning the successes or failures of voter microtargeting matters less than the shared belief among party leaders that future electoral victories hinge on which party and candidates are smartest about amassing and analyzing voter data. This

125. Eitan D. Hersh & Brian F. Schaffner, *Targeted Campaign Appeals and the Value of Ambiguity*, 75 J. POL. 520, 532 (2013).

126. *See* WOLFFE, *supra* note 12, at 4 (noting that in Ohio, results in the 2012 presidential election "were within one percentage point of the model"); Chris Cillizza, *Romney's Data Cruncher*, WASH. POST, July 5, 2007, at A1 (Republicans believed that voter models used in Pennsylvania judicial races achieved a 90 percent accuracy rate); Gretchen Gavett, *Electing a President in a Microtargeted World*, HBR BLOG NETWORK (Nov. 2, 2012, 11:00 AM), http://blogs.hbr.org/2012/11/electing-a-president-in-a-micr/ (As one Democratic microtargeting expert stated, "good targeting can provide a few percentage points improvement for a campaign.").

127. *See, e.g.*, James Verini, *Big Brother Inc.*, VANITY FAIR (Dec. 13, 2007), http://www.vanityfair.com/politics/features/2007/12/aristotle200712?printable=true&currentPage=all (As direct-marketing pioneer Richard Viguerie put it, "[i]n the 2004 presidential race, Karl Rove and his team applied this strategy masterfully in battleground states such as Ohio, where they sent shock troops into Democratic pockets of blue-collar workers and minorities with personalized appeals to the churchgoing, the gun-owning, the abortion-hating. The result was a lead of 130,000 votes that tipped the election to Bush."); *see also* Marc Ambinder, *How Democrats Won the Data War in 2008*, ATLANTIC (Oct. 5, 2009), http://www.theatlantic.com/politics/archive/2009/10/exclusive-how-democrats-won-the-data-war-in-2008/27647/ (citing evidence that Catalist's data-mining and targeting efforts measurably helped elect Barack Obama); Thomas B. Edsall, *The G.O.P.'s Digital Makeover*, N.Y. TIMES (Apr. 3, 2013, 10:55 PM), http://opinionator.blogs.nytimes.com/2013/04/03/the-g-o-ps-digital-makeover (noting that many post-election accounts of the 2012 race credited Obama's victory to his campaign team's greater aptitude in voter modeling).

128. *See* Edsall, *supra* note 127; Kenneth P. Vogel & Maggie Haberman, *Karl Rove, Koch Brothers Lead Charge to Control Republican Data*, POLITICO (Apr. 22, 2013, 5:04 AM), http://www.politico.com/story/2013/04/karl-rove-koch-brothers-control-republican-data-90385.html.

129. *See* Parry, *supra* note 12.

belief in the efficacy of data-driven campaigning makes it inevitable that political actors will seek even more voter data.

3. HOW MUCH DATA IS NECESSARY FOR MICROTARGETING?

It is universally acknowledged in privacy circles that large databases raise heightened privacy concerns, especially if the database is very diverse, and even more so if it processes sensitive information (i.e., data revealing racial or ethnic origin, political opinions, religious beliefs, or medical conditions). As we have seen, political databases hit the jackpot on all three grounds by storing records on almost 200 million voters, covering hundreds if not thousands of data types, including many types of sensitive data.[130] Is all this data necessary? Does more information produce better results?

Numerous accounts of the past two Obama races suggest that political actors seek to acquire and analyze as much data as possible, thereby obeying what legal scholar Julie Cohen calls "the information-processing imperative."[131] With respect to the 183 million voter-file records that the party then held in its political database, the political director of the RNC, Rich Beeson, spoke for many politicos when he said: "We have pinned every bit of information we can ever find to [these records]."[132]

Academics, on the other hand, remain skeptical about whether more voter data ensures better results. For example, in an important study by political scientist Eitan Hersh, he develops and tests a model of campaign targeting strategy using the Catalist database of all registered voters in the U.S.[133] He argues that politicians have limited capacity to infer voters' political attitudes and therefore campaigns must be sensitive to data quality.[134] And his model suggests that they may achieve better results by relying on high-quality attributes from voter registration records (even though the attributes are only slightly predictive) in lieu of more predictive but inaccurate data gleaned from multiple, non-public data sources.[135] In effect, Hersh's study suggests that 10% of the political data does 90% of the work in explaining voter behavior, and this 10%

130. *See* supra note 93 and accompanying text.

131. JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 136 (2012).

132. ELECTING THE PRESIDENT, 2008: THE INSIDERS' VIEW 157–58 (Kathleen Hall Jamieson ed., 2009).

133. Eitan Hersh, At the Mercy of Data: Campaigns' Reliance on Available Information in Mobilizing Supporters (July 5, 2001) (unpublished manuscript), *available at* https://www.pdffiller.com/en/project/22848252.htm?form_id=321528.

134. *Id.* at 22, 25.

135. *Id.* at 22, 25–27.

comes from data that campaigns collect from public records.[136] Other academic researchers using different approaches have reached similar conclusions.[137] Even the chief data scientist in the Obama campaign, Rayid Ghani, seems to believe that voter registration records and response data are more instructive than any other data appended to these records.[138]

If the academics are correct, why do campaigns expend so much time, money, and effort in acquiring and analyzing non-public data, especially when this data is far more likely to raise serious privacy concerns? There are three likely answers. One is that party registration is available only in 27 states, so campaigns must acquire this information from PDBs.[139] Second, even if Hersh is correct that as much as 90 percent of the data makes relatively little difference, in very close elections, PDBs like Aristotle and Catalist may be successful at capturing the advantage of these additional few percentage points. Thus, candidates for whom this small advantage is the margin of victory are quite willing to pay for it.[140] And, finally, consulting firms have done a good job of marketing their services, in part by appealing to the data collection imperative mentioned above. In any case, even if there is limited empirical support for the proposition that more data is better, political actors show no signs of curbing their voracious appetite for voter data. This sets the table for examining the privacy risks of data-driven campaigns, to which we now turn.

II. PRIVACY VIOLATIONS AND HARMS ASSOCIATED WITH CAMPAIGN DATA PRACTICES

The accumulation of massive political dossiers for voter microtargeting purposes raises a number of threats to privacy. In particular, campaign data practices undermine *information privacy* by

136. E-mail from Eitan Hersh, Assistant Professor of Political Sci., Yale Univ., to Ira S. Rubinstein, Adjunct Professor of Law & Senior Fellow, Info. Law Inst., N.Y. Univ. Sch. of Law (July 1, 2013, 8:10 PM) (on file with author).

137. *See* KATE KENSKI ET AL., *supra* note 110, at 22–23 (verifying that party identification is highly predictive of election outcomes); *see also* Scherer, *supra* note 12 ("About 75% of the determining factors were basics like age, sex, race, neighborhood and voting record.").

138. *See* Salman Haqqi, *Obama's Secret Weapon in Re-election: Pakistani Scientist Rayid Ghani*, DAWN.COM (Jan. 21, 2013, 3:36 AM), http://beta.dawn.com/news/780327/obamas-secret-weapon-in-re-election-pakistani-scientist-rayid-ghani; *see also* Duhigg, *supra* note 12 ("Officials at both campaigns say the most insightful data remains the basics: a voter's party affiliation, voting history, basic information like age and race, and preferences gleaned from one-on-one conversations with volunteers.").

139. CVF REPORT, *supra* note 18, at 15.

140. IAB REPORT, *supra* note 12, at 7 & n.4.

diminishing the ability of individual voters to maintain control over their personal information while potentially violating the FIPs. Additionally, these practices threaten *political privacy* by compromising the personal sphere that many commentators consider necessary for both democratic deliberation and self-determination. Information privacy concerns the collection, use, and disclosure of personal information.[141] It is an increasingly familiar topic in law and policy as are the FIPs. In contrast, political privacy receives less explicit attention even though "it underwrites the freedom to vote, to hold political discussions, and to associate freely away from the glare of the public eye and without fear of reprisal."[142]

For privacy scholar Paul Schwartz, both information and political privacy concern the pre-conditions of democracy. Schwartz argues that the very meaning and purpose of the FIPs is to safeguard the democratic process.[143] However, for analytic purposes, it is helpful to separate information privacy concerns from political privacy concerns,[144] especially given the differences in the harms associated with each of them. The privacy harms that may result from violating the FIPs are extremely varied. For example, privacy scholar Daniel Solove's innovative work on conceptualizing privacy identifies four categories of privacy-threatening conduct, each of which is subdivided into different but related subgroups of harmful activities for a total of sixteen sub-categories.[145] Solove takes a similarly pluralistic approach to understanding the harms that may result from these diverse privacy problems. Privacy statutes and common law decisions tend to fixate on individual harms supported by proof of physical injury, financial loss, or emotional distress.[146] But Solove offers a more comprehensive analysis of individual and societal harm, one that encompasses psychological harms (like shame, embarrassment, ridicule, and humiliation), relationship harms, vulnerability harms, chilling effects, and power imbalances.[147] The harms associated with political privacy, on the other hand, are more unified; they almost always involve threats to the health and integrity of democratic life.

---

141. SOLOVE & SCHWARTZ, *supra* note 16, at 1.

142. C. Keith Boone, *Privacy and Community*, SOC. THEORY & PRAC., Spring 1983, at 1.

143. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 533, 557–65 (1995).

144. *See* Mary J. Culnan & Priscilla M. Regan, *Privacy Issues and the Creation of Campaign Mailing Lists*, 11 INFO. SOC'Y 85, 88 (1995).

145. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 103–05 (2008).

146. *Id.* at 174–75.

147. *Id.* at 174–79.

Before turning to the information privacy problems associated with campaign data practices and voter microtargeting, a brief review of the FIPs is necessary. The FIPs were conceived of almost 50 years ago in a privacy report by the U.S. Department of Health, Education, and Welfare (HEW), which responded to the growing use of automated data systems by public and private sector organizations for record-keeping purposes.[148] This groundbreaking report identified a "Code of Fair Information Practices" consisting of five core principles that would afford maximum protection to the personal data individuals were surrendering to these organizations:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him [or her] that was obtained for one purpose from being used or made available for other purposes without his [or her] consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him [or her].
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[149]

Over the years, these five core HEW principles have been expanded,[150] contracted,[151] codified,[152] and critiqued.[153] Among the more

148. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS) 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), *available at* http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf.

149. *Id.* at xx–xxi.

150. *See* Org. for Econ. Co-operation & Dev., *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD.ORG (Sept. 23, 1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [hereinafter OECD Guidelines]. The OECD Guidelines encompass eight principles: collection limitation, data quality, purpose specification, use limitation, data security, transparency, access and rectification, and accountability. *Id.*

151. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7–11 (June 1998), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a.pdf (limiting FIPs to four core principles—notice, choice, access, and security).

152. *See* Council Directive 95/46, 1995 O.J. (L281) 31 (EC).

important additions to the HEW principles are data minimization, limits on data retention, and accountability.[154] Recently, the White House, the European Commission, and the Organisation for Economic Co-operation and Development (OECD) have set out to re-examine the FIPs in light of the Internet and the profound changes it has wrought in the scale, complexity, and value of personal data in all aspects of modern life.[155] All of these efforts at updating the FIPs treat the expanded set of principles as fundamentally sound, even though they need to be supplemented in various ways. In short, despite divergent formulations,[156] the FIPs coalesce around a common set of principles. For the sake of clarity and convenience, the analysis that follows relies on the seven principles articulated in the White House Report: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[157]

Although the FIPs are universally recognized privacy principles, the unavoidable fact is that, in the U.S., the collection, use, and transfer of voter data face almost no regulation. Indeed, political actors mostly treat the FIPs as optional and non-binding. One significant reason is the First Amendment. As Kreiss observes, "institutional political actors . . . such as parties, candidates, and advocacy organizations, currently enjoy wide latitude to collect and store political data under the auspices of political speech."[158] This Article postpones consideration of possible First Amendment constraints on regulating campaign data practices until Part III.B, which examines the issue in detail. Political actors offer a second justification for avoiding the FIPs, namely, that political data mainly consists of public records or voluntarily provided data, neither of which raises any privacy concerns.[159] This, too, will be examined at some length below in Part II.A.5. For now, suffice it to say that any conclusory

153. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 342–43 (Jane K. Winn ed., 2006).

154. *See* OECD Guidelines, *supra* note 150.

155. *See, e.g.*, WHITE HOUSE REPORT, *supra* note 105; *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; Org. for Econ. Co-operation & Dev., *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)*, OECD.ORG, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (as amended July 11, 2013).

156. *See* Cate, *supra* note 153 (discussing six different versions of FIPs).

157. WHITE HOUSE REPORT, *supra* note 105.

158. Kreiss, *supra* note 14, at 72.

159. *See* SOLOVE, *supra* note 39 and accompanying text.

view of campaign data practices as beyond the scope of the FIPs encounters at least two problems: first, this is at best a partial justification given that a great deal of voter data is neither a public record nor voluntarily provided; second, it ignores the privacy problems that occur when political actors comingle voter data with large volumes of multiple types of additional data and use the resulting aggregate to profile and target individual voters.

This Part begins by examining three information privacy issues that arise when campaign data practices are evaluated against the requirements of the FIPs—lack of individual control, insecurity, and secondary use—and the resulting privacy harms. It then pauses to consider the reasons that political actors give for minimizing these privacy concerns. Next, this Part explores political privacy issues by analyzing the role of "information preserves" in democratic life, the constitutional dimensions of political privacy and the dignitary harms associated with voter microtargeting, as well as the overall impact on American democracy of compromising political privacy.

A. Information Privacy

1. LACK OF INDIVIDUAL CONTROL

The FIPs are premised on giving individuals control over personal information, where this implies empowering individuals to determine "when, how, and to what extent information about them is communicated to others."[160] According to the White House Report, individual control requires "clear and simple choices, presented at times and in ways that enable . . . meaningful decisions about personal data collection, use, and disclosure" as well as "means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place."[161] In fact, voters have few such "choices" or "means." The White House Report further notes that data brokers and other companies that collect personal data without "direct consumer interactions or a reasonably detectable presence in consumer facing activities" may find it impractical to implement individual controls.[162] It therefore recommends that they "go to extra lengths to implement other principles" such as transparency, access and accuracy, and accountability.[163]

Campaign data practices are deficient with respect to each of these requirements. Although the Obama (and Romney) campaign aggregated,

160. ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).
161. WHITE HOUSE REPORT, *supra* note 105, at 11.
162. *Id.* at 13.
163. *Id.*

integrated, and analyzed data from multiple sources, neither candidate nor their political parties offered voters a clear and concise description of campaign data practices *in their entirety* or what choices they had (if any) to (1) grant, limit, or withdraw consent about the collection, use, and disclosure of their personal data; (2) access, correct, or request the deletion of data about them; or (3) make an inquiry or lodge a complaint.[164] As Howard points out, "there's no chance of opting out of or accessing these political databases. We don't have access to our electronic political identities."[165] These problems are intensified for PDBs because most voters are clueless about their very existence much less the role they play in accumulating or integrating political data. It should not be left to voters to research the relationship between candidates and PDBs. Rather, campaigns must be more transparent about data-sharing arrangements with PDBs and impose enforceable contractual obligations requiring PDBs to handle the data consistently with the campaign's own privacy principles. Without greater visibility into the relevant agreements or practices, it is impossible to judge whether this is happening.

2. SECONDARY USE

All versions of the FIPs embody a purpose specification principle that prohibits the use or disclosure of data for purposes unrelated to those for which the data was initially obtained unless the organization holding the data first obtains the data subject's consent. Secondary use of political data may occur in any of three ways. First, as just discussed, campaigns may acquire personal data from a myriad of sources without obtaining the consent of the data subject to the use of the information for political purposes. This is far more likely to raise privacy concerns associated with secondary uses if the new uses are for incompatible purposes, if voters lack control over these new uses, and/or if the data is highly sensitive.[166]

Second, political actors may engage in secondary uses by transferring a political database to a third party. For example, in 2001, a bankrupt political web site sought to auction off its consumer database "including the e-mail addresses, party affiliations and political interests

164. *Romney Privacy Policy*, *supra* note 103; *Obama Privacy Policy*, *supra* note 62. The Obama Privacy Policy offers such rights for a very limited range of data such as web site account registration data and certain web site preferences. *Obama Privacy Policy*, *supra* note 62.

165. Verini, *supra* note 127.

166. Culnan & Regan, *supra* note 144, at 94–96.

of about 170,000 subscribers."[167] Under pressure from consumer watchdog groups, the company agreed, in accordance with its privacy policy, to sell its database "only to another political newsletter or political media company, not to a marketing or fund-raising company."[168] After Obama's victories in 2008 and 2012, similar questions arose about the transfer of the "Obama database" to new entities. For example, the campaign donated its e-mail list to the Inaugural Committee and eventually transferred some of its data assets to a successor group known as "Organizing for America."[169] This seems legitimate in cases where all of the data in question consists of unrestricted public record information or are covered by the Obama campaign's online privacy policy (which permits sharing of personal data "with organizations, groups or causes that we believe have similar viewpoints, principles or objectives").[170] Without more transparency regarding the sources and types of the transferred data, however, it is impossible to determine if these conditions were met.[171]

Third, organizations that control national voter files may engage in business activities that violate the letter or spirit of state laws prohibiting the transfer of voter registration data for non-political purposes. For example, people associated with the National Voter File Co-op, which contains both public record data and voter beliefs and preferences, have indicated an interest in selling voter data to companies for commercial purposes.[172] According to an attorney for the co-op, "information freely provided to the party by the voter, or data about who participated in a primary [that the party collects] is not subject to any prohibition on it being sold."[173] This is true as long as the co-op segregates all public records and voluntarily provided data from any other types of voter data and only offers the former for sale, provided further that the public record data originate in states that permit its sale for commercial use. Again, there is no way for outside observers to verify any of this.

---

167. Edmund Sanders, *Planned Sale of Voter.com's Data Raises Privacy Concerns*, L.A. TIMES, Mar. 8, 2001, http://articles.latimes.com/2001/mar/08/business/fi-34937.

168. *Id.*

169. Michael Isikoff, *Obama Campaign Gives Database of Millions of Supporters to New Advocacy Group*, NBC NEWS (Jan. 28, 2013, 1:48 AM), http://investigations.nbcnews.com/_news/2013/01/28/16726913-obama-campaign-gives-database-of-millions-of-supporters-to-new-advocacy-group.

170. *Obama Privacy Policy*, *supra* note 62.

171. *See* Confessore, *supra* note 12 (noting uncertainty over future role of Obama's voter data infrastructure).

172. *See* Lois Beckett, *Will Democrats Sell Your Political Opinions to Credit Card Companies?*, SALON (Feb. 6, 2013, 9:38 AM), http://www.salon.com/2013/02/06/will_democrats_sell_your_political_opinions_to_credit_card_companies_partner/.

173. *Id.*

3. INSECURITY

Data security incidents are a fact of modern life. A well-respected annual report of security incidents counted more than 2,500 data breaches in the last nine years, resulting in 1.1 billion compromised records.[174] Breaches occur due to multiple factors including hacking, loss or theft of storage devices, administrative and programming errors, and misuse or abuse of network privileges.[175]

Some of the most publicized hacking incidents in recent years are those involving attacks on government agencies[176] and CDBs.[177] Not surprisingly, state election agencies, campaign organizations, and PDBs have also suffered data breaches. For example, an advocacy group hacked into Chicago's voter database to demonstrate its inadequate security, thereby compromising the names, SSNs, and dates of birth of 1.35 million residents;[178] a suspect stole computers from a Tennessee election office with voter data including SSNs on 337,000 voters;[179] a web programming error forced a Pennsylvania election office to shut down a voter registration web site that exposed sensitive data of 30,000 voters to anyone who visited the web site;[180] a campaign web site was allegedly hacked exposing the private information of nearly 5,000 donors in a Minnesota Senatorial race;[181] and both the Obama and McCain campaigns were reportedly victims of a sophisticated cyberattack

---

174. *2013 Data Breach Investigations Report*, VERIZON (2013), http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

175. *Id.*

176. Dan Goodin, *FBI Warns Hacking Spree on Government Agencies Is a "Widespread Problem,"* ARS TECHNICA (Nov. 15, 2013, 6:35 PM), http://arstechnica.com/security/2013/11/fbi-warns-hacking-spree-on-government-agencies-is-a-widespread-problem/.

177. Chris Merritt, *Data Breach Trends in the Financial Sector*, LUMENSION (Feb. 23, 2012), http://blog.lumension.com/4687/data-breach-trends-in-the-financial-sector/ ("Overall, the CDB [Chronology of Data Breaches] has 2929 breaches in the 2005–2012 timeframe [sic], involving 544,591,013 records . . . ."); *see also* Brian Krebs, *Data Broker Giants Hacked by ID Theft Service*, KREBSONSECURITY (Sept. 25, 2013, 12:02 AM), http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/.

178. Privacy Rights Clearinghouse, *Chicago Voter Database*, CHRONOLOGY OF DATA BREACHES, https://www.privacyrights.org/node/1924 (last visited Oct. 14, 2014).

179. *Police Recover Stolen Election Computers*, WMC ACTION NEWS 5 (Jan. 18, 2008, 1:59 PM) http://www.wmcactionnews5.com/story/7742414/police-recover-stolen-election-computers.

180. Privacy Rights Clearinghouse, *supra* note 178.

181. Brian Prince, *Minnesota Sen. Coleman Deals with Donor Data Breach*, EWEEK (Mar. 12, 2009), http://www.eweek.com/c/a/Security/Minnesota-Senator-Coleman-Deals-With-Donor-Data-Breach/.

possibly by Russian or Chinese hackers.[182] There is every reason to believe that additional, unreported incidents have occurred, and that more serious incidents will occur in the future.[183]

Every organization must guard against curious staffers misusing network privileges to gawk at celebrity records. A more serious threat in political campaigns is that inadequately designed campaign tools with a social dimension may expose sensitive political data to anyone wishing to see it. For example, the Obama campaign's "call tool" enabled volunteers with a registered account to make canvassing calls from home without having to visit a local campaign office.[184] All they had to do was to sign into the Obama web site, access a list of targeted voters, and begin making calls using individualized scripts; they could also record their notes about the call for later analysis.[185] This tool exposed the target voter's personal data—name, location, telephone number, and political preferences (as reflected in the script)—to any registered account holder, ranging from Obama supporters, to political adversaries, to the idly curious.[186] Although earlier versions of the tool were especially ripe for abuse,[187] the Obama campaign defended the 2012 version on two main grounds: first, the data in question was publicly available and, hence, enjoyed weak or no privacy protections; and, second, the tool had built-in checks on the number of voters any volunteer could conceivably canvass.[188] But neither rationale survives closer scrutiny. The calling scripts were based on highly sensitive data, much of which was not in any public record.[189] And even if the tool prevented mass exposure of

182. Daren Briscoe et al., *How He Did It: Center Stage*, NEWSWEEK, Nov. 17, 2008, at 87.

183. *See, e.g.*, *Majority of Data Breaches Go Unreported*, IT SECURITY WATCH (July 23, 2012), http://www.itsecuritywatch.com/data-security/news/2012/07/majority-of-data-breaches-go-unreported/; *Majority of Malware Analysts Aware of Data Breaches Not Disclosed by Their Employers*, THREATTRACK SECURITY (Nov. 6, 2013), http://www.threattracksecurity.com/press-release/majority-of-malware-analysts-aware-of-data-breaches-not-disclosed-by-their-employers.aspx.

184. Lois Beckett, *Is Your Neighbor a Democrat? Obama Has an App for That*, PROPUBLICA (Aug. 3, 2012, 2:52 PM), http://www.propublica.org/article/is-your-neighbor-a-democrat-obama-has-an-app-for-that; Stephanie Mencimer, *The Democrats' Voter Privacy Fail*, MOTHER JONES (Oct. 21, 2010), http://www.motherjones.com/politics/2010/10/organizing-for-america-voter-privacy-fail.

185. Beckett, *supra* note 184; Mencimer, *supra* note 184.

186. Betsy Hoover, *How to Use the Online Call Tool on BarackObama.com*, YOUTUBE (Aug. 21, 2012), http://www.youtube.com/watch?v=qBiHhfSI83s.

187. Sandhya Somashekhar, *Conservatives Use Democratic Phone Bank for Own Purposes, Raise Privacy Concerns*, WASH. POST (Nov. 1, 2010, 9:47 AM), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/01/AR2010110102265.html.

188. Beckett, *supra* note 184; Mencimer, *supra* note 184.

189. Duhigg, *supra* note 12 (stating that scripts and call lists were based on "access to details like whether voters may have visited pornography Web sites, have

political preferences, it failed to address the reputational harms that individuals might suffer if, against their wishes, or simply as a result of erroneous data or inferences, a family member, neighbor, co-worker, or co-religionist learned that, for example, they did (or did not) support a candidate who favors same-sex marriage or reproductive rights.

4. PRIVACY HARMS

If the preceding Sections achieve the goal of demonstrating that campaign data practices fall short of what the FIPs require, a privacy skeptic still might declare, so what? How does the lawful collection of large volumes of information from diverse sources for purposes of sharing more interesting and relevant political communications conceivably hurt voters? In short, where is the harm? As noted above, Solove's taxonomy of privacy problems enumerates a range of privacy harms beyond those that courts traditionally have been prepared to remedy. In particular, Solove identifies several harms that come from aggregation (by which he means combining diverse bits of data about a person), exclusion (which is very similar to the failure to offer the access and accuracy demanded by the FIPs), secondary use, and insecurity.

Aggregation upsets settled expectations by revealing facts about individuals "far beyond anything they expected when they gave out the data."[190] And it enables powerful institutions to judge and make important decisions about people (e.g., whether to extend credit, provide insurance coverage, make a job offer, or solicit their vote) without their knowledge or direct input. These decisions may result from incomplete or inaccurate data and/or the use of what Turow calls "reputation silos," which dictate the flow of content to individuals and the availability of opportunities, based on preconceived profiles of who they are (or who else they resemble), for reasons they do not understand, using data over which they have little control.[191] Exclusion creates additional harms by heightening uncertainty over why a decision was taken and making people feel powerless and alienated from the forces that determine their chances in life.[192] And the potential for secondary use of personal data exacerbates an individual's fear and uncertainty over future uses of her digital dossier,[193] thereby "creating a sense of powerlessness and

homes in foreclosure, are more prone to drink Michelob Ultra than Corona or have gay friends or enjoy expensive vacations").

190. SOLOVE, *supra* note 145, at 119.

191. TUROW, *supra* note 85, at 190–92.

192. *See* Oscar H. Gandy, Jr., *Consumer Protection in Cyberspace*, 9 TRIPLE C: COGNITION, COMMUNICATION, CO-OPERATION 175, 176 (2012), *available at* http://www.triple-c.at/index.php/tripleC/article/view/267.

193. SOLOVE, *supra* note 39, at 13–26.

vulnerability."[194] Secondary uses may also have chilling effects that force individuals to withdraw from certain activities because they believe that refusing to give out data is the only way to prevent unwanted sharing.[195]

Finally, any unwarranted disclosure of personal data due to a security breach may cause harms ranging "from embarrassment to financial loss and physical harm."[196] A breach of political data may also cause unique harms such as "diminished faith in publicly supervised political processes."[197] Although the FIPs require secure and responsible handling of personal data, and this obligation is magnified when sensitive political data is at stake, little is known about whether political actors maintain adequate security measures due to a lack of transparency and oversight. Nor is it even clear whether existing federal and state computer security laws,[198] or security breach notifications laws,[199] apply to political databases.

Are voters suffering the harms of vulnerability, distortion, powerlessness, and chilling effects? A 2005 survey found that 23% of Californians say they have not registered to vote because they want their information to remain private.[200] A 2012 national telephone survey found that 86% of adult Americans "do not want political campaigns to tailor advertisements to their interests" and that 64% of voters would be less likely to vote for a candidate who engages in these practices.[201] There is also some evidence that voters in the political minority within their

194. SOLOVE, *supra* note 145, at 132.

195. Many scholars view databases as an instrument of surveillance. *See, e.g.*, DAVID LYON, THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND (2011); JAMES B. RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE, at x–xi (2007). For an early and influential analysis, see Roger A. Clarke, *Information Technology and Dataveillance*, *in* COMPUTERIZATION AND CONTROVERSY: VALUE CONFLICTS AND SOCIAL CHOICES 496, 498 (Charles Dunlop & Rob Kling eds., 1991) (defining dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons").

196. FTC REPORT, *supra* note 105, at 7–9; WHITE HOUSE REPORT, *supra* note 105, at 19.

197. Kreiss & Howard, *supra* note 14, at 1043.

198. Federal and state security laws apply to specific industrial sectors and to commercial entities regulated by § 5 of the FTC Act. Fewer than a dozen states require businesses to implement and maintain reasonable security procedures and practices to protect the personal information. *See* Thomas J. Smedinghoff, *The State of Information Security Law: A Focus on the Key Legal Trends*, 37 EDPACS: EDP AUDIT, CONTROL & SECURITY NEWSL., Jan.–Feb. 2008, at 1, 5–7, *available at* http://www.cert.org/archive/pdf/state_infosec_law0801.pdf. But many of these laws are too limited in scope to cover political actors.

199. *See supra* note 109.

200. Cal. Voter Found., *California Voter Participation Survey*, CALVOTER.ORG (Apr. 7, 2005), http://www.calvoter.org/issues/votereng/votpart/surveyresults.html.

201. Turow et al., *supra* note 20.

community are more concerned than those in the political majority with ballot secrecy and, indeed, all aspects of voter privacy.[202] However, the jury is still out on the extent or seriousness of these privacy harms because most Americans are still in the dark about the nature and extent of campaign data practices and voter microtargeting or their implications for information privacy.

5. WHY POLITICAL ACTORS MINIMIZE PRIVACY CONCERNS

Like commercial entities, political actors make statements professing to care about users' privacy.[203] Yet the preceding discussion establishes that campaign data practices violate multiple FIPs—individual control, transparency, access and accuracy, accountability, secondary use, and security. The reasons for this discrepancy are multiple and complex but fall into three main buckets: a penchant for secrecy, rationalizing away the problem by relying on false assumptions, and misunderstanding the contextual norms applicable to democratic elections.

a. A Penchant for Secrecy

While the FIPs emphasize openness and transparency, political actors prefer secrecy, which they perceive as a competitive advantage. "We have no interest in telling our opponents our digital strategy," said one Obama spokesperson;[204] another said: "They are our nuclear codes."[205] A Romney campaign official was more blunt: "You don't want your analytical efforts to be obvious because voters get creeped out."[206]

Political actors are cagey about their data practices for self-serving reasons. Campaign web sites post privacy notices yet they remain largely silent about the transfer of voter data to and from PDBs, whose practices are even more opaque. For example, Campaign Grid's privacy policy addresses the collection of data from its own clients (i.e., campaigns and consultants) but does not address how it handles individual voter data,

202. *See* Christopher F. Karpowitz et al., *Political Norms and the Private Act of Voting*, 75 PUB. OPINION Q. 659, 660 (2011), *available at* http://poq.oxfordjournals.org/content/75/4/659.full.pdf.

203. *See, e.g.*, Lois Beckett, *How Microsoft and Yahoo Are Selling Politicians Access to You*, PROPUBLICA (June 11, 2012, 11:45 AM), http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you.

204. *Id.*

205. Scherer, *supra* note 12 (quoting Obama campaign spokesman, Ben LaBolt); *see also* Barocas, *supra* note 14; Kreiss & Howard, *supra* note 14.

206. Duhigg, *supra* note 12.

and it emphasizes partner relationships without identifying these partners or describing their practices or policies.[207] In any case, PDBs (like CDBs) have no direct relationship with voters, making it extremely unlikely that a voter would happen upon the Campaign Grid's web site or invest time in reviewing its policies, especially when they offer voters no recourse against objectionable practices.

b. Rationalizing the Problem

Political actors tend to rationalize voter microtargeting in either of two ways. First, they claim voter microtargeting avoids using personal data and therefore is outside the scope of the FIPs.[208] Second, they argue that even if microtargeting implicates the FIPs, campaigns follow the highest commercial privacy standards.[209] Both claims are false.

The first claim disregards the privacy problems that arise even when campaigns rely solely on voter data consisting of non-PII. For example, voter microtargeting relies on a data infrastructure that includes both public data (which is not subject to the FIPs) and a great deal of personal data, ranging from the four types of web data (required, volunteered, observed, and inferred) to a vast array of consumer data sourced from multiple data brokers and data aggregators.[210] In short, this first justification by reference to public records is not only incomplete, but it also ignores the hybrid nature of political databases, which combine and integrate public and non-public data into an undifferentiated mass.

Moreover, the use of database technology has profound privacy implications. The computerization of public records transforms isolated and obscure bits of information into something far more accessible, storable, shareable, and searchable.[211] Twenty-five years ago, in a case holding that the release of FBI "rap sheets" was an invasion of privacy under the privacy exemption of the Freedom of Information Act, the Supreme Court noted that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[212] As Solove observes, this case shows that "privacy can be

207. *Campaign GRID's Online Privacy Policy and Practices*, CAMPAIGN GRID, http://www.campaigngrid.com/privacy/ (last visited Oct. 8, 2014).

208. *See infra* notes 216–20 and accompanying text.

209. *See infra* notes 226–27 and accompanying text.

210. *See supra* Part I.A.

211. SOLOVE, *supra* note 39, at 131–32.

212. *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763–64 (1989) (citing *Whalen v. Roe*, 429 U.S. 589, 605 (1977) (upholding a state law requiring computerized records of personal prescription drug

violated by altering levels of accessibility."[213] These early cases are but the tip of the iceberg for the emerging set of privacy issues associated with big data.[214]

Similarly, when political actors defend their data practices by suggesting that voters impliedly consent to later uses or transfers of information they volunteered about themselves, subject to the terms and condition of applicable privacy policies, they ignore the fact that national voter files contain both voluntarily provided data and other data that is not voluntarily provided. Moreover, the "voluntary" label is too easily applied when survey after survey demonstrates that people are unaware of the amount of data invisibly collected by web sites and social networking services. This "volunteered data"[215] is often voluntary in name only. Even response data—the very paradigm of voluntarily provided data—may not be truly voluntary. Most voters understand that when a campaign volunteer knocks on the door or calls a voter at home, any data they supply will be used by the campaign in support of a candidate or cause. But many fewer voters are likely to realize that in a data-driven campaign, their response data is translated into a standardized format, uploaded to a computerized voter file, combined with other data in a massive database, shared as the campaign sees fit, and retained indefinitely in a manner that allows predictive data analysis for voter microtargeting purposes.

Finally, political actors claim that voter microtargeting is outside the FIPs to the extent that it relies on anonymous data. For example, in the 2012 election cycle, a number of PDBs developed the ability to match the data in national voter files with online, cookie-based profiles and began offering new services capable of delivering targeted ads to voters at any web site they might visit.[216] Targeted Victory and its partner Lotame stated that matching would occur "in an anonymous and privacy-safe manner."[217] Similarly, Campaign Grid later argued that the

information, while also noting that there is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files . . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.")).

213. SOLOVE, *supra* note 39, at 143.

214. The Obama Administration recently completed a 90-day review of big data and privacy. *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

215. *See supra* Part I.A.3.

216. *See supra* notes 80–85.

217. *See* Matthias Reynolds, *Targeted Victory Partners with Lotame to Expand Audience Targeting Platform*, TARGETED VICTORY (Mar. 12, 2012), http://www.

cookies it used to target voters did not contain, collect, or convey any PII.[218] Instead, each cookie contains anonymous, non-personally identifiable categories of information.[219] These aggregated anonymous demographic categories are derived from off-line sources, and the applicable category for a user is assigned to a cookie when the user registers through one of Campaign Grid's registration partners and *exercises a choice to allow third-party marketing*.[220]

This line of defense is telling for three reasons. First, this supposed "choice to allow third-party marketing" is more rhetorical than real. When consumers register with a service whose privacy policy states that it may share their personal data with unspecified partners, for unspecified purposes, at some unspecified future date, this hardly constitutes consent to secondary uses. To the contrary, ordinary web activities such as buying goods or services, subscribing to a magazine, going online to read a book or stream music or movies, or even watching cable TV, all leave a data trail that political actors exploit for targeting purposes[221] without having first obtained a voter's consent. Second, cookie matching inflames longstanding consumer concerns over combining online and off-line data without explicit affirmative consent.[222] And yet some PDBs now boast about utilizing cookie-matching techniques that give political actors the ability "to cross the offline-to-online digital divide" and for the first time "target individuals online based on their *actual* offline political and civic behavior."[223] Third, this appeal to anonymous data assumes that

---

targetedvictory.com/2012/03/targeted-victory-partners-with-lotame-to-expand-audience-targeting-platform/; *see also* Beckett, *supra* note 203.

218. *See* Lois Beckett, *Web Cookies Used by Companies to Tailor Political Ads You See Online*, HUFFINGTON POST (Oct. 23, 2012, 12:27 PM), http://www.huffingtonpost.com/2012/10/23/companies-web-cookies-political-ads_n_2005723.html.

219. *Id.*

220. Jordan Lieberman et al., *Yes We Can (Profile You) – And Our Political System Is Stronger for It. An Industry Response from Campaign Grid to a Recent Essay in the Stanford Law Review Online*, CAMPAIGN GRID (Feb. 7, 2012), https://web.archive.org/web/20120218181102/http://www.campaigngrid.com/_blog/CampaignGrid_News/post/Yes_We_Can_%28Profile_You%29_And_Our_Political_System_Is_Stronger_for_I_An_Industry_Response_from_CampaignGrid,_LLC/ (retrieved from Internet Archive). This blog posting responds directly to Kreiss, *supra* note 14.

221. McCoy, *supra* note 12.

222. When DoubleClick sought to combine web-tracking and off-line data in the early 2000s, it provoked a severe consumer backlash, which led directly to the advertising industry's adoption of its first self-regulatory code of conduct. *See* Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 906 (2011); Stefanie Olsen, *FTC Drops Probe into DoubleClick Privacy Practices*, CNET (Jan. 22, 2001, 5:35 PM), http://news.cnet.com/2100-1023-251325.html.

223. *Catalist and DSPolitical Announce New Partnership Bringing Cutting Edge Online Targeting to Progressive Community*, PR NEWSWIRE (July 24, 2012), http://www.prnewswire.com/news-releases/catalist-and-dspolitical-announce-new-partnership-bringing-cutting-edge-online-targeting-to-progressive-community-163540246.html.

as long as digital advertising firms take some steps to anonymize or "de-identify" voter data, they have fully satisfied any conceivable privacy obligation owed to voters. This is naïve and disingenuous. De-identification is not only difficult technologically but also highly controversial from a policy standpoint.[224] More importantly, the mere fact that unknown firms playing a hidden role take obscure steps to anonymize data may not be all that comforting to users who believe they are being spied on.[225]

The second rationalization relied upon by political actors—that campaigns follow the highest industry standards—reflects the creeping commercialization of political campaigns. Online advertising and voter microtargeting have much in common: a vast data infrastructure, the ability to construct detailed individual profiles, and the application of statistical modeling techniques to identify and persuade targeted consumers or voters. Nor do political actors shy away from this comparison with commercial activities.[226] Rather, they defend their own data practices by insisting that they abide by the highest commercial privacy standards. Both points are captured in a post-election op-ed by the data director of Obama for America, Ethan Roeder, in which he tellingly states: "You may chafe at how much the online world knows about you, but campaigns don't know anything more about your online behavior than any retailer, news outlet or savvy blogger."[227]

But Roeder's argument falls short on two counts. First, campaigns probably know quite a bit *more* about voters than commercial firms know about consumers. After all, campaigns engage in certain practices that the advertising industry is uncomfortable with. These include merging online and off-line data and utilizing sensitive data without restraint. And both the Obama and Romney campaigns developed innovative methods for gaining access to their supporters' social networks with scant regard for the privacy implications of encouraging

224. There is a large and growing literature on whether anonymization remains an effective strategy for protecting privacy. *Compare* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010), *with* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 (2011).

225. TUROW, *supra* note 85, at 190 ("If a company can follow and interact with you in the digital environment . . . its claim that you are anonymous is meaningless, particularly when firms intermittently add offline information to the online data and then simply strip the name and address to make it 'anonymous.'").

226. Robert Draper, *The Late Adopters*, N.Y. TIMES MAGAZINE, Feb. 17, 2013, at 31 (quoting Obama's political director as comparing targeted voters' interaction with the Obama campaign to shopping online at Amazon); Duhigg, *supra* note 12 (quoting Romney's political director as comparing voting to shopping at Target stores).

227. *See* Ethan Roeder, *I Am Not Big Brother*, N.Y. TIMES, Dec. 6, 2012, at A35.

web site visitors to sign-in using Facebook credentials[228] or asking supporters to download a social networking app that sends targeted campaign messages to their Facebook friends.[229] Second, over the years, the online advertising industry has sought to ward off federal privacy legislation by developing self-regulatory codes of conduct (which prohibit the targeting of consumers based on certain types of sensitive data)[230] along with a variety of privacy-friendly consumer tools such as "ad icons" that provide information about behavioral advertising and give consumers some ability to block such ads.[231] And yet, neither the Obama nor the Romney campaigns signed up to use these codes. At best, the campaign web sites notified users that their web sites use third-party cookies and other tracking technologies, but they offered no effective means of control beyond self-help remedies (i.e., advice about changing

228. *See* Micah L. Sifry, *Yes They Can: What Voters Have Lost and Campaigns Have Gained From 2008 to 2012*, TECH PRESIDENT (Mar. 13, 2012), http://techpresident.com/news/21902/yes-they-can-what-voters-have-lost-and-campaigns-have-gained-2008-2012 ("[B]oth the Obama and Romney campaigns try very hard to get people to sign up on their websites [sic] using Facebook, which automatically enrolls them in the campaign's Facebook apps. . . . [B]oth the Obama and Romney apps can not only access your basic info, including name, picture, gender, birthday, religious and political views, they can also post status messages, notes, photos and videos on your behalf and access your data when you're not using the app.").

229. The Obama technical team developed a social outreach program known as "targeted sharing" that matched voter data with Facebook information so that Obama supporters could persuade their friends to vote for Obama. *See* Scherer, *supra* note 12. The Obama supporter had to download a Facebook app, which automatically shared his or her Facebook friend list with the campaign; campaign data analysts then matched these friends' lists with their internal lists of persuadable voters and devised the optimal campaign message for targeting each of them. *See id.* Using this app, over a million Obama supporters contacted approximately 5 million of their friends with various campaign messages. *Id.*; *see also* Madrigal, *supra* note 12. This use of Facebook as a politically oriented social organizing tool raises some complex privacy issues, which are characteristic of all social-networking apps. *See generally* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (discussing "peer-to-peer" privacy violations). In the case of targeted sharing, these privacy issues stem from the very different position and choices available to Obama supporters versus their friends. The former group opts-in to participating in this program, while the latter group has no opportunity to consent either to sharing their Facebook profiles with the Obama campaign or to the campaign matching their profiles with their voter records. *See* Kate Kaye, *Democratic Firm Ties Voter Data to Facebook Friends*, CLICKZ (July 24, 2012), http://www.clickz.com/ clickz/news/2193630/democratic-firm-ties-voter-data-to-facebook-friends.

230. *See, e.g.*, NETWORK ADVERTISING INITIATIVE, 2013 NAI CODE OF CONDUCT 3 (2013), www.networkadvertising.org/2013_Principles.pdf (imposing additional obligations on targeting of "[s]ensitive [d]ata," including "[n]on-PII related to precise health information and sexual orientation").

231. *See infra* note 310.

browser preferences or visiting external web sites to learn more about opting-out of third-party cookies).[232]

c. Mistaking the Context

Finally, in claiming (falsely) that campaign data practices adhere to advertising industry privacy standards, political actors implicitly endorse the idea that the informational norms associated with commercial ads should also govern the activity and setting of political campaigns. The privacy scholarship of Helen Nissenbaum strongly emphasizes the connection between privacy concerns and the norms governing distinct social contexts.[233] Nissenbaum's theory of privacy as contextual integrity begins with the observation that norms govern the flow of information in highly specific social contexts.[234] Familiar social contexts include health care, education, employment, religion, family, and the commercial marketplace.[235] These and other contexts may be more fully understood in terms of the roles people play within them, the activities and practices they engage in within such roles, the norms that define acceptable and unacceptable behaviors within a given context, and the values around which activities in a given context are defined. Different social contexts have distinctive sets of rules governing information flows. Nissenbaum identifies two fundamental types of informational norms: appropriateness (which prescribes what personal data is (or is not) allowable, expected, or even required to be revealed in a given context) and distribution (which prescribes how and with whom data may be shared in a given context).[236] These and other informational norms define contextual integrity, which is preserved when such norms are respected and violated when they are breached.

Nissenbaum discusses the informational norms governing voting (and electronic voting)[237] but has less to say about political campaigns, although she does note that campaign web sites are new enough that "no preexisting rules apply."[238] According to Nissenbaum, the "right

232. *See* Daniel Castro, *Comparing the Privacy Policies of the Presidential Campaign Websites*, INNOVATION FILES (Aug. 2, 2012), http://www.innovationfiles.org/comparing-the-privacy-policies-of-the-presidential-campaign-websites/.

233. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 176–77, 214–15 (2010).

234. *Id.* at 129–30.

235. *Id.*

236. *Id.* at 144–45; *see also* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 101, 138–43 (2004).

237. *Id.* at 176–77.

238. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 44 (2011), *available at* http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf.

approach" to tracking voters who visit political web sites "is not an opportunistic information grab. Although this may serve immediate needs of an imminent political campaign, it does not serve the purposes of encouraging frank political discussion, which is understood to flourish in environments of great freedom."[239] A more thorough analysis of campaign data practices using Nissenbaum's theory is beyond the scope of this Article. However, her point is obvious. Laissez-faire norms govern the marketplace, and individuals are free to seek their best advantage by buying and selling their property as they see fit.[240] But these norms are out of place in the context of democratic elections, which are animated by very different ends, purposes, and goals.[241] And every mainstream political candidate intuitively understands that certain data gathering practices should be avoided. For example, political actors *could* photograph everyone who attends a political event, *could* use facial recognition software to link them to their Facebook profiles or Flickr albums and learn their names,[242] and *could* scrape their social networks to discover useful data for targeting purposes.[243] But it seems safe to say that few candidates would risk violating implicit campaign norms prohibiting these practices, especially when they may rely on less controversial methods of voter profiling.

B. Political Privacy

The preceding Section focused mainly on the individual harms that occur when political actors collect, use, and disclose data in disregard of the FIPs. In contrast, political privacy mainly implicates the integrity and health of American democracy. It therefore marks a shift from privacy as an individual value to privacy as a social or public value that matters to individuals in their role as citizens.[244] This Section begins by describing a

239. *Id.* at 45; *see also* Parry, *supra* note 12.

240. *See, e.g.*, MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY 103–15 (1983).

241. *Id.* at 100–01, 306–11; *see also* Spencer Overton, *Restraint and Responsibility: Judicial Review of Campaign Reform*, 61 WASH. & LEE L. REV. 663, 707–18 (2004) (describing the democratic values animating elections and voting). Not only are marketplace norms different from voting norms, in the U.S., vote buying is illegal in federal elections and in all fifty states. *See* Richard L. Hasen, *Vote Buying*, 88 CALIF. L. REV. 1323, 1323 (2000).

242. Declan McCullagh, *Face-Matching with Facebook Profiles: How It Was Done*, CNET (Aug. 4, 2011, 7:40 PM), http://www.cnet.com/news/face-matching-with-facebook-profiles-how-it-was-done/ (describing research showing how to match photographs of students to their Facebook profiles).

243. Bonneau et al., *supra* note 60.

244. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225–27 (1995).

theory of privacy as constitutive of democracy and then considers the political harms that may result from tracking and targeting voters.

1. PRIVACY AND DEMOCRATIC PARTICIPATION

There is widespread agreement among both First Amendment and privacy scholars that privacy is a precondition of democratic life. As Thomas Emerson writes:

> In its social impact a system of privacy is vital to the working of the democratic process. Democracy assumes that the individual citizen will actively and independently participate in making decisions and in operating the institutions of society. An individual is capable of such a role only if he can at some point separate himself from the pressures and conformities of collective life.[245]

Responding to then-recent debates over the twin menaces of communism and mass society, Emerson viewed privacy as a redoubt from collective life—a zone in which the individual can "think his own thoughts, have his own secrets, live his own life, reveal only what he wants to the outside world."[246] Although the threats to freedom of thought have shifted from collectivism to pervasive surveillance and the creation of digital dossiers, Emerson's idea of privacy as a legally protected "preserve" or "zone" still resonates in the work of leading contemporary privacy scholars such as Paul Schwartz,[247] Julie Cohen,[248] and Neil Richards.[249]

---

245. THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 546 (1970).

246. *Id.* at 545.

247. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999). Schwartz argues that privacy rules are needed to establish "information preserves," i.e., areas or spaces insulated from surveillance, manipulation, and coercion, and that such information preserves, premised on the FIPs, are necessary for democracy to flourish. *Id.* at 1667.

248. In her recent work, Cohen seeks to reconceptualize privacy as shorthand for "breathing room to engage in . . . processes of boundary management" that enable and constitute self-development. *See* COHEN, *supra* note 131, at 149. With a nod to Schwartz, Cohen views privacy as protecting "the capacity for autonomous choice and self-determination" while noting that "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship." Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013).

249. In contrast to Schwartz and Cohen, Richards' work focuses explicitly on freedom of thought. *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008) (defining intellectual privacy as "the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others"). According to Richards, First Amendment theory has largely neglected

Political privacy also has constitutional dimensions. As Priscilla Regan observes, political privacy is a "public value" that supports democratic political systems.[250] As such, it is constitutive of the rights of anonymous speech and freedom of association.[251] Additionally, it implicates the institution of the secret ballot[252] and the right to vote without undue burdens.[253] It would be very helpful in establishing the privacy rights of voters if there were strong constitutional arguments to the effect that data-driven campaign practices and voter microtargeting undermine or threaten these core political rights.[254] Indeed, there is a very strong argument that campaign data practices and voter microtargeting undermine anonymous speech by subjecting voters to a form of political surveillance in which their beliefs and preferences are monitored and tracked. This argument is simple: If, per *McIntyre v. Ohio Elections Commission*,[255] an author's decision to omit his or her name from campaign literature is "an aspect of the freedom of speech protected by the First Amendment,"[256] then surely an author's—or a voter's—underlying thought process also must be protected as a necessary aspect of intellectual privacy.

---

intellectual privacy, in part because the surveillance of intellectual activity is itself a fairly new phenomenon only made possible by two recent developments: digital dossiers and data-driven decision making. *See id.* at 389.

250. REGAN, *supra* note 244, at 226–27.

251. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (holding that state election law requiring disclosure of one's name on campaign materials had potential chilling effect on citizens and infringed right of anonymous speech, which outweighed any government interests in preventing election fraud); *NAACP v. Alabama*, 357 U.S. 449 (1958) (holding that state licensing requirement infringed right of association where NAACP proved that disclosure of membership list would result in reprisals, threats, and hostility).

252. In *Burson v. Freeman*, 504 U.S. 191 (1992), the Court upheld a ban on distributing campaign literature within a 100-foot zone around polling places, reasoning that a restricted zone was necessary to help prevent voter intimidation and election fraud, and that all 50 states and numerous other Western democracies deploy similar means to overcome these twin evils, namely, "a secret ballot secured in part by a restricted zone around the voting compartments." *Id.* at 206.

253. *See* Schwartz, *supra* note 143, at 570–71 (citing *Greidinger v. Davis*, 988 F.2d 1344, 1354–55 (4th Cir. 1993) (holding that Virginia's practice of requiring SSNs for voter registration purposes and sharing them with third parties unconstitutionally burdened the right to vote largely due to concerns over identity theft and related financial harm)).

254. Given the longstanding difficulties in recovering for privacy wrongs absent proof of physical injury, financial loss, or emotional distress, it seems unlikely that courts would extend the *Greidinger* holding to cases involving campaign data practices and voter microtargeting unless a major security breach of political databases occurred, resulting in identity theft or in pervasive instances of "re-identification" using voter registration data.

255. 514 U.S. 334 (1995).

256. *Id.* at 342.

This line of argument is anticipated in Julie Cohen's work on the right to anonymous reading and receiving of ideas.[257] Cohen's argument takes off from an alternative interpretation of *McIntyre* and its progeny in light of *Lamont v. Postmaster General*,[258] which reviewed a 1962 federal statute requiring that the post office detain unsealed foreign mailings that it had determined were "communist political propaganda" and deliver them only upon the addressee's written request.[259] The Court struck down the statute on the ground that this affirmative obligation amounted to an unconstitutional limitation of the addressee's First Amendment rights due to its chilling effect.[260] Cohen argues that when *Lamont* and *McIntyre* are read together, they support a broad right of anonymity that extends to all aspects of communication, not only speaking but "the entire series of intellectual transactions through which [individuals form] the opinions they ultimately choose to express."[261] And if the First Amendment protects the right to read anonymously, then this protection also must extend to seeking information online and refusing to share information about one's tastes, preferences, interests, and beliefs, which is exactly the type of information that campaigns obtain through cookie-based profiling. In short, Cohen's broad understanding of the freedom to read anonymously suggests that voters are entitled to seek and gain access to online political information without having to disclose their political leanings or suffer the chilling effect of pervasive monitoring and tracking of their every thought and belief.[262] In the face of such pervasive monitoring and tracking of voters' online behavior by every campaign web site and every ad-funded online newspaper, magazine, blog, and most other sources of political information, surely the First Amendment must protect voters' freedom of thought. If not, an essential precondition of democracy will be undermined.

---

257. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996). In the almost 20 years since Cohen published her article, the privacy concerns about reading anonymously have shifted from copyright management tools to advertising and other big data uses. *See, e.g.*, David Streitfeld, *As New Service Track Habits, the E-Books Are Reading You*, N.Y. TIMES (Dec. 24, 2013), http://www.nytimes.com/2013/12/25/technology/as-new-services-track-habits-the-e-books-are-reading-you.html (describing companies that "get reading data from subscribers who, for a flat monthly fee, buy access to an array of titles, which they can read on a variety of devices").

258. 381 U.S. 301 (1965).

259. *Id.* at 302.

260. *Id.* at 307.

261. Cohen, *supra* note 257, at 1007.

262. *See* EMERSON, *supra* note 245; REGAN, *supra* note 244; Richards, *supra* note 249; Schwartz, *supra* note 247.

2. POLITICAL HARMS

In recent years, commentators have analyzed the ways in which the growing reliance on political dossiers and voter microtargeting not only undermine political privacy but also threaten democratic interests.[263] Hillygus and Shields argue that candidates have started taking more extreme positions on wedge issues and advertising these positions to "cross-pressured" voters (i.e., voters who generally support the opposing party but may agree with the candidate on these wedge issues).[264] They further argue that voter microtargeting makes this strategy possible by allowing "candidates to surgically deliver different messages to different constituencies."[265] This discussion of political privacy would be incomplete without briefly considering the political harms associated with voter microtargeting. The following paragraphs rely on Hillygus and Shields' analysis as a starting point to help organize the relevant literature on the potentially harmful implications of voter microtargeting for American democracy.[266]

The political harms that Hillygus and Shields discuss fall into three broad categories. The first involves political inequality, which takes the specific form of paying attention to a strategic set of voters in selected districts as determined by voter modeling techniques, while ignoring others.[267] Some candidates court a small group of crucial voters rather than a majority of the people, a strategy that Howard calls "political redlining."[268] These candidates write off whole segments of the population who either do not test well for approved messages, live in districts that are not in play, or who are least likely to vote.[269] Voter microtargeting thereby makes possible a political strategy that not only departs from the democratic ideal but also exacerbates inequities in the American political system, which routinely ignores voters who have been "excluded or marginalized from the political process."[270] Even worse,

263. Kreiss & Howard, *supra* note 14, at 1034; *see also* Barocas, *supra* note 14, at 33–34; Parry, *supra* note 12. *See generally* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU 147–64 (2011); CASS SUNSTEIN, REPUBLIC.COM 2.0 (2007).

264. HILLYGUS & SHIELDS, *supra* note 110, at 4.

265. *Id.* at 151.

266. *Id.* at 186–93.

267. *Id.* at 186–87.

268. Verini, *supra* note 127.

269. *See Audiences: Politics and Public Affairs: Data-Driven Digital Advertising for Candidates and Causes*, AUDIENCE PARTNERS, http://www.audiencepartners.com/audiences/#politics (last visited Oct. 8, 2014) ("In politics and public affairs, only a small percentage of the public matters. The rest is waste.").

270. Barocas, *supra* note 14, at 33 (citing findings by HILLYGUS & SHIELDS, *supra* note 110, at 13–15, that the overall contact rate for registered and non-registered

some candidates may utilize voter microtargeting techniques to expand or suppress turnout among specific subgroups of voters.[271]

The second category of political harms consists of superficial politics, a term encompassing many related sins. "Candidates emphasize wedge issues because they help create a strategic advantage, not because they are necessarily the most important issues."[272] Campaign messages therefore have little to do with the priorities of the American public. Of course, political candidates have always said what they think people want to hear, not what they should hear. But voter microtargeting makes politics not only superficial but also distorted and insular.[273] Distortion occurs when candidates precisely calibrate which message will appeal to certain individuals, create multiple versions of the same message, and deliver them to individuals meeting the predetermined criteria, via e-mail, online ads, cable TV, or social media.[274] As Peter Swire points out, when candidates "know exactly what each voter cares about . . . it creates a huge temptation to exaggerate or lie."[275] Insularity is a side effect of superficiality and distortion because voter microtargeting makes it increasingly difficult to have a public argument when there is no "basis for a common conversation about . . . political decision[s]."[276] Kreiss and Howard refer to this breakdown in public discourse as "the democratic deficit," a problem they associate with a lack of political leadership.[277] As Bennett and Mannheim observe, elite actors "are increasingly less likely to 'lead' because they are more likely to reinforce latent opinions than to reframe them."[278]

The third category of political harms is the crisis in governance that results when a superficial and fragmented campaign dialogue drives

---

voters began to diverge in the early 1990s, when electronic voter files first became widely available).

271. *See* Nichole Rustin-Paschal, *Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues*, 19 WM. & MARY BILL RTS. J. 907, 925 (2011) (describing the use of online profiling for voter suppression purposes).

272. HILLYGUS & SHIELDS, *supra* note 110, at 187.

273. *See* Parry, *supra* note 12.

274. *See* Murphy, *supra* note 12, at 45–46 (noting that "a single [Obama] fundraising email came in no less than 11 different varieties" and that the Romney campaign's digital director boasted about being able to "beam totally different messages to two voters in the same house").

275. Verini, *supra* note 127.

276. PARISER, *supra* note 263, at 155–56 (contrasting targeted messages with broadcast TV ads); *see also* KENSKI ET AL., *supra* note 110, at 307 (commenting on Obama's use of "interpersonal microtargeting" to create "insular worlds, [in which] individuals find shelter from counterarguments and scrutiny of their candidate's problematic claims").

277. Kreiss & Howard, *supra* note 14, at 1044–45.

278. Bennett & Manheim, *supra* note 113, at 213.

a wedge between campaigning and governing. As Hillygus and Shields note, "It is difficult to construct a sustainable notion of electoral accountability without a shared public discourse on the candidates' policy positions and future agendas."[279] Swire anticipated this dilemma in 2004 when he explained to a reporter:

> In the nightmare, every voter will get a tailored message based on detailed information about the voter . . . . There might even be several different messages sent by a candidate to the same home—one for the wife, one for the husband and one for the 23-year-old kid . . . . [This] means that the public debates lack content and the real election happens in the privacy of these mailings. The candidate knows everything about the voter, but the media and the public know nothing about what the candidate really believes. It is, in effect, a nearly perfect perversion of the political process. [280]

III. A MODEST PROPOSAL

Having explored voters' privacy interests by showing how the misuse and abuse of voter data may violate the FIPs and result in both privacy and political harms, this Article now sets forth a two-part proposal for addressing several of these harms. The first part borrows a page from the federal campaign finance system by imposing a new form of disclosure and disclaimer requirements on political actors. Specifically, Congress would amend the Federal Election Campaign Act (FECA) to require political actors to (1) disclose their campaign data practices to the general public and (2) provide a disclaimer identifying targeted advertising materials as such. By exposing campaign data practices to the light of day, these transparency measures would foster individual control over voters' personal data and encourage candidates to adopt better practices by seeking to retain and, thereby, avoid potential reputational injuries that might cost them an election.

The second part seeks to limit the harmful effects of campaign data practices and voter microtargeting, but to do so without directly regulating the speech of political actors. Rather, it would impose FIPs-based rules on certain currently unregulated aspects of the existing commercial data infrastructure and some related advertising practices. This component draws upon FTC Commissioner Julie Brill's "Reclaim

279. HILLYGUS & SHIELDS, *supra* note 110, at 189.

280. *See* Gertner, *supra* note 72.

Your Name" initiative.[281] Arguing that big data brokers are "taking advantage of us without our permission,"[282] Brill calls upon Congress "to require data brokers to provide notice, access, and correction rights to consumers scaled to the sensitivity and use of the data at issue."[283] Her proposal also urges industry to adopt a voluntary "Do Not Track" (DNT) standard that "would allow consumers to choose when their online data is monitored for marketing purposes."[284] Brill's initiative would complement the transparency measures imposed on political actors by enabling voters to find out how data brokers are collecting and using data about them and selling it to political actors for voter microtargeting purposes; it would also allow them to opt-out of such uses or correct errors in information used to target them if they so choose.

Admittedly, this two-part proposal is "modest" in the sense that it imposes relatively few burdens on political actors as compared with the more robust privacy principles recommended in both the White House Report and the FTC Report. For example, it does not address security and only indirectly addresses the political harms discussed above.[285] But it is modest by necessity because it operates in the shadow of the First Amendment. Under well-established doctrine, political speech is "central to the meaning and purpose of the First Amendment,"[286] which "'has its fullest and most urgent application' to speech uttered during a campaign for political office."[287] At first glance, then, it seems very likely that the

---

281. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the Twenty-Third Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013).

282. *Id.* at 11.

283. *Id.* at 10.

284. *Id.* at 11. In an earlier report, the FTC urged industry to develop a "uniform and comprehensive consumer choice mechanism," involving a DNT list, which would be implemented either "by legislation or . . . through robust, enforceable self-regulation" and might involve "placing a setting on a consumer's browser to signal whether [he or she] want[ed] to be tracked or to receive targeted advertisements." *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS 66 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Although a W3C working group has been trying to adopt a DNT technical standard for over three years, progress has been very slow and the group may never reach consensus. *See* Wendy Davis, *Ad Industry Urges Web Standards Group to Abandon Do-Not-Track Effort*, MEDIAPOST (June 19, 2014, 4:38 PM), http://www.mediapost.com/publications/article/228399/ad-industryurges-web-standards-group-to-abandon-d.html.

285. *See supra* Part II.B.2.

286. *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 329 (2010); *see also Shapero v. Ky. Bar Ass'n*, 486 U.S. 466, 483 (1988) (O'Connor, J., dissenting) ("Political speech . . . is at the core of the First Amendment.").

287. *Eu v. S.F. Cnty. Democratic Cent. Comm.*, 489 U.S. 214, 223 (1989) (quoting *Monitor Patriot Co. v. Roy*, 401 U.S. 265, 272 (1971)); *see also Brown v. Hartlage*, 456 U.S. 45, 52–53 (1982).

Court would subject privacy-based limitations on campaign data practices and voter microtargeting to strict scrutiny, which is usually fatal. Nor does it help matters that in a series of disclosure cases involving both campaign finance laws and ballot initiatives, the Court has adopted a very narrow understanding of privacy interests.[288] However, this first impression is misguided. The modest proposal described below is both reasonably effective and does not impermissibly restrict speech-related campaign activity.

A. The Two-Part Proposal

1. DISCLOSURES AND DISCLAIMERS

Disclosure is an important form of campaign finance regulation at both the state and federal levels.[289] Many view it as "an essential element in any effort to guarantee a relatively open, transparent democratic process."[290] In a series of decisions beginning with the landmark case of *Buckley v. Valeo*,[291] the Supreme Court has generally upheld mandatory campaign disclosure laws.[292] In a few narrow cases, however, it has also ruled that disclosure can violate the First Amendment when it prevents anonymous speech by individuals concerning ballot initiatives[293] or exposes the members and supporters of minority parties to threats, harassments, and reprisals.[294] In *Buckley*, the court upheld the campaign disclosure and disclaimer requirements in FECA mainly on the grounds that they helped to deter corruption and the appearance of corruption.[295] After briefly discussing these requirements, this Section examines how to adjust them for purposes of making campaign data practices and voter microtargeting more transparent to voters.

Federal election law requires the disclosure of campaign contributions and expenditure by a variety of individuals and political actors. In particular, "federal political committees"[296] must register with

288. *See infra* notes 345–49 and accompanying text.

289. Richard Briffault, *Campaign Finance Disclosure 2.0*, 9 ELECTION L.J. 273 (2010).

290. Trevor Potter, *Campaign Finance Disclosure Laws*, *in* NEW CAMPAIGN FINANCE SOURCEBOOK 123 (Anthony Corrado et al. eds., 2005).

291. 424 U.S. 1 (1976) (per curiam).

292. *See, e.g.*, *id.* at 143.

293. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995).

294. *Brown v. Socialist Workers Comm.*, 459 U.S. 87, 101 (1982).

295. *Buckley*, 424 U.S. at 66–67.

296. Potter, *supra* note 290, at 127. "Federal political committees . . . include candidate campaign committees, political parties, and political action committees" and

the FEC and, along with certain other individuals and organizations, file periodic disclosure reports regarding donors and/or expenditures.[297] In addition, various "public communications"[298] must bear an advertising disclaimer, which identifies who paid for and/or authorized the communication.[299] Additionally, TV and radio ads must include an audio statement indicating who is responsible for the content of the ad.[300] In practice, these disclosure requirements are complex and burdensome. Moreover, they require a large bureaucracy to receive reports describing millions of financial transactions from thousands of filers.[301] Campaign disclosure requirements are also rife with exceptions and evasions.[302]

The proposed disclosure and disclaimer regime as applied to campaign data practices would be far simpler in every respect. It would simply require campaign committees and political parties that collect personal data from voters, or that compile, maintain, or use voter files, to provide comprehensive notices on their web sites of their data processing practices. This notice requirement is directed at voters and entails no reporting to the FEC and therefore requires little bureaucratic activity or oversight. And while the goal of campaign privacy disclosures and disclaimers is not to reduce political corruption, these requirements share with the campaign finance disclosure system the broader goal of safeguarding the democratic process by making it more open and transparent. They also would achieve this by using very similar means, namely, providing voters with information needed to control the collection and use of their personal data by political actors, exposing potentially invasive campaign data practices to the light of day, and giving regulators and intermediaries access to information necessary to detect and discourage bad behavior.

Every version of the FIPs requires transparency in the form of disclosure of the details of personal data collection and use. Web sites and services typically implement the transparency and individual control

---

hence encompass most of the "political actors" under discussion throughout this Article. *Id.*

297. *Id.*

298. *Id.* at 129.

299. *Id.*

300. *Id.* at 129–30.

301. *See* FED. ELECTION COMM'N, ANNUAL REPORT 4 (2004), *available at* http://www.fec.gov/pdf/ar04.pdf (stating that the FEC entered 2,131,999 detailed records in its database). Appendix 5, Statistics on Commission Operations, further states that in the 2004 election cycle, the FEC received reports of over $8.2 billion in campaign transactions from over 7,000 filers. *Id.* at 79.

302. *See* MOLLY MILLIGAN, CTR. FOR GOVERNMENTAL STUDIES, LOOPHOLES, TRICKS AND END RUNS: EVASIONS OF CAMPAIGN FINANCE LAWS, AND A MODEL LAW TO BLOCK THEM 1 (2009), *available at* http://policyarchive.org/collections/cgs/index?section=5&id=21930.

principles by posting a privacy policy describing the key elements of their data practices, such as what information they collect from users, why and how the organization uses and protects such information, and what choices, if any, a user has in providing such information or restricting its use and/or retention. Because this modest proposal relies so heavily on transparency and individual control to protect very sensitive voter information, it is important that political actors face a heightened burden of disclosure.

One of the most privacy-protective disclosure rules on the books today is the recently amended Children's Online Privacy Protection Act (COPPA) rule.[303] If the rigorous transparency requirement found in COPPA were translated into the political sphere, it would mandate that political actors disclose: (1) what personal information they collect from voters or obtain about them from third parties and how they use this data; (2) their data-sharing practices including any transfers of this data for secondary uses; (3) the purposes for which they collect this data (including any use of persistent identifiers in connection with voter microtargeting) and whether the provision of such information for the purposes indicated is voluntary or optional; (4) what opportunities voters have to obtain access to and correct or delete this data and/or to prevent its further use or maintenance, including any choices for limiting the use of this data in voter microtargeting; (5) the length of time they retain this data; (6) relevant security measures applied to this data; and (7) applicable oversight measures including where and how voters may lodge a complaint.[304]

Robust privacy disclosures along these lines would give voters all the information they need to understand the scale, scope, and sensitivity of the personal data that political actors have accumulated about them from all sources as well as the use of such data for voter microtargeting purposes. In theory, this would enable voters to make meaningful decisions about the collection, use, and disclosure of their voter data. In practice, many voters may not fully benefit from these heightened disclosures due to longstanding deficiencies with the informed choice

303. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2014). *See generally* Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(A)(i)–(ii), (b)(2) (2012). Although COPPA addresses the unique privacy and safety risks that arise when young children access the Internet, it seems especially relevant here for two reasons: first, both COPPA and the proposed disclosure regime deal with sensitive information; and, second, the COPPA rule represents the FTC's most recent efforts to devise transparency requirements that confront many of the recent technological developments discussed above (such as the explosion of social networking, the proliferation of mobile web technologies, and the use of persistent identifiers that recognize a user over time and across different web sites or online services in connection with targeted advertising).

304. *See* § 6502(b)(1)(A)(i), (b)(1)(A)(iii), (b)(2).

model. This is a large topic, but the two main deficiencies are: first, almost all privacy notices are long and incomprehensible, so that nobody reads or understands them;[305] second, even if users fully comprehend privacy notices, providing them with a choice is not necessarily the same as protecting their privacy.[306] More generally, the informed choice model tends to advance procedural requirements over substantive protections such as data quality, data minimization, and avoidance of harm.[307] What, if anything, might be done to make privacy disclosures more effective in the political setting, taking into account any unique aspects of political campaigns?

Research suggests that people respond best to information when it is "embedded" in their decision-making routines, which in turn requires that the information contribute to achieving the user's goals.[308] When voters visit a campaign web site or otherwise interact with a campaign or political party, their primary goal is to learn about the issues and the candidates and decide whom to vote for, not to protect their privacy and security interests. As noted previously, any interaction with a campaign web site results in the collection and use of observed and inferred data.[309] If a voter also decides to play an active role in a campaign by volunteering, donating money, reaching out to a friend through social media, and so on, the campaign will also collect and use required and volunteered data. In either case, privacy disclosures are likely to be effective only if they relate to the primary task of deciding which candidates to support. If privacy disclosures merely help voters decide how to weigh the costs and benefits of the collection, use, or disclosure

305. *See, e.g.*, Cate, *supra* note 153, at 358–61 (critiquing the informed choice model of privacy); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL. INFO. SOC'Y. 543, 563–66 (2008) (demonstrating the excessive amounts of time it takes consumers to make informed choices about privacy by reading privacy policies); Schwartz, *supra* note 247, at 1660–63, 1681–85 (critiquing the same as Cate, *supra* note 153).

306. *See* Schwartz, *supra* note 247, at 1660–63, 1681–85; *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 256–59 (2011).

307. *See* Cate, *supra* note 153, at 355–56. For many years, U.S. privacy policy suffered from this flaw. In their recent reform efforts, however, both the FTC and the White House have recognized that informed choice alone is insufficient and have therefore begun to insist on a more robust version of the FIPs. *See* FTC REPORT, *supra* note 105, at 24; WHITE HOUSE REPORT, *supra* note 105, 9–22.

308. ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 55–65 (2007) (arguing that embedded decision making depends on the value of the information in achieving user's goals, its compatibility with decision-making routines, and its comprehensibility). For a similar view derived from lab studies of privacy notices, see Lorrie Faith Cranor, *Privacy Notice and Choice in Practice*, LORIE.CRANOR.ORG (July 2013), lorrie.cranor.org/talks/notice-choice-pets2013.pdf.

309. *See supra* note 62 and accompanying text.

of voter data, voters will ignore them just as they do commercial privacy policies.

This is where disclaimers might play an especially useful role. Suppose that targeted political communications (via web content, e-mail, and ads) had to include a disclaimer that not only identified who paid for and/or authorized the communication but also a label or icon indicating that the ad in question is targeted.[310] Suppose further that this label or icon (consistent with the Brill proposal) had to include a link to (1) additional information about how targeting works and what data it depends on and (2) a choice mechanism allowing voters to permit or prevent the collection, use, or disclosure of their data for voter microtargeting purposes. If—and, as discussed below, this is a big if—the icons were prominently displayed, easy to recognize and understand, meaningful in the choices they offered, and standardized (i.e., consistent across all parties and candidates), then disclaimers might help voters achieve meaningful control over their personal information in the course of deciding which candidate to support. In other words, disclaimers would help ensure that privacy disclosures were embedded in voters' decision-making routines regarding the candidate. There are several reasons why this approach might work.

This Article focuses mainly on presidential campaigns, which are all about candidates persuading "donors, staffers, activists, and voters that their vision of where they want to take the country is credible,

310. For example, the Digital Advertising Alliance (DAA), a consortium of leading national advertising and marketing associations, has created the "AdChoices" icon, which it characterizes as:

> [A] sign for consumer information and control for interest-based advertising . . . . When you see the AdChoices Icon on a Web page or near a Web banner, it lets you know that information used to infer your interests is being gathered or used to improve the ads you see. By clicking on the AdChoices Icon, you learn about how interest-based ads are delivered to you. More importantly, the AdChoices Icon gives you the ability [to] control whether you receive interest-based advertising and from which companies.

See Frequently Asked Questions, ADCHOICES, http://www.youradchoices.com/faq.aspx (last visited Oct. 8, 2014). The DAA's AdChoices program offers consumers a limited form of control by enabling them to opt-out of *receiving* targeted ads. *Id.* In contrast, the most recent version of the W3C's Do Not Track proposal allows consumers to opt-out of data collection, retention, use, and sharing. As stated by Justin Brookman, a co-chair of the W3C Tracking Protection Working Group (which is drafting the Do Not Track specification), "The meaning of the Do Not Track signal is now standardized—it means you're telling a server that you don't want it to collect data about you across different companies' websites [sic]." *See* Justin Brookman, *At Last, Some Progress on Do Not Track*, CENTER FOR DEMOCRACY & TECH. (Apr. 24, 2014), https://cdt.org/blog/at-last-some-progress-on-do-not-track/.

achievable, and preferable to that of any other candidate."[311] Candidates express their vision through a message, and a winning candidate must at all times maintain control over his or her message, which means making sure that the many messages they send out are "coherent, unified, and account for the actions of the opponent."[312] In short, messaging boils down to the candidate establishing his or her own character and credibility, how he or she relates to the party and its platform, and how he or she differs from opposing candidates, while undermining the opponent's character and credibility, chipping away at the foundation of his or her vision, and undermining any professed differences between the candidate and his or her party.[313]

In the battle over campaign messaging, privacy disclosures and disclaimers become additional grist for the mill. Over the past decade, privacy-related stories have emerged as an important sub-genre of technology reporting. There are quite a few examples of adverse publicity forcing firms accused of violating consumers' privacy expectations to modify their data collection practices or to back down on plans to change their privacy terms by combining or using data in new ways.[314] In short, there is evidence that if a firm's reputation comes under attack due to criticism of its privacy practices, the firm will often choose to preserve its reputation by modifying its data practices.[315] It seems reasonable to suppose that if a newspaper published a negative story on a campaign's privacy practices and blogs and other news outlets ran this story until it became "viral," the campaign would respond by changing the offending practices rather than risk losing control of the news cycle or, ultimately, the candidate's message.[316] Indeed, a few episodes in which a presidential campaign underwent a crisis precipitated by a major

311. SAMUEL L. POPKIN, THE CANDIDATE: WHAT IT TAKES TO WIN – AND HOLD – THE WHITE HOUSE 33 (2012).

312. *Id.* at 35.

313. *Id.* at 36.

314. *See, e.g.*, Miguel Helft, *Google Alters Buzz to Tackle Privacy Flaws*, N.Y. TIMES (Feb. 13, 2010, 11:48 PM), http://bits.blogs.nytimes.com/2010/02/13/google-alters-buzz-to-tackle-privacy-flaws/; Seth Rosenblatt, *Microsoft Revises Privacy Policy in Wake of Hotmail Search Case*, CNET (Mar. 21, 2014, 2:13 PM), http://www.cnet.com/news/microsoft-revises-privacy-policy-in-wake-of-hotmail-search-case/; Donna Tam, *Facebook Deletes Controversial Privacy Policy Language*, CNET (Nov. 15, 2013, 4:24 PM), http://www.cnet.com/news/facebook-deletes-controversial-privacy-policy-language/. For a discussion of the effect of reputational sanctions on privacy (and security) decisions, see Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1440–44 (2011).

315. *See* Ira S. Rubinstein & Nathan Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1377–407 (2013).

316. *See* POPKIN, *supra* note 311, at 50–51; *see also* Rutenberg, *supra* note 12 (comparing presidential campaigns to "start-ups aimed at a one-day sale").

security breach, a serious transgression of intellectual privacy norms, or a losing candidate's sale of voter data to a commercial entity would undoubtedly shine a spotlight on campaign data practices and possibly launch an era of heightened transparency across the political spectrum.[317]

Ideally, icon-based privacy disclaimers would make campaign data practices and voter microtargeting more salient to the average voter or at least more interesting and available to privacy advocates and/or reporters covering the emerging topic of data-driven campaigning. To begin with, potentially hundreds of millions of voters would interact with targeted political ad icons. If the icons were visually arresting and/or perceived by voters as linking to important information or choices, then some number of voters would take action in response to seeing them, making it incumbent upon political actors to justify their practices or risk alienating voters. Second, even if very few voters notice or click on these ad icons,[318] privacy advocates will do so and analyze and publicize whatever they find out. So will a candidate's political opponents. Indeed, the most important group holding a candidate accountable for his or her campaign data practices may well be the opposition party and candidates. This might result in negative publicity in the form of reporters highlighting various shortcomings in a campaign's data practices or a candidate's media team going after his or her opponent's privacy practices on similar grounds. Third, icons might assist researchers in compiling examples of targeted ads from the same campaign and analyzing them to determine if a candidate's targeted messages are consistent or contradictory across a range of audiences.[319]

In short, there are reasons to believe that *campaign* disclosure and disclaimers may be more salient than consumer privacy notices in purely commercial settings. If campaign data and related microtargeting practices emerge as a controversial topic in presidential campaigns, candidates may well decide to end a disputed practice that places them in

317. FUNG ET AL., *supra* note 308, at 106–10 and accompanying text (discussing the role of crises in jumpstarting transparency systems). Of course, this requires a crisis of sufficient magnitude to drive far more negative news coverage than any candidate has experienced to date. *See supra* note 12.

318. In fact, the DAA's "AdChoices" program has met with mixed success. Several recent user studies by researchers found numerous shortcomings with choice mechanisms related to online behavioral advertising including the AdChoices icon. For an overview of these experimental studies, see Cranor, *supra* note 308. For an industry response, see Peter Kosmala, *Yes, Johnny Can Benefit from Transparency and Control*, ABOUT ADS BLOG (Nov. 3, 2011), http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control.

319. *See* Barocas, *supra* note 14, at 34–35 (proposing a project called "Soap Box" that "would function as a clearinghouse for targeted, tailored campaign materials, forcing candidates to account for and reconcile the different positions they present to different audiences").

a bad light rather than risk defeat in an all-or-nothing contest. Or—even better for privacy purposes—campaign-related privacy controversies may force candidates to take steps designed to make their campaigns less vulnerable to such controversies in the first place.[320]

On the other hand, election campaigns are a unique setting in which time is a precious resource and relatively few issues remain in the public spotlight for very long. Obviously, voter privacy is at best a secondary or tertiary issue compared to war and peace, the economy, health care and social security benefits, and so on. So it is quite possible that voter privacy issues will not garner sufficient attention to provoke these salutary changes in campaign data practices. Hence, the need for additional measures as described below.

2. RESTRICTING COMMERCIAL DATA PRACTICES

The Fair Credit Reporting Act (FCRA) requires that credit agencies and other firms that collect and analyze consumers' financial information to assess credit, housing, and employment risks provide consumers with notice, access, and correction rights.[321] FTC Commissioner Brill's "Reclaim Your Name" proposal responds to a group of privacy challenges linked to the growing use of big data techniques by the credit industry as well as by firms not traditionally regulated under FCRA.[322] In response to these challenges, Brill has proposed that companies build more privacy protections into their products and services, perform risk assessments, and minimize and de-identify data whenever possible.[323] Additionally, if companies do not implement these measures voluntarily, she supports legislation requiring data brokers "to give consumers the ability to access their information and correct it when it is used for eligibility determinations, and the ability to opt-out of information used for marketing."[324] Finally, data brokers would be obliged to follow a risk-based approach by "tailor[ing] their data handling and notice and

320. These further steps might include adhering to self-regulatory codes of conduct followed by the online advertising industry, *see* Bennett, *supra* note 222, at 908–12, or employing a Chief Privacy Officer (CPO) to take charge of campaign-related privacy issues. The CPO would be responsible for ensuring that the campaign (1) complies with applicable privacy laws, (2) designs and implements data and targeting practices that satisfy voter (and societal) expectations regarding "appropriate" conduct in a political campaign, and (3) develops an integrated set of data and targeting practices—including the campaign privacy policy—that fits within the candidate's unified messaging.

321. *See generally* Fair Credit Reporting Act, Pub. L. No. 91-508 (1970) (codified at 15 U.S.C. §§ 1681–1681x (2012)).

322. Brill, *supra* note 281, at 4–5.

323. *Id.* at 9.

324. *Id.* at 9–10.

choice tools to the sensitivity of the information at issue."[325] According to Brill, these steps would also complement the FTC's ongoing support for "a universal, simple, persistent, and effective Do Not Track mechanism that allows a consumer to stop companies from mining cyberspace for information about her for marketing purposes."[326]

If data brokers and other commercial firms that rely on big data were to implement Brill's Reclaim Your Name proposal, this would address a number of the privacy concerns with campaign data practices as well. To begin with, it would allow voters to access some of the information about them held by PDBs, correct or supplement any part of their political dossier governed by the proposal, and opt-out of the use of their (non-public) personal data for marketing purposes, including the sale of such information to political actors for delivering targeted messages. These measures would give voters the knowledge and tools to reassert control over their personal data, thereby addressing both individual control and secondary use issues. It would not address security issues except to the extent that greater transparency might raise public doubts about whether political actors are taking steps to safeguard voter data adequately and have the know-how to handle a major security incident. But Reclaim Your Name would indirectly address some of the privacy and political harms analyzed in earlier Sections. For example, it would enable voters who take issue with their profiles to access some of the information in their dossiers and correct any information that is inaccurate or out-of-date (if they so wished) or to opt-out of receiving targeted ads,[327] thereby reducing autonomy-based harms such as

325. *Id.* at 10.

326. *Id.* at 11 (noting that the FTC prefers a system that would "allow consumers to make choices about tracking that would travel with them wherever they went in cyberspace; that would apply across the ecosystem to all types of tracking; that would be easy to find and use; and that would let consumers stop, not just the serving of targeted ads, but the collecting of their personal information as they browsed online or used their mobile devices"). There is considerable disagreement about the meaning of DNT and whether it would be an effective privacy tool. The following analysis avoids taking a position on competing proposals. Rather, it assumes that Congress has enacted Brill's Reclaim Your Name program in full, including a DNT system that satisfies the various criteria set forth in earlier FTC reports on behavioral advertising. *See* Brill, *supra* note 281, at 11. Of course, the W3C may not succeed in finalizing a specification along these lines. For a discussion of the key issues on which the Tracking Protection Working Group has failed to reach consensus, see *A Status Update on the Dev. of Voluntary Do-Not-Track Standards: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 113th Cong. 6–8 (2013) (statement of Justin Brookman, Director, Consumer Privacy Ctr. for Democracy & Tech.), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=f262274e-003e-4945-b238-82434b69007f.

327. Acxiom, a very large data broker, recently launched a web site, Aboutthedata.com, where individuals may view information that Acxiom collects about them from various sources, remove or correct any data that is in error, and opt out of

aggregation and exclusion. At the same time, Reclaim Your Name would cast a spotlight on voter microtargeting and its use in political redlining and superficial politics. Greater access to political databases would in turn make it easier for privacy advocates and public interest groups to understand the relationship between specific data sets and targeted campaign materials, providing additional insights into how candidates present their positions to different audiences and whether they are consistent in their messaging.

B. First Amendment Concerns

Having set forth the two-part proposal, this Article now turns to the constitutional principles developed in the campaign finance cases to show how a disclosure and disclaimer regime would pass constitutional muster. Next, it argues that for First Amendment purposes, the Reclaim Your Name proposal should be treated no differently from other extant privacy laws that would survive constitutional review if analyzed under commercial speech standards, although it would need to overcome a number of serious objections, including those discussed in the *Sorrell* decision.

1. DEFENDING DISCLOSURE AND DISCLAIMER REQUIREMENTS

The obvious starting point for examining privacy disclosures and disclaimers in the election context is *Buckley*, which upheld contribution limits, disclosure requirements, and the public financing system established by FECA, but which struck down the limits on spending by candidates, campaigns, and individuals.[328] In its analysis, the Court rejected the goal of "equalizing" influence and voices in the electoral process as legitimate reasons for restricting contributions and expenditures.[329] Instead, the Court held that the only government interest sufficient to warrant such restrictions were the prevention of corruption or the appearance of corruption.[330] The Court then drew a sharp

receiving tailored ads based on "Acxiom's online and/or offline marketing data." *See* Natasha Singer, *Acxiom Lets Consumers See Data It Collects*, N.Y. TIMES (Sept. 4, 2013), http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html (noting that critics object that the site omits many details about Acxiom's data-gathering and analysis practices and promotes "data-driven marketing without explicitly describing some of Acxiom's more sophisticated consumer-tracking techniques").

328. *Buckley v. Valeo*, 424 U.S. 1, 143 (1976).

329. *Id.* at 48–49.

330. *Id.* at 26–27. The Court never explicitly defined corruption but warned that, "[t]o the extent that large contributions are given to secure a political *quid pro quo* from

distinction between the First Amendment implications of a restriction on expenditures, which "necessarily reduces the quantity of expression,"[331] and a limitation on contributions, which "entails only a marginal restriction upon the contributor's ability to engage in free communication."[332] Having drawn this sharp distinction, the Court upheld contribution limits because they posed a danger of quid pro quo corruption but struck down restrictions on independent expenditures because they did not.[333]

The *Buckley* Court concluded that FECA's disclosure and reporting regime is constitutionally valid primarily on the grounds that it imposes no ceiling on campaign-related speech activities and serves important government interests.[334] The Court also considered whether the required dissemination of individual donor information under § 434(e) amounted to a form of compelled disclosure in violation of the privacy and associational rights recognized in *NAACP v. Alabama.*[335] Applying a standard of "exacting" scrutiny,[336] the Court found that the benefits of a disclosure and reporting regime far outweighed the costs, reasoning that disclosure reduced corruption (1) by providing the electorate with information about the sources of election-related spending, (2) "by exposing large contributions and expenditures to the light of publicity," and (3) by "gathering the data necessary to detect violations of the contribution limitations."[337] These benefits outweighed the costs of disclosure, which the Court saw in terms of exposing potential contributors to "harassment or retaliation."[338] While acknowledging that "[t]hese are not insignificant burdens on individual rights," the Court concluded that they were "the least restrictive means of curbing the evils . . . that Congress found to exist."[339] In its most recent campaign finance decision, the Court has continued to emphasize that even though disclosure requirements burden speech, "they do not impose a ceiling on speech" and therefore represent "a less restrictive alternative to flat bans on certain types or quantities of speech."[340]

---

current and potential office holders, the integrity of our system of representative democracy is undermined." *Id*.

331. *Id.* at 19 (for example, "by restricting the number of issues discussed, the depth of their exploration, and the size of the audience reached").

332. *Id.* at 20–21.

333. *Id.* at 28–29, 45.

334. *Id.* at 64.

335. 357 U.S. 449 (1958).

336. *Buckley*, 424 U.S. at 64–65.

337. *Id.* at 66–68.

338. *Id.*

339. *Id.* at 68.

340. *McCutcheon v. Fed. Election Comm'n*, 134 S. Ct. 1434, 1459–60 (2014).

Although the *Buckley* court gave short shrift to what this Article calls information or political privacy concerns, in the dissenting portion of his own opinion, then-Chief Justice Burger argued that the public right to know is not absolute "when its exercise reveals private political convictions" and that a threshold of $100 for having to report contributions fails to give sufficient weight to competing First Amendment values.[341] In 1980, Congress adjusted the disclosure threshold from $100 to $200[342] yet even this higher threshold deprives individual contributors of control over clearly sensitive information from which it is easy to infer their political beliefs. As McGeveran points out, *Buckley* and its progeny "place too little emphasis on the privacy costs of disclosure"[343] while greatly overstating its benefits.[344] Despite these criticisms, neither Congress nor the courts have taken any steps toward adopting a more privacy-sensitive disclosure policy.[345]

A recent decision involving the disclosure of the names of supporters of a referendum that unsuccessfully sought to overturn a Washington law extending various benefits to same-sex couples further reinforces these observations. In *Doe v. Reed*,[346] the Court refused to block the public release of the names of backers of this ballot measure, notwithstanding a reasonable probability that they would be subject to threats, harassment, and reprisals (as were supporters of California's Proposition 8).[347] Relying heavily on the campaign finance precedents, the Court emphasized that the state public records law "is not a prohibition on speech, but instead a *disclosure* requirement."[348] The Court then applied "exacting scrutiny" in holding that the disclosure of supporters' names was justified based on the state's interest in preserving electoral integrity.[349]

---

341. *Buckley*, 424 U.S. at 237 (Burger, J., concurring in part and dissenting in part).

342. Federal Election Campaign Act Amendments of 1979, Pub. L. No. 96-187, 93 Stat. 1339 (1980) (codified as amended at 2 U.S.C. § 432(c)(3) (1980)).

343. McGeveran, *supra* note 43, at 14–20.

344. *Id.* at 24–33; Briffault, *supra* note 289, at 286–90.

345. For a privacy-sensitive disclosure framework, see Deborah G. Johnson et al., *Campaign Disclosure, Privacy and Transparency*, 19 WM. & MARY BILL RTS. J. 959, 976–82 (2011), and McGeveran, *supra* note 43, at 48–54.

346. 561 U.S. 186 (2010).

347. *Id.* at 201.

348. *Id.* at 196. "[D]isclosure requirements may burden the ability to speak, but they . . . do not prevent anyone from speaking." *Id.* (quoting *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 366 (2010)).

349. *Id.* at 196, 199. In *Doe*, the only question before the Court was whether disclosure of petitioners' names in general violated the First Amendment—not disclosure of this same-sex rights petition in particular. *Id.* at 200. The Court left open the possibility of an as-applied challenge to disclosure in this specific case. *Id.* at 201. For an analysis of

These decisions justifying the value of election-related disclosures strongly suggest that the Court would also uphold a FECA amendment requiring political actors to be more transparent about their campaign data and voter microtargeting practices. Like a campaign disclosure requirement, a transparency rule based on the FIPs neither reduces the quantity of expression nor prevents anyone from speaking.[350] Transparency serves important government interests such as providing voters with information about the collection, use, and disclosure of their personal data. As noted above, this is information that voters may find highly relevant to deciding whether to register to vote or otherwise participate in election campaigns in the first place.

Moreover, the information disclosed in a privacy policy implicates voters' privacy interests and may help limit both privacy and political harms.[351] And it is certainly less burdensome than other ways of preventing these harms, such as requiring political actors to obtain opt-in consent to the collection and use of voter data for microtargeting purposes. Most importantly, in the campaign finance cases, as in *Doe,* the Court balanced the benefits of disclosure to the public and to democracy against the burdens of disclosure to individuals who would suffer a potential loss of privacy. In weighing the interests affected by the proposed data transparency rule, however, the Courts would have to compare the benefits of disclosure, both to the public and to democracy, against the likely privacy burdens. Unlike the campaign finance cases, where it is individuals who suffer privacy burdens associated with disclosure, here the disclosure burden falls on organizations, not individuals. But there is no personal data at stake when organizations disclose their data processing practices, and hence no privacy-based burdens to weigh in the balance.

2. REGULATING DATA BROKER PRACTICES

If Congress enacted laws consistent with Brill's Reclaim Your Name proposal, they would restrict campaign data practices and voter microtargeting in several ways. The proposal's data broker provisions grant consumers access, correction, and certain opt-out rights, thereby

---

the "cramped view of privacy interests" at work in both the campaign finance cases and *Doe*, as well as how a better-developed privacy theory would result in a wiser disclosure policy in election law, see William McGeveran, *Mrs. McIntyre's Persona: Bringing Privacy Theory to Election Law*, 19 WM. & MARY BILL RTS. J. 859, 861, 865–70 (2011).

350. *See* Marshall, *supra* note 101 (comparing the reasons for and against the prohibition of corporate campaign expenditures in *McConnell* with the arguments for and against regulation of deceptive campaign speech and concluding that because the Court upheld the former, it would also uphold the latter).

351. *See infra* Part II.A.4, II.B.2.

potentially limiting the overall availability of consumer data to all customers including PDBs. Thus, political actors would have less access to consumer data for political marketing, fund raising, and get-out-the-vote efforts. Similarly, a DNT provision would limit the ability of web sites and commercial advertising firms to gather information for targeted marketing from individuals who signal their wish not to be tracked or targeted for online ads (including political ads). In other words, both provisions indirectly affect political actors to the extent that they purchase data or services from commercial data brokers.[352]

In short, Brill's proposal regulates commercial activities by limiting the sharing and use of personal information to protect consumers' privacy, yet it affects both commercial and political actors engaged in targeted marketing activities. Do these restrictions constitute an abridgement of free speech under the First Amendment? The following analysis tackles this question by considering the very broad issue of whether privacy rules in general are consistent with the First Amendment. First, it reviews and rejects the argument that the FIPs create a "right to stop people from speaking about you" and hence that any regulation limiting the collection, use, and disclosure of personal data violates commercial speech standards. Second, it analyzes *Sorrell v. IMS Health, Inc.*[353] and concludes that the FIPs satisfy the "heightened scrutiny" standard explored in *Sorrell*.

a. Do the Fair Information Practices Violate the First Amendment?

The view that the FIPs are incompatible with the First Amendment is widely associated with a 2000 law review article by Eugene Volokh. He argued that while the FIPs may sound plausible in the abstract, "my right to control your communication of personally identifiable information about me is a right to have the government stop you from speaking about me. We already have a code of 'fair information practices,' and it is the First Amendment."[354]

352. DNT would also affect political actors directly to the extent that they engage in their own tracking and targeting of voters by placing first- or third-party tracking cookies on voters' browsers when they visit a party or campaign web site.

353. 131 S. Ct. 2653 (2011).

354. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000). Others besides Volokh have contributed to this "First Amendment critique" of privacy rules. *See* Neil Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1162–63 nn.53–60 (2005) (citing additional sources).

Volokh's position sounds convincing in part because it draws upon decades of case law in which speech rights trump the tort of public disclosure of private facts.[355] As Schwartz points out, however, Volokh treats the FIPs as if the entire set of principles were directed at preventing the disclosure of true facts.[356] This is far from the case. Rather, a closer look at the FIPs demonstrates that most of them "regulate the business practices of private entities without silencing their speech."[357] As Schwartz points out, the only FIPs that even roughly "correspond to Volokh's idea of information privacy as the right to stop people from speaking about you" are the principles addressing individual control and limitations on secondary use.[358] But disclosure and use restrictions are very common elements of privacy statutes, and Schwartz defends them against First Amendment objections with a familiar point: as long as such laws are viewpoint-neutral, they are "a necessary element of safeguarding free communication in our democratic society."[359]

A more recent and detailed response to Volokh by Neil Richards bolsters and expands the scope of Schwartz's argument.[360] Richards begins by dividing privacy rules that implicate information flows into four categories: collection rules, use rules, nondisclosure rules, and telemarketing rules.[361] He then demonstrates that well-established First Amendment doctrine fully supports existing privacy regulations. Courts typically treat collection and use rules as outside the scope of the First Amendment because they are rules of "general applicability."[362] Both types of rules are ubiquitous in the law, and they raise few constitutional difficulties.[363] In a handful of cases interpreting the Fair Credit Reporting

355. *See, e.g.*, *Fla. Star v. B.J.F.*, 491 U.S. 524, 526 (1989); *Okla. Publ'g Co. v. Dist. Court*, 430 U.S. 308, 308–09 (1977); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975).

356. Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1561–62 (2000).

357. *Id.* at 1562 (arguing that the FIPs are "akin to a broad range of other measures that regulate information use in the private sector and do not abridge the freedom of speech under any interpretation of the First Amendment").

358. *Id.* at 1562–63.

359. *Id.* at 1563.

360. *See* Richards, *supra* note 354.

361. *Id.* at 1181–210.

362. *Id.* at 1186.

363. *Id.* at 1190–94. Courts are divided over whether to treat privacy rules that restrict the use of certain information for marketing purposes as commercial speech subject to the *Central Hudson* test or as economic conduct that can be regulated without First Amendment implications. In *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), the court, applying the *Central Hudson* test, invalidated an FCC rule prohibiting telephone companies from using customer information for marketing purposes without the opt-in consent of their customers. *Id.* at 1233–39. In 2007, the FCC modified the order at issue in *U.S. West* so that opt-in consent would be required only with respect to a

Act, courts have generally treated credit reports as "speech" while concluding that consumers' privacy interests are sufficient to outweigh the commercial speech interests of credit reporting bureaus under the *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York*[364] intermediate-scrutiny standard.[365]

Nondisclosure rules (Richards' third category) are also pervasive and range from mandatory duties of confidentiality to trade secret laws to wiretap laws to a wide swath of commercial laws. Although the Supreme Court has consistently upheld the rights of established media to publish private facts even in the face of statutes to the contrary and the tort of nondisclosure, Richards identifies two factors that help explain why the vast majority of nondisclosure rules do not raise any constitutional issues. The first is contract law, which forms the basis for many valid nondisclosure rules, even including those in which one party is a newspaper and the relevant information is a matter of public concern.[366] Second, many nondisclosure rules can be justified as outside the scope of the First Amendment on the grounds that they are generally applicable laws and therefore do not place "a significant burden upon protected, expressive conduct."[367]

Finally, Richards considers direct marketing rules such as commercial speech restrictions on junk mail, telemarketing, and spam. All of these laws undeniably regulate speech and therefore implicate First Amendment interests to a greater extent than do collection, use, or disclosure rules. At the same time, Richards argues that the privacy interests at stake, at least in the telemarketing context, are quite strong.[368] Courts have upheld this interest not only in cases supporting residential privacy,[369] but also in cases challenging marketing restrictions such as

---

carrier's sharing of customer information with third-party marketers. *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 999 (D.C. Cir. 2009). Again applying the *Central Hudson* test, the D.C. Circuit upheld the modified order. *Id.* at 1000–03.

364. 447 U.S. 557 (1980).

365. *See, e.g.*, *id.* at 564–66; *Trans Union Corp. v. FTC*, 245 F.3d 809, 818–19 (D.C. Cir. 2001) (holding that the FCRA's restriction on a consumer reporting agency's sale of targeted marketing lists did not violate the First Amendment); *King v. Gen. Info. Servs.*, 903 F. Supp. 2d 303 (E.D. Pa. 2012) (holding that FCRA's provisions requiring consumer reporting agencies to exclude certain information from consumer reports did not violate the First Amendment); *Individual Reference Servs. Group, Inc. v. FTC*, 145 F. Supp. 2d 6, 40 (D.D.C. 2001), *aff'd sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) (same). *But see Equifax Servs., Inc. v. Cohen*, 420 A.2d 189 (Me. 1980) (invalidating under the First Amendment a state law requiring the consent of a consumer before a firm could request that consumer's credit history).

366. Richards, *supra* note 354, at 1201–04.

367. *Id.* at 1205.

368. *Id.* at 1207–08.

369. *See, e.g.*, *Frisby v. Schultz*, 487 U.S. 474 (1988); *Rowan v. U.S. Post Office Dep't*, 397 U.S. 728 (1970).

the FCC's Do Not Call registry and other telemarketing cases under the Telephone Consumer Protections Act (TCPA).[370] In *Van Bergen v. Minnesota*,[371] the Eighth Circuit reviewed the enforcement of a Minnesota law regulating the use of a device that automatically dialed home phone numbers and delivered a prerecorded message.[372] Although the plaintiff was a gubernatorial candidate and planned to use the device to reach potential voters with a campaign message, the court upheld the law as a content-neutral restriction on all uses of the device.[373] As in *FTC v. Mainstream Marketing Services, Inc.*,[374] and other TCPA cases, the court found that the government had a significant interest in protecting residential privacy, which justified the law.[375] A similar argument may be mounted regarding the constitutionality of regulating campaign data practices and voter microtargeting as part of a general privacy regulation of data brokers and commercial online advertisers.

Recall that Brill's proposal requires data brokers to (1) minimize the data they collect, (2) provide consumers with notice as well as the ability to (3) access and correct some of their information, and (4) opt-out of some marketing uses.[376] Brill also supports (5) a complementary DNT mechanism enabling consumers to prevent companies from tracking them as they navigate the web or from serving them targeted ads.[377] Are any of Brill's five proposed privacy rules problematic from a First Amendment perspective? As to rules one through three, Schwartz would defend them as nonsilencing.[378] Richards would classify them as

---

370. *See FTC v. Mainstream Mktg. Servs., Inc.*, 345 F.3d 850, 854–55 (10th Cir. 2003) (upholding the constitutionality of the Do Not Call registry under *Central Hudson* based partly on the grounds that Congress's declared interest in protecting privacy in the home was sufficiently substantial to justify that regulation), *cert. denied*, 543 U.S. 812 (2004); *see also Missouri v. Am. Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003) (upholding opt-in requirements for unsolicited faxes); *Destination Ventures, Ltd. v. FCC*, 46 F.3d 54 (9th Cir. 1995) (same).

371. 59 F.3d 1541 (8th Cir. 1995).

372. *Id.*

373. *Id.* at 1551.

374. 345 F.3d 850, 854–55 (10th Cir. 2003).

375. *Van Bergen*, 59 F.3d at 1554–55. In *Mainstream Mktg. Servs., Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004), the Tenth Circuit stated that one of the "key aspects" supporting its conclusion that the Do Not Call registry met First Amendment requirements was the fact that it "restricts only core commercial speech." *Id.* at 1233. However, it is a mistake to infer that a DNT provision would also requires a legislative carve-out for political speech. Do Not Call directly regulates communication, i.e., making unsolicited telephone calls that fail to meet certain requirements, whereas DNT only regulates the collection and use of data and does not directly regulate speech. *See infra* text accompanying notes 387–90.

376. *See supra* notes 283–84 and accompanying text.

377. *See supra* notes 283–84 and accompanying text.

378. Schwartz, *supra* note 356, at 1562.

collection or use rules that raise no serious First Amendment issues.[379] A similar analysis applies to rule four. Indeed, numerous federal privacy statutes include opt-out rights,[380] or even more restrictive opt-in rights.[381] And First Amendment challenges of these rules have been largely unsuccessful, with only a few limited exceptions.[382]

Nor does this analysis change merely because political campaigns acquire some of the voter data they rely on from commercial data brokers or utilize third-party tracking cookies to serve targeted ads. The data brokers restrictions in Reclaim Your Name would have *no* impact on voter registration data, donor data, or response data, the three categories of voter data that many commentators consider the most important for voter microtargeting purposes.[383] Rather, these restrictions would only affect consumer data, although granting consumers access and correction rights might benefit political actors by making consumer data more accurate, at least for individuals who exercise these rights. Adverse impacts are likely to occur only if large numbers of consumers opt-out from data brokers sharing their data for marketing purposes. But opt-out rates are generally very low.[384] More to the point, Richards demonstrates that commercial actors are bound by contractual agreements and by generally applicable laws and this includes political actors insofar as they purchase commercial data subject to various contractual or regulatory restrictions.

What about the proposed DNT mechanism? As long as it restricts advertisers and web sites very broadly and prohibits unwanted tracking and targeting with only a few limited exceptions, the courts are likely to treat it as a permissible form of commercial speech regulation. Under the intermediate scrutiny standard for commercial speech as set forth in *Central Hudson*, First Amendment challenges often turn on whether the government has asserted a substantial interest to be achieved by the regulation and if so whether there is a "reasonable fit" between those

379. Richards, *supra* note 354, at 1181–94.

380. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 156 (2013) (listing six federal privacy statutes with opt-out rights).

381. *Id.* (listing eight federal privacy statutes with opt-in rights).

382. *See supra* notes 363–65.

383. *See supra* notes 135–38 and accompanying text.

384. Michael E. Staten & Fred H. Cate, *The Impact* of *Opt-In Privacy Rules on Retail Credit Markets*: *A Case Study of MBNA*, 52 DUKE L.J. 745, 767 (2003) (noting that "less than 10 percent of the U.S. population ever opts out of a mailing list"). There are obvious tensions between the privacy measures described above and fundamental First Amendment values. The more extensively these measures limit data collection, the more likely they are to run afoul of commercial speech standards. This tension is unavoidable in addressing voter privacy issues; it comes with the territory.

interests and the challenged regulation.[385] Much would depend on the specifics of the Reclaim Your Name initiative as enacted into law but Brill's proposal should pass constitutional muster given that it establishes a direct relationship between a widely recognized harm (unauthorized tracking and targeting) and provides a narrow and specific remedy (new data minimization, notice, access, and opt-out requirements on data brokers along with a DNT mechanism).[386] In particular, the proposed requirement would have a relatively small impact on the data collection practices of political campaigns. So far DNT has a low rate of participation,[387] making it unlikely that a high percentage of the electorate would "turn on" this mechanism. Second, the DNT mechanism prohibits only tracking and targeting aimed at consumers who have affirmatively indicated that they do not want to be tracked or targeted and for whom such activity would constitute an invasion of privacy.[388] Third, this mechanism only prevents targeting based on the use of unique online identifiers to track users around the web such as third-party cookies.[389] Even if a potential voter turns on this mechanism, a campaign may still send targeted ads to him or her as long as the targeting uses other voter data, including the voter registration and response data that

385. The four-part intermediate scrutiny test articulated in *Central Hudson* holds that a government restriction on commercial speech must (1) concern lawful activity, (2) not be misleading, and (3) directly advance a substantial government interest that is not (4) "more extensive than is necessary to serve the interest." *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 564–66 (1980). Later cases have emphasized the need for "a reasonable fit between the means and the end of the regulatory scheme" and the government's need to carefully calculate "the costs and benefits associated with the burden on speech imposed" by the regulation. *See, e.g.*, *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 561 (2001) (quoting *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993)).

386. *See* Brill, *supra* note 281.

387. One ad network estimates that about eight percent of users across all browsers are transmitting a DNT signal, thereby indicating a preference not to be tracked. *See* Joe Newman, *Tracking Do Not Track: New Ad Network Data Shows that 8 Percent of Users Have DNT On*, FUTURE OF PRIVACY FORUM (Dec. 18, 2013), http://www.futureofprivacy.org/2013/12/18/. Other estimates are higher. *See* Alex Fowler, *Mozilla's New Do Not Track Dashboard: Firefox Users Continue to Seek Out and Enable DNT*, MOZILLA PRIVACY BLOG (May 3, 2013), https://blog.mozilla.org/privacy/2013/05/03/mozillas-new-do-not-track-dashboard-firefox-users-continue-to-seek-out-and-enable-dnt/ (stating that "approximately 17 percent" of U.S. users of Mozilla's Firefox browser have adopted DNT).

388. *See Mainstream Mktg. Servs., Inc. vs. FTC*, 358 F.3d 1228, 1242 (10th Cir. 2004) (making a similar point regarding the Do Not Call registry).

389. A DNT mechanism might interfere with targeted political ads in either of two ways: first, it might prevent the campaign from using consumer data collected via third-party cookies; second, it would limit the reach of partnership agreements premised on matching voter files with cookie-based profiles as described above. *Supra* notes 80–85 and accompanying text.

many argue is more effective for accurate targeting. Fourth, this mechanism has no impact on other forms of campaign communications, including both web-based contextual and display ads as well as traditional TV and radio ads, which still account for the vast majority of campaign media buys.[390] Finally, and most importantly, DNT is not a direct prohibition on speech. Rather, it is a narrowly tailored regulation that, depending on how it is implemented, would present both advertisers and consumers with a number of different options for sending and receiving ads, restricting some avenues of communication but not others.[391]

b. Does Sorrell *Bar New Commercial Privacy Regulations?*

Although direct marketing restrictions raise more serious First Amendment concerns than collection, use, or disclosure rules, they still pass muster under existing commercial speech tests. A recent decision threatens to upend this conclusion and possibly wreak havoc for privacy regulation generally. In *Sorrell v. IMS Health, Inc.*, the Court struck down a Vermont law restricting the transfer and use for marketing purposes of pharmacy records containing information on the prescribing habits of physicians, unless the physician expressly consents to the transfer.[392] Pharmacies maintain detailed records of their customers' prescription information, including the prescribing doctor's name and the patient's age, gender, and health condition.[393] Many pharmacies sell this information to data-mining firms, which append additional information about doctors to produce reports on prescribing behavior for manufacturers of brand-name drugs.[394] The manufacturers then use the reports to promote their drugs to targeted physicians through a process called "detailing."[395]

The Vermont law, known as Act 80, prohibited pharmacies and other entities from selling "prescriber-identifying information" (P-II) or allowing the use of such information for marketing unless the prescribing physician consents, while also barring pharmaceutical manufacturers or marketers from using this information for marketing without the

390. Katy Bachman, *Forecast: Online Political Ad Spend Still Tiny*, ADWEEK (Mar. 8, 2012), http://www.adweek.com/news/online/forecast-online-political-still-tiny-138810 (forecasting that online political advertising will capture only $159 million, or 1.5 percent of the estimated $9.8 billion total ad spend in 2012).

391. *Mainstream Mktg.*, 358 F.3d at 1243–44.

392. 131 S. Ct. 2653, 2672 (2011).

393. David Orentlicher, *Prescription Data Mining and the Protection of Patients' Interests*, 38 J.L. MED. & ETHICS 74, 75 (2010).

394. *Id.* at 74.

395. *Id.* at 74–75.

prescriber's consent.[396] These prohibitions on sale, disclosure, and use of P-II for marketing purposes were subject to numerous exceptions allowing the transfer and use of P-II for health care research, patient care management and education, law enforcement, and other non-commercial purposes.[397] Vermont's goal in enacting this law was to reduce the overall cost of healthcare and curb the use of brand name prescription drugs by ensuring that physicians receive unbiased information.[398] Vermont sought to achieve multiple state policy objectives including preserving physicians' privacy, improving public heath, and cost containment.[399]

In his majority opinion in *Sorrell*, Justice Kennedy quickly sounded the death knell of Act 80 by noting that it enacts both content-based and viewpoint-based restrictions and thereby "burdens disfavored speech by disfavored speakers."[400] As a consequence, the intermediate scrutiny standard developed in *Central Hudson* fails to protect the pharmaceutical manufacturer's speech rights.[401] Rather, "heightened scrutiny" applies to Act 80 because the state created a speech regulation due to disagreement with the message it conveys.[402] Although Vermont offered several arguments for why this higher standard was unwarranted, the Court flatly rejected them.

Ultimately, the Court concluded that even if it were to rely on commercial speech standards, the state failed to show that section 4631(d) advanced a substantial government interest or that the measure was drawn to achieve that interest.[403] In particular, the Court found that section 4631(d) did not advance the privacy interests of prescribing physicians because it allowed the wide dissemination and use of P-II for myriad purposes other than marketing.[404] Interestingly, the Court noted that Vermont might have advanced its asserted privacy interest by allowing the sale or disclosure of P-II "in only a few narrow and well-justified circumstances" (as is the case, for example, with Health Insurance Portability and Accountability Act of 1996 (HIPAA)).[405] But

396. *See* VT. STAT. ANN. tit. 18, § 4631(d) (2007). This sub-section is quoted in full in *Sorrell*, 131 S. Ct. at 2660.

397. *Sorrell*, 131 S. Ct. at 2660.

398. *Id.* at 2661.

399. *Id.* at 2668.

400. *Id.* at 2663–64.

401. *Id.* at 2666–72.

402. *Id.* at 2664 (citing *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)).

403. *Id.* at 2667–68.

404. *Id.* at 2668.

405. *Id.*

as the Court made clear, Vermont did not do this.[406] The Court also rejected Vermont's claim that the law advanced important public policy goals of cost containment and promoting public health.[407] While acknowledging that these goals were proper, Vermont "[did] not advance them in a permissible way."[408] Rather, it sought to diminish the influence of detailers whose use of P-II was "too persuasive" in promoting brand-name drugs.[409] Although the state could oppose these views through its own speech, it may not "burden the speech of others in order to tilt public debate in a preferred direction."[410] Accordingly, the Court found that Act 80 violated the First Amendment.[411]

Sorrell sent a shockwave through the privacy community and for good reason. If the Supreme Court were to begin applying heightened scrutiny to all laws restricting the disclosure or use of personal information for marketing purposes, then many longstanding and uncontroversial privacy laws would be imperiled,[412] along with a number of proposed rules including DNT.[413] And yet there are sound reasons for rejecting a doomsday reading of *Sorrell* and interpreting it more narrowly and cautiously. To begin with, many extant data privacy laws do a better job of identifying and advancing privacy interests than Act 80 did.[414] For example, federal privacy statutes addressing credit reports, educational records, cable TV records, video rental records, medical records, and children's information, respectively, all follow the Court's preferred model of restricting use and disclosure except in a few "narrow circumstances."[415] Second, unlike the Vermont law, these and other privacy statutes are content-, speaker-, and viewpoint-neutral. While seeking to protect privacy or confidentiality interests of users in specific

406. *Id.*

407. *Id.* at 2670.

408. *Id.*

409. *Id.* at 2671.

410. *Id.*

411. *Id.* at 2672.

412. *See id.* at 2685 (Breyer, J., dissenting) (noting that the majority opinion threatens to open "a Pandora's Box of First Amendment challenges to many ordinary regulatory practices that may only incidentally affect a commercial message").

413. *See* Thomas R. Julin, Sorrell v. IMS Health *May Doom Federal Do Not Track Acts*, 10 PRIVACY & SEC. L. REP. (BNA) No. 35, at 6 (2011), *available at* http://www.hunton.com/files/Publication/86a85a32-bb2d-4176-8683-7e985093cb2f/Presentation/PublicationAttachment/be10be7a-b942-494d-8463-865e505fd7f6/Julin_BNA_Federal_Do_Not_Track_Acts.pdf.

414. *Sorrell*, 131 S. Ct. at 2668; *see* Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 36 VT. L. REV. 931, 966–68 (2012) (observing that since there is support for recognizing a patient's constitutional right to privacy in medical information, Vermont's law might have fared better if it had protected both patient's and prescriber's privacy interests).

415. *Sorrell*, 131 S. Ct. at 2672; Julin, *supra* note 413, at 3 n.15.

settings, they avoid taking sides in ongoing policy debates by favoring speech that the government prefers or disfavoring speech that it opposes. While conceding that opt-in provisions in the hands of private decision makers avoid government partiality and therefore insulate a privacy law from First Amendment challenge, the Court rejected that argument here because the state conditioned privacy protection on physicians' acquiescence "in the State's goal of burdening disfavored speech by disfavored speakers."[416] Third, even though the majority opinion in *Sorrell* seemingly rejected intermediate scrutiny as the appropriate standard for commercial speech, it ultimately resolved the case by demonstrating the Vermont law fails the *Central Hudson* test. This is important because, as Schwartz and Richards both argue, privacy laws (including direct marketing rules) generally prevail under traditional commercial speech standards.

Fourth, despite dicta in Justice Kennedy's opinion indicating that "data is speech" for First Amendment purposes, and thereby suggesting to some commentators that all privacy laws are suspect, the holding in *Sorrell* does not rely on this theory, which has its share of detractors and supporters.[417] Indeed, Justice Kennedy suggests that if Vermont had addressed physician confidentiality through "a more coherent policy" along the lines of HIPAA, the law would have been constitutional.[418] Finally, despite the popular impression that *Sorrell* strikes a devastating

---

416. *Sorrell*, 131 S. Ct. at 2669 (explaining that the opt-in provision "may offer a limited degree of privacy, but only on terms favorable to the speech the State prefers").

417. In dicta, Justice Kennedy states:

> This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment . . . . Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.

Sorrell, 131 S. Ct. at 2667. For articles suggesting that facts are speech deserving full First Amendment protection under the strict scrutiny standard, see Jane R. Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 57 (2014), and Ashutosh Bhagwat, Sorrell v. IMS Health: *Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 875–76 (2012). For articles offering a narrow reading of *Sorrell*, see Agatha M. Coles, *Internet Advertising After* Sorrell v. IMS Health: *A Discussion on Data Privacy & the First Amendment*, 30 CARDOZO ARTS & ENT. L.J. 283, 305 (2012); Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, WM. & MARY L. REV. 2 (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335196; Smith, *supra* note 414.

418. *Sorrell*, 131 S. Ct. at 2668 (quoting *Greater New Orleans Broad. Ass'n, Inc. v. United States*, 527 U.S. 173, 195 (1999)). As both Bhagwat and Smith point out, if HIPAA—which is probably the most comprehensive and rigorous of U.S. privacy statutes—is narrowly drawn, then other privacy laws are not in any danger. Bhagwat, *supra* note 417; Smith, *supra* note 414, at 994.

blow against privacy, the majority opinion concludes by strongly embracing it. As Justice Kennedy puts it:

> The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure . . . [p]rivacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers.[419]

The preceding analysis implies that privacy laws restricting the sale and marketing use of personal information may survive even heightened scrutiny under *Sorrell* provided they (1) avoid content or viewpoint discrimination by not singling out particular uses or particular groups as being subject to certain restrictions while exempting others or otherwise tilting the public debate, (2) identify a substantial government interest, and (3) use narrowly tailored means to protect privacy.[420] Brill's proposal meets these requirements without difficulty. Neither the data broker nor the DNT components of Reclaim Your Name involve any content or viewpoint discrimination.[421] Both components serve the substantive state interest of preventing data brokers and online advertisers from taking advantage of consumers without their permission. And both components are narrowly tailored to achieve these goals. Indeed, even if Reclaim Your Name was successful at overcoming consumer inertia and a significant percentage of consumers opted-out of targeted marketing or took steps to prevent tracking and targeting, this would limit the flow of *consumer data* to political actors while having no impact on the availability of *voter data* or volunteered *response data*, which many commentators consider more essential for voter microtargeting purposes in any case. Nor does the proposed law have any impact on non-targeted ads including broad media buys or generic messaging to supporters and potential supporters.

---

419. *Sorrell*, 131 S. Ct. at 2672.

420. *See, e.g.*, Coles, *supra* note 417, at 309; Smith, *supra* note 414, at 989–93.

421. *See King v. Gen. Info. Servs., Inc*., 903 F. Supp. 2d 303, 313 (2012) ("GIS's eager attempt to color section 1681c with the same flaws of the Vermont statute in *Sorrell* is misplaced. As previously noted, section 1681c was not enacted in order to tilt the public debate in a preferred direction or to simply favor one speaker over the other. Congress' decision to single out consumer reporting agencies was explicitly based on their unique impact on American commerce and personal privacy. Through a coherent policy that has been justified on such neutral grounds, this Court finds section 1681c to sufficiently comport with First Amendment standards.").

CONCLUSION

Data-driven campaigning helps modern political candidates mobilize supporters and donors using voter microtargeting techniques that identify the most persuadable voters while paying far less attention to the rest of the electorate. These techniques promise to engage high value voters and increase their political participation by delivering more relevant campaign messages that appeal directly to their most pressing concerns. At the same time, unbeknownst to most citizens, and certainly without their informed consent, presidential candidates, the major parties, and a cadre of data consultants have amassed huge political dossiers on every American voter, which are subject to few if any privacy regulations.

This Article has described campaign data practices and voter microtargeting in considerable detail and how they potentially jeopardize voters' information and political privacy interests and harm the democratic process. It has offered a modest proposal for addressing these harms through greater transparency and a few familiar restrictions on commercial data practices. And it has argued that this proposal will be effective only if (1) the transparency measures are politically salient (i.e., help voters decide whom to vote for) and (2) harmonize with new federal privacy restrictions on commercial data brokers, which (3) should include a DNT mechanism empowering individuals (and hence voters) to decide whether and to what extent commercial firms may track or target them. Finally, this Article has analyzed the First Amendment concerns associated with the proposed solution and, relying on the campaign finance cases and well-established First Amendment doctrines, has demonstrated how these concerns may be overcome.

A pessimist might respond to this modest proposal with despair. After all, despite being modest, it stands almost no chance of becoming law for a simple reason: elected officials have a weak track record on restricting any campaign techniques that helped them get elected. Despair not. Nothing prevents the relevant political actors from voluntarily adopting both parts of the modest proposal. And a powerful incentive for doing so is ready at hand: the very same desire to win elections. Over time, data-driven campaigns will become more transparent about their collection and transfer of voter data and use of microtargeting techniques, and they will adopt best practices for protecting voter data, at pains of facing the nightmare scenario of a major data breach or privacy gaffe that derails an election bid. So the same calculus that makes data-driven campaigning politically irresistible should eventually lead candidates to develop a more privacy-protective approach to voter data even if solely for self-interested purposes.