Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 25, *Issue* 4 2015 *Article* 3

VOLUME XXV BOOK 4

Cracking the One-Way Mirror: How Computational Politics Harms Voter Privacy, and Proposed Regulatory Solutions

Kwame N. Akosah*

*Fordham University School of Law

Cracking the One-Way Mirror: How Computational Politics Harms Voter Privacy, and Proposed Regulatory Solutions

Kwame N. Akosah*

* J.D., Fordham University School of Law, 2015; B.A., Political Science, University of California Los Angeles, 2010. I would like to thank Prof. Olivier Sylvain for his guidance and support while advising me on this Note, and to Kate Patton, Max Shapnik, Stephen Dixon, and the rest of the *IPLJ* staff for their hard work and thorough editing. For their support throughout my academic and professional endeavors, thank you to Prof. Robin Lenhardt, Prof. Zephyr Teachout, Prof. Elizabeth Cooper, Dora Galacatos, Hillary Exter, Bonda Lee-Cunningham, Henry Berger, Jerry Goldfeder, Lawrence Mandelker, Daniel Weiner, John Kowal, Julie Ebenstein and Michelle Rupp. Most importantly, thanks mom and dad for loving me and helping make my dreams come true.

INTRODUCTION

In June 1972, Chile's democratically elected leader, Salvador Allende, hired the British cyberneticist, Stafford Beer, to bring Chile into the computer age.[1] Beer proposed "Project Cyberfolk," a cybernetic system that would further popular participation and democracy by allowing citizens to communicate their feelings directly to the government.[2] Beer built a device that would allow citizens to adjust a pointer on a voltmeter-like dial in order to indicate moods ranging from extreme unhappiness to complete bliss.[3] The

---

[1] Evgeny Morozov, *The Planning Machine Project Cybersyn and the Origins of the Big Data Nation*, THE NEW YORKER (Oct. 13, 2014), http://www.newyorker.com/magazine/2014/10/13/planning-machine.

[2] "Project Cyberfolk consisted of a relatively simple technological system that would function within a complex social system with the aim of improving its management .... Beer proposed building several [algedonic] meters and using them to conduct experiments on how technology could further popular participation and democracy." *See* EDEN MEDINA, CYBERNETIC REVOLUTIONARIES: TECHNOLOGY AND POLITICS IN ALLENDE'S CHILE 81–92 (2011).

[3] Morozov, *supra* note 1.

device would record a citizen's happiness—ideally during a live television broadcast featuring some proposed new political policy—and electronically send the data directly to the government for real-time aggregation and review.[4] Beer theorized that his system would improve public well-being and bring homeostatic stability between government and constituent.[5]

Beer's dream would not be realized.[6] However, despite his optimism, it is easy to see how such a device could be misused by the government or partisan groups.[7] In particular, the stark data-asymmetry between constituent and government places all the power of data in the hands of the government without transparency and accountability to the citizens producing the data. Citizens would be unable to know how their data is processed or aggregated, nor would the government be obligated to reveal what a citizen's data reveals compared to historical trends. The data could even be used to identify and persecute political dissidents based on the views born out of their data. Beer did anticipate these problems, and he designed safeguards into the system in order to foster visibility and transparency and ensure the process remained analog to keep a citizen's meter anonymous.[8]

Today, political consultants, technologists, and entrepreneurs are all helping American politicians effect even larger data-asymmetries by gathering data on citizens through more advanced tools of monitoring and persuasion, and with even fewer safeguards. With these data services,[9] campaigns have access to massive electronic databases containing information gleaned and purchased from public and private sources on nearly every voter in the

---

4 *Id.*

5 *Id.*

6 "Beer commissioned several prototype meters and used them in small group experiments. They were never implemented as the form of real-time, adaptive political communication that Beer imagined." MEDINA, *supra* note 2, at 92.

7 "Despite Beer's good intentions, it is easy to imagine how a government might abuse such a device or how partisan groups might manipulate them to suit their interests." *Id.* at 91.

8 "Beer recognized that the meters, like the telephone voting systems already in existence at the time, brought with them the potential for political oppression … [He] insisted that the devices be analog, not digital, which would make it more difficult to identify individual meters and, by extension, individual users." *Id.*

9 *See infra* Parts I.A–C.

United States.[10] The public data, in part, is composed of lists of registered voters and can be obtained from official voter lists and records maintained by states.[11] The private data is more emblematic of "Big Data," encompassing a galaxy of information purchased from data brokers and revealing a limitless range of consumer habits including magazine subscription records, credit histories, and even grocery "club card" purchases.[12] With all this data, campaigns can use powerful analytic tools to distill myriad disjointed and seemingly innocuous data points into an individualized voter profile that reveals intimate details about a voter's life and behavior.[13] These profiles allow campaigns to craft messages individually tailored to a voter's attitudes or ideology as well as economize campaign resources by focusing only on "persuadables."[14]

Most citizens, as they engage in their roles as consumers and voters, do not appreciate the degree to which their data is freely traded in data markets. As a matter of law, when an individual freely discloses their data to a third party, online or offline, there is no reasonable expectation that the data can be kept private[15] (barring certain types of data protected by federal statute).[16] Very few people are aware that their data is being shipped off and aggregated in data warehouses where it is organized, stored, and analyzed.[17] This is partly due to the passive role users play in micro-targeting practices, which for the most part are surreptitious by design. For

---

[10] Chris Evans, *It's the Autonomy, Stupid: Political Data-Mining and Voter Privacy in the Information Age*, 13 MINN. J.L. SCI. & TECH. 867, 867–68 (2012).

[11] *See infra* Part I.C.

[12] "An everyday example of data gathering occurs at supermarkets, which use information they obtain from customer loyalty cards to send consumers targeted coupons and advertisements." Preston N. Thomas, *Little Brother's Big Book: The Case for a Right of Audit in Private Databases*, 18 COMMLAW CONSPECTUS 155, 158 (2009); *see also* Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data*, 64 STAN. L. REV. ONLINE 70, 71 (2012).

[13] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

[14] *See* Kreiss, *supra* note 12.

[15] Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477, 528 (2006) (explaining the third-party doctrine); *see also* Evans, *supra* note 10, at 879 ("The parties to a financial transaction are said to equally own the facts to the transaction.").

[16] *See* Evans, *supra* note 10.

[17] Helen Nissenbaum, *Privacy As Contextual Integrity*, 79 WASH. L. REV. 119, 121 (2004).

example, a practice known as "cookie matching" allows marketers to serve advertising to users based on data aggregated by actors not present at the initial transaction that generated the data.[18] Given the surreptitious and unexpected nature of micro-targeting trends like cookie matching and more,[19] voters lack the notice necessary to exercise autonomy over their data held in the private databases of political data companies. With more autonomy, voters can minimize privacy and democracy harms associated with political data practices, like the data's capacity to socially engineer voters in unfair or impermissible ways,[20] the potential political chilling effect caused by unaccountable, imperceptible, and pervasive surveillance,[21] and the power imbalances perpetuated by unregulated "black box" algorithms.[22]

All of this matters because political campaigns are increasingly interacting with voters based on data and shaping the nature of that interaction based on what the data reveals.[23] Much of this data is proprietary and unregulated,[24] which prevents voters from knowing what their would-be elected officials know about them or how they have used their data to surreptitiously influence and persuade them. Without knowledge of or autonomy over data, voters are increasingly at the mercy of a "one-way mirror"[25] that scrutinizes intimate details about their lives, judges them on that basis, and surreptitiously influences their behavior. Given the essential role the right to vote plays in ensuring our government serves its people, it is necessary to understand the ways in which a loss of informational autonomy can harm voters when they exercise that essential right, and explore ways to mitigate that harm.

This Note will argue that, when voters lose informational autonomy, democratic harms can result. It will examine the legal ba-

---

18 Evans, *supra* note 10, at 879.

19 *See infra* Part I.C.

20 *See infra* Part II.C.

21 *Id.*

22 *See infra* Part II.C.3.

23 *See, e.g.*, Ryan Cooper, *How Big Data Sucked the Soul Out of Democratic Politics,* THE WEEK (Nov. 6, 2014) http://theweek.com/article/index/271411/how-big-data-sucked-the-soul-out-of-democratic-politics.

24 *See* FRANK PASQUALE, THE BLACK BOX SOCIETY 3, 193 (2015).

25 I borrow the term "one-way mirror" from Frank Pasquale. *Id.* at 9.

sis for federal and state regulation and will discuss legislative or regulatory options at the federal and state level. Part I will provide additional context about political data practices, describe the organizations that track it, and examine where the data comes from. Part II will discuss the theoretical underpinnings behind informational autonomy and discuss the various ways Big Data political trackers can harm normative conceptions of privacy and democracy. Part III will discuss challenges to reforming political data practices and explain why regulation is necessary. Part IV will examine various federal and state regulatory reforms and provide a legal basis for federal and state regulation.

I. BACKGROUND

A. Computational Politics

Given the promise of effective insights into voter behavior, it is no wonder that campaigns are availing themselves of larger and more diverse datasets. A famous example of this trend is the Obama campaign's Facebook app, "Obama 2012 - Are You In?" At the height of the campaign the app boasted 23 million unique users. Each user gave up personal information like his or her name, gender, birthday, current city, religion, and political views as well as shared their list of friends, the information they shared with friends, and the information those friends shared on Facebook.[26] The data was used to improve voter communication in every facet of the campaign, from individually crafted online display advertising to personalized appeals used for offline get-out-the-vote (GOTV) operations like signing up volunteers, knocking on doors, phone banking, and identifying likely voters.[27] With so much data the campaign was able to engage previously untapped voters and expand Democratic political participation.[28]

---

[26] Micah Sifry, *How Obama's Data-Crunching Prowess May Get Him Re-Elected,* CNN (Oct. 9, 2011), http://www.cnn.com/2011/10/09/tech/innovation/obama-data-crunching-election/.

[27] *Id.*

[28] Kreiss, s*upra* note 12, at 74; John McCormick, *Democrats Keep Voter Registration Lead in 4 Key States*, BLOOMBERG (Oct. 9, 2012), http://www.bloomberg.com/news/2012-10-10/democrats-keep-voter-registration-lead-in-4-battleground-states.html.

A more recent example would be the Koch Brothers-backed political data firm, i360.[29] i360 has spent 50 million dollars to link lists of registered voters with consumer data purchased from credit bureaus, information from social networks, estimated income, recent addresses, voter history, the brand of car a voter drives, and his or her TV viewing habits.[30] This was in order to help campaigns target ads more precisely and cost effectively.[31] A number of Republican Senate and gubernatorial candidates that were victorious during the 2014 elections count themselves among i360's clients, including Tom Cotton, Joni Ernst, and Larry Hogan.[32]

Indeed, electronically stored data used for political purposes is nothing new. Political parties have for decades legally maintained membership lists and voter management databases used in every facet of a campaign, including fundraising, GOTV operations, recruitment of volunteers, and the tracking of issues across key geographic and demographic constituencies.[33] It should also come as no surprise that political campaigns are in the advertising and marketing business and that the ties between consumer data brokers,[34] parties, and campaigns run deep.[35] Even Acxiom, the country's largest consumer data broker, began in 1969 as a data processing

---

[29] i360, http://www.i-360.com/ (last visited Dec. 19, 2014).

[30] Mike Allen & Kenneth P. Vogel *Inside the Koch Data Mine*, POLITICO (Dec. 8, 2014), http://www.politico.com/story/2014/12/koch-brothers-rnc-113359.html.

[31] *Id.*

[32] *Id.*

[33] Colin Bennett, *The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies*, 18(8) FIRST MONDAY (Aug. 5, 2013), *available at* http://uncommonculture.org/ojs/index.php/fm/article/view/4789/3730.

[34] "Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud." FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC REPORT].

[35] "We also know that U.S. parties make extensive use of commercial marketing databases. Thus the political data on party affiliation and behavior is combined with other data on activities, interests and purchasing habits available from data brokerage firms such as Acxiom, Dun and Bradstreet, InfoUSA and aristotle.com." Bennett, s*upra* note 33.

company for the Democratic party.[36] What has changed in recent years is that campaigns are now utilizing advancements in data tracking and storage to find novel ways to combine diverse digital datasets and use statistics and other data mining techniques to extract hidden information and surprising correlations.[37] This trend was precipitated by the exponential decrease in the cost for storing, managing, and analyzing large diverse sets of data.[38]

This phenomenon is called "computational politics," and it refers to the application of computational methods to large datasets derived from online and offline data sources for conducting outreach, persuasion, and mobilization in the service of electing, furthering, or opposing a candidate, policy, or legislation.[39] For example, as a forerunner in this area,[40] the 2012 Obama campaign developed a "likelihood of turnout" index based on public and private datasets including consumer data on a massive nationwide scale.[41] The index was a number generated between 0 (not going to vote) to 100 (will certainly vote) for each potential voter.[42] This number was appended to every voter, and served as a simple and efficient heuristic for campaign staffers to target the right voters at the right time in their online and offline GOTV efforts.[43] The index also allowed the campaign to dive deep into parts of the country thought

---

[36] Natasha Singer*, Mapping, and Sharing, the Consumer Genome,* N.Y. TIMES, June 16, 2012, http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

[37] "Big Data … may be understood as a more powerful form of data mining that relies on huge volumes of data, faster computers, and new analytic techniques to discover hidden and surprising correlations." Ira S. Rubenstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INTERNATIONAL DATA PRIVACY LAW 74 (2013).

[38] David W. Nickerson & Todd Rogers, *Political Campaigns and Big Data* 2 (Harvard Kennedy Sch. Working Paper Series, No. RWP13-045, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354474.

[39] Zeynep Tufekci, *Engineering the Public: Big Data, Surveillance and Computational Politics*, 19(7) FIRST MONDAY (July 7, 2014), *available at* http://dx.doi.org/10.5210/fm.v19i7.4901.

[40] Sasha Issenberg, *How President Obama's Campaign Used Big Data to Rally Individual Voters,* MIT TECH. REV. (Dec. 19, 2012), http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters/.

[41] Tufekci, *supra* note 39.

[42] *Id.*

[43] *Id.*

to be Republican enclaves, and pick off individual voters never before targeted by Democrats.[44]

B. Political Data Firms

A popular narrative after the 2012 elections was that Democrats won the election with good data,[45] and the GOP lost because of bad data.[46] In the intervening years there has been a land rush of partisan and non-partisan political firms incorporating sophisticated voter data services into their suite of campaign products.[47] Products like mobile applications allow canvassers to access data in real time and generate relevant lists for telephone marketing, email marketing, and door-to-door canvassing.[48] These firms develop these products in order to vie for the business of campaigns and candidates. Because these firms are proprietary about their data and computational practices, it is difficult to know how much they really know about American voters beyond what they choose to reveal in press releases and promotional material. However, what

---

[44] *Id.*

[45] *See* Issenberg *supra* note 40; Dan Balz, *How the Obama Campaign Won the Race for Voter Data*, WASH. POST, July, 28 2013, http://www.washingtonpost.com/politics/how-the-obama-campaign-won-the-race-for-voter-data/2013/07/28/ad32c7b4-ee4e-11e2-a1f9-ea873b7e0424_story.html; Andrew Lampitt, *The Real Story of How Big Data Analytics Helped Obama Win,* INFOWORLD (Feb. 14, 2014), http://www.infoworld.com/article/2613587/big-data/the-real-story-of-how-big-data-analytics-helped-obama-win.html.

[46] The Republican party voiced concerns about their 2012 data operations in the so-called "GOP Autopsy Report," stating: "To win campaigns, the GOP needs better data, better access to data, and better tools to make the most of that data. Although the RNC has always made significant investment in data, there is significant remaining work to do to ensure that our data is the best it can be." REPUBLICAN NAT'L COMM., GROWTH & OPPORTUNITY PROJECT 28 (2013), *available at* http://growthopp.gop.com/RNC_Growth_Opportunity_Book_2013.pdf; *see also* Kenneth P. Vogel & Maggie Haberman, *Karl Rove, Koch Brothers Lead Charge to Control Republican Data*, POLITICO (Apr. 22, 2013), http://www.politico.com/story/2013/04/karl-rove-koch-brothers-control-republican-data-90385.html.

[47] NGP VAN is a progressive service offering Data Analytics, Voter File Management, Volunteer Management, RoboCalls, and RoboSurveys. *See* NGP VAN, http://www.ngpvan.com/ (last visited Dec. 19, 2014). NationBuilder is a non-partisan campaign platform that offers voter data, website management, and campaign finance compliance services. *See* NATIONBUILDER, http://nationbuilder.com/ (last visited Dec. 19, 2014); VoterGravity is a conservative service that offers mobile apps for door-to-door canvassing, phone banking software, and preloaded voter files. *See Features*, VOTER GRAVITY, http://votergravity.com/features/ (last visited Dec. 19, 2014).

[48] *See* Bennett, *supra* note 33.

little is known still paints a picture of widespread and pervasive voter tracking across a diverse set of data.

i360, rVotes, and Voter Gravity are three notable conservative-facing companies that offer campaign software and voter data services. According to its website, i360 operates a database of "190+ million active voters and 250+ million U.S. consumers" and can offer a campaign "hundreds of data points on every American adult that is currently or potentially politically active."[49] rVotes boasts a "Unified Voter Database" that contains a "voters' position on the issues, their voting history [and] their current contact information."[50] Voter Gravity offers an "Integrated Solution" that "integrates mobile technology and a web-based phone system through one interface" with "an extensive database of every U.S. voter with key data points, real time access to data collected and a user-friendly dashboard that helps you turn information into votes."[51]

NGP VAN and Catalist are well known as the de facto data services for Democrats.[52] NGP VAN offers field campaign software and voter files used by the Obama campaign, with accurate 50-state voter files appended with sets of consumer data for "the most sophisticated targeting."[53] Catalist offers data analytics that give campaigns insight into voters "such as relative likelihood to turn out to vote [and] likelihood to be married or have a college degree, to name just a few."[54]

As for nonpartisan firms, Aristotle Inc. has proven to be one of the most dominant.[55] According to its website, Aristotle "provides

---

[49] I360, http://www.i-360.com/ (last visited Dec. 19, 2014).

[50] RVOTES, http://www.rvotes.com/?p=931 (last visited Dec. 19, 2014).

[51] *Features*, VOTER GRAVITY, http://votergravity.com/features/ (last visited Dec. 19, 2014).

[52] "Democrats built their voter data advantage partly because their data is more centralized. A few well-connected firms like Catalist and NGP VAN have earned de facto endorsements from the Democratic establishment and used those blessings to build near monopolies on the left. As a result, Democratic candidates and liberal interest groups have benefited from enhancing and sharing the same data through the same interfaces." *See* Vogel & Haberman, *supra* note 46.

[53] *SmartVAN*, NGP VAN, http://www.ngpvan.com/smartvan (last visited Dec. 19, 2014).

[54] *Products*, CATALIST, http://www.catalist.us/product (last visited Dec. 19, 2014).

[55] "[M]ost … candidates employ some data-mining firm that learned its business in part from Aristotle, which has served as a consultant for every president since Ronald

high-quality political data for political organizations, campaigns, consultants and governmental agencies worldwide."[56] Aristotle has an ever-growing database of more than 190 million voters. Its CEO John Phillips touts the more than 500 attributes his company tracks on each voter—"such as interests and charitable causes, educational level, homeowner/renter, estimated income or presence of children in the household."[57]

All of these firms operate on a longstanding principle of campaigning: identify and mobilize voters that are likely to vote for your candidate, and avoid wasting time on the rest.[58] Increasingly, campaigns are using political data firms in order to harness massive datasets of information on individual voters in order to micro-target on the individual level. In the past, campaigns had to rely on demographic proxies for persuadability like "race, union membership, residential geography, and voter registration" information.[59] Now, services like Aristotle can dive deeper and sort voters by utilizing hundreds of data points that help boost the signal of individual "persuadables" submerged in larger demographic groups.[60] Instead of simply targeting "women voters" or "minority voters," campaigns have enough data to accurately profile the libertarian white male in Cobb County, Georgia, or the socially conservative

---

Reagan …. In the 2006 elections, Aristotle sold information to more than 200 candidates for the House of Representatives (even its Republicans had an astounding win record), a good portion of those running for Senate, and candidates for governor from California to Florida, to New York." James Verini, *Big Brother Inc.,* VANITY FAIR, Dec. 13, 2007, http://www.vanityfair.com/politics/features/2007/12/aristotle200712.

[56] *Accurate and Up-To-Date Voter Lists Covering U.S. and Abroad*, ARISTOTLE, http://aristotle.com/political-data/ (last visited Dec. 19, 2014).

[57] David Zax, *Football Fans Vote Republican: Hardcore Data Miners Track 'Neo Tribes' with 'Micro-Targeting,'* FAST COMPANY (Jan. 11, 2012), http://www.fastcompany.com/1807087/football-fans-vote-republican-hardcore-data-miners-track-neo-tribes-micro-targeting.

[58] "The goal of mining for data is not to figure out who is important in your district. It is actually about figuring who not to spend any time with. The major source of waste in a political campaign is to try to communicate with people you know are not going to vote for you." Philip Howard & Kris Erickson, *Data Collection and Leakage*, 84 CHI.-KENT L. REV. 737, 738 (2010); It is a tactic common among all marketers—political or otherwise—to identify individuals as a "targets" or "waste." *See* Joseph Turow, THE DAILY YOU 7 (2011).

[59] Michael S. Kang, *From Broadcasting to Narrowcasting: The Emerging Challenge for Campaign Finance Law*, 73 GEO. WASH. L. REV. 1070, 1078 (2005).

[60] *Id.*

African-American in Chicago, and tailor a campaign message directly to them.[61]

C. The Sources of Data

Computational politics requires accurate and current lists of registered voters from each state's voter database. States are mandated under the Help America Vote Act (HAVA) to maintain state-wide computerized voter registration databases, along with uniform procedures for processing registration data.[62] When citizens register to vote, most registration forms require a name, address, birth date, phone number, and party affiliation, among other things.[63] Publicly available records of individual voting history are also maintained by states.[64] State "sunshine"[65] laws mandate disclosure of most public records barring exemptions similar to the Freedom of Information Act (FOIA).[66] As a result, states—as a matter of course—sell voter records and registration lists to political parties and candidates as well as non-partisan political data firms.[67]

---

[61] *Id.*

[62] SASHA ISSENBERG, THE VICTORY LAB 245 (2012).

[63] Kim Zetter, *Mining the Vein of Voter Rolls*, WIRED (DEC. 11, 2003), http://archive.wired.com/techbiz/media/news/2003/12/61507. "All states require voters to provide their name, address and signature; Every state but one requires voters to provide their date of birth; 46 states ask voters to provide their phone number; 34 states ask voters to declare their gender; 30 states ask voters to provide all or part of their Social Security number; 27 states require voters to select a party affiliation; 14 states ask voters to provide their place of birth; Eleven states ask voters for their drivers' license number; Nine states ask voters to declare their race; Four states ask voters if they need special assistance at the polls; Three states require voters to provide a parent's name; Two states ask voters to provide an email address; One state, Arizona, requires voters to state their occupation." CAL. VOTER FOUND., VOTER PRIVACY IN THE DIGITAL AGE (June 9, 2004), *available at* http://www.calvoter.org/issues/votprivacy/pub/voterprivacy/keyfindings.html.

[64] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

[65] *Id.* at 1160.

[66] *Id.* at 1163.

[67] *See* Zetter, *supra* note 63. "Voter data is widely disseminated to secondary users, including commercial interests in 22 states, typically without any notice to voters that their information will be shared: All states grant candidates and political parties access to voter lists; 43 states use voter lists as a juror source list; 22 states allow unrestricted access to voter lists, which permits the lists to be used for commercial purposes; Four states grant scholars and academics access to voter lists under state statutes; Four states

Demographic data from the U.S. Census is another form of data that has been used in political micro-targeting for a very long time.[68] Starting in 1990, the U.S. Census Bureau began releasing more granular demographic information about race, ethnicity, age, and family type at the level of city blocks.[69] The data typically includes 800 households, in three dozen demographic categories—each attached to a nine-digit ZIP code.[70]

Data is also acquired from voters directly by parties and campaigns through a variety of online and offline sources. For example, a campaign's website requires voters to volunteer personal information whenever they sign up to volunteer, receive campaign communications, or donate. Facebook apps,[71] until recently,[72] have also proven to be a valuable source for campaigns to track users and their friends.[73] Campaigns also maintain records of offline engagement at rallies and volunteer events, all typically recorded by canvassers,[74] and they receive data from political parties, who maintain their own set of data collected over a longer period of time, which typically includes donor data, voter history, attendance at party events, data on volunteers, and information collected by canvassers.[75] Campaigns are also utilizing data received from online tracking cookies[76] that monitor a voter's web traffic.[77] When working in

---

grant journalists access to voter lists under state statutes." *See* CAL. VOTER FOUND., *supra* note 63.

68 *See* ISSENBERG, *supra* note 62, at 42.

69 *Id.* at 59.

70 *Id.* at 59.

71 PEW RESEARCH CENTER, HOW THE PRESIDENTIAL CANDIDATES USE THE WEB AND SOCIAL MEDIA (Aug. 15, 2012), *available at* http://www.journalism.org/2012/08/15/how-presidential-candidates-use-web-and-social-media/.

72 Luke Shuman, *A Facebook Change Makes It Harder for Political Campaigns to See Your Friends*, N.Y. TIMES, Nov. 28, 2014, http://www.nytimes.com/2014/11/29/upshot/a-facebook-change-makes-it-harder-for-political-campaigns-to-see-your-friends.html?ref=politics&abt=0002&abg=0.

73 *See* Sifry, *supra* note 26.

74 Tim Murphy, *Inside the Obama Campaign's Hard Drive*, MOTHER JONES (Oct. 2012) http://www.motherjones.com/politics/2012/10/harper-reed-obama-campaign-microtargeting.

75 *Id.*

76 "A cookie is a very simple text file that gets downloaded onto your PC when you visit a website. They generally contain two bits of information: a site name and a unique user ID. Once the cookie is on your computer, the site 'knows' that you have been there before and can then use that knowledge to tailor the experience that you have. The vast

tandem with online advertising exchanges and media partners, a tracking cookie can serve ads personalized to an individual voter based on the data surveyed.[78] For example, eXelate, one of the largest behavioral targeting firms, tracks 200 million unique individuals per month through cookies that track a user's web traffic.[79] These cookies are able to determine a user's age, sex, ethnicity, marital status, and profession as well as predict what items a user is looking to purchase based on web searches and sites frequented.[80] Ads are served utilizing eXelate data in a process where marketers bid to cookie match their own cookies with eXelate's cookies and identify potential targets.[81]

As mentioned earlier, campaigns also rely on consumer data for their micro-targeting efforts.[82] Consumer data is a diverse category of data typically acquired by campaigns, parties, and political data firms from data brokers like Acxiom or Experian.[83] Consumer data can reflect a voter's buying patterns, lifestyle, demographics, and more. For example, Experian's website has a category for "Life-Event Triggers" and advertises the company's ability to predict when individuals are new parents, homeowners, or have recently moved.[84] Datalogix is a consumer data broker that allows its clients to target SUV drivers, green consumers, and pet owners, and segments individuals into 700 data categories based on their past purchasing habits, demographics, and financial data.[85] These various

---

majority of commercial websites—be they major online publishers, banks or ecommerce sites—will use them." Olivia Solon, *A Simple Guide to Cookies and How to Comply with EU Cookie Law*, WIRED (May 25, 2012), http://www.wired.co.uk/news/archive/2012-05/25/cookies-made-simple.

77 "[Companies are] combining records from voter registration and records purchased from consumer data brokers and cookie-based profiles into very large troves of data about individual voters and their preferences and attitudes that are all things that are used for targeting purposes." Meg Schwenzfeier, *Consumer Data Privacy in Politics*, PULITZER CENTER ON CRISIS REPORTING (Feb. 21, 2014), http://pulitzercenter.org/reporting/north-america-united-states-political-campaigns-consumer-data-privacy.

78 *See* Issenberg, *supra* note 40.

79 *See* TUROW, *supra* note 58, at 79.

80 *Id.*

81 *Id.* at 80.

82 *See supra* text accompanying notes 10–14.

83 *See* Kreiss, *supra* note 12, at 71; *see also* ISSENBERG, *supra* note 62, at 174–75.

84 *See* Schwenzfeier, *supra* note 77.

85 *Id.*

consumer data points are then combined with publicly available data like voter history, party affiliation, or age, or a campaign's internal data to enable campaigns to target voters more precisely.[86] For example, Aristotle appends consumer data to voter lists purchased from state voter databases, allowing its clients to search voters based on home purchase price, credit rating, pet ownership, or refinance loan type.[87]

II. PRIVACY AND DEMOCRACY

In order to understand how computational politics can harm a voter's informational autonomy, and by extension privacy and democracy, it is important to first understand the theoretical underpinnings of informational autonomy and how it relates to normative conceptions of privacy and democracy.

A. Theoretical Underpinnings

In 1890, Samuel Warren and Louis Brandeis famously situated privacy in "the right to be let alone."[88] In their article, Warren and Brandeis were decrying a new technology of the day, smaller cameras that could take an "instantaneous photograph," allowing journalists to surreptitiously snap photos of private persons without their consent.[89] In the past, getting your picture taken was an ordeal that required sitting and posing for hours, and cameras were too large, bulky, and expensive to be portable.[90] With the advent of new technologies, Warren and Brandeis feared that people would be powerless to keep their personal image private or control how it is used.[91]

---

[86] "I might use your vote history, meaning what elections did you participate in, are you registered with one of the parties, what's your age, and what's your income, things like that …. And that information is combined with commercially available data and takes into account your buying patterns, lifestyle patterns, demographics, all kinds of other data." *Id.*

[87] *Premium Enhancements*, ARISTOTLE, http://www.aristotle.com/political-data/premium-enhancements/ (last visited Dec. 19, 2014).

[88] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[89] *Id.* at 195–96; *see also* Solove, *supra* note 15, at 532.

[90] *See* Solove, *supra* note 15, at 532.

[91] *Id.*

Essential in Warren and Brandeis's conception of privacy—whether they knew at the time or not[92]—is a conception of privacy as informational autonomy. Professor Alan Westin took a similar approach in his oft-quoted definition of privacy, calling privacy the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[93] Paul Schwartz also takes an informational autonomy approach, describing privacy as "[seeking] to achieve informational self-determination through individual stewardship of personal data, and by keeping information isolated from access."[94] The Supreme Court also recognized that "the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[95] Key to all of these analyses is a conception of informational autonomy as the right of individuals to determine for themselves how their personally identified information (PII)[96] can be used, a principle that is also reflected in most privacy protection laws.[97]

Indeed, privacy, self-determination, and personal autonomy serve as essential elements for democratic governance. Paul Schwartz has compared Internet surveillance to George Orwell's

---

[92] Warren and Brandeis did not describe the unauthorized photograph as "information," but their concern about the information conveyed in the unauthorized photographs—and what that may suggest about the subject's reputation—does suggest that they were prefiguring what would later be known as "information privacy." *See* Warren & Brandeis, *supra* note 88.

[93] *See* ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

[94] Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

[95] U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press, 489 U.S. 749, 763 (1989).

[96] "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES n.1 (2007).

[97] "Privacy laws in their various forms usually prohibit the release of personally identifiable information …. Information is personally identifiable if it can be traced to a specific individual." Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 6–7 (2011).

telescreen,[98] and he concluded that the harm to a citizen's self-determination from Internet surveillance is more potent due to "data storage possibilities and efficient search possibilities in any database using complex algorithms and other techniques of data mining."[99] Ruth Gavison also echoed the importance of privacy in a "democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy."[100] Neil Richards argues that informational autonomy shapes the struggle "between individuals on the one hand and the corporate and government entities that seek information about them on the other."[101] An example from German law states: "[A] person who cannot oversee with sufficient certainty which of the information about him is known in … his social environment, and who is unable to evaluate the knowledge of a possible communication partner, can be greatly inhibited in his freedom to decide or plan in personal self-determination."[102] This inhibition takes the form of "forced obedience," which can eventuate when the state and private organizations can "transform themselves into omnipotent parents and the rest of society into helpless children."[103] Joel Reidenberg also writes that adequate standards for the treatment of personal information are a necessary condition for citizen participation in a democracy,[104] citing an analog from ancient Greece, where

---

98 Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656 (1999) (citing GEORGE ORWELL, 1984 6 (Penguin Books 1954) (1949)).

99 *Id.* at 1702 n.294.

100 Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980)

101 Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1092 (2006). "The problem with databases does not stem from any specific act, but is a systemic issue of power caused by the combination of relatively small actions, each of which when viewed in isolation would appear quite innocuous. Many modern privacy problems are the product of information flows, which occur between a variety of different entities. There is often no single wrongdoer; responsibility is spread among a multitude of actors, with a vast array of motives and aims, each doing different things at different times." Daniel J. D'Amico, Book Review, 1 J.L. ECON. & POL'Y 537, 541 (2005) (reviewing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004)).

102 Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 562 (1995).

103 *Id*. at 560.

104 "Politically, adequate standards for the treatment of personal information are a necessary condition for citizen participation in a democracy. Since ancient Greece, a citizen's right to participate in society has depended on the ability to control the

a "citizen's right to participate in society has depended on the ability to control the disclosure of personal information."[105]

However, what are we to make of the non-governmental status computational politicians enjoy? Is it fair to assume that normative conceptions of privacy and democracy have purchase when the agent conducting the surveillance and social engineering is a non-profit political party, campaign, or for-profit corporation? The answer must be that the distinction should not matter given the important role private institutions do play—and must play—in our electoral process. Moreover, privacy harms are not totally alleviated by the fact that private institutions largely engage in computational politics. No doubt, federal[106] and state[107] institutions are incredibly secretive about their data, but citizens do have some levers to pull, whether it be via sunshine laws or the political process. Parties, campaigns, and corporations that engage in computational politics are very proprietary about the PII they have gathered and their analytical methodologies,[108] and guard data closely out of fear that partisan opponents will gain access.[109] It is arguable that in-

---

disclosure of personal information. Without appropriate standards, citizens may be unduly constrained in their interactions with society. Socially, the treatment of personal information is an element of basic human dignity. Fair treatment of personal information accords respect to an individual's personality. Standards, thus, structure social relationships." Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497–98 (1995).

105 *Id.*

106 "[E]xisting policies of online transparency are largely developed for the sake of public accountability, but fail to achieve it. In some cases, appropriate transparency requirements exist but are not enforced. In other instances, transparency policies allow agencies considerable discretion to decide which information will be disclosed. In still other cases, transparency policies target information that is irrelevant for purposes of public accountability. To realize the unfulfilled potential of open government, an alternative regulatory regime is required." Jennifer Shkabatur, *Transparency with(Out) Accountability: Open Government in the United States*, 31 YALE L. & POL'Y REV. 79, 140 (2012).

107 *See* Justin Cox, *Maximizing Information's Freedom: The Nuts, Bolts, and Levers of FOIA*, 13 N.Y.C. L. REV. 387, 416 (2010) (describing the need for FOI litigation in some states because state and local officials can be antagonistic and uncooperative with those that request information).

108 PASQUALE, *supra* note 24, at 3, 193.

109 "The 50-state voter file, which is available for the first time to organizations other than the Obama campaign and Democratic candidates (but not to Republicans or Republicans fronts), is updated over 200 times each year." *SmartVAN*, NGP VAN, https://www.ngpvan.com/smartvan (last visited Mar. 31, 2015).

formational autonomy is even more at stake when private unregulated actors trade in PII, especially if legislators are likely to exempt political data from any larger data privacy regulatory regime out of self-interest.[110]

B. Fair Information Practices

While informational autonomy is a well-developed principle in legal theory[111] and in legal doctrine,[112] harms to informational autonomy caused by computational politics are in no way illegal. Federal privacy laws that mandate protections for PII, like the Children's Online Privacy Protection Act (COPPA),[113] Fair Credit Reporting Act (FCRA),[114] Health Insurance Portability and Accountability Act (HIPAA),[115] Gramm-Leach-Bliley Act,[116] and Privacy

---

[110] "'Often when data laws are being proposed and put forward, the politicians exempt themselves,' said Don Hinman, senior VP for data strategy at Epsilon, which gets some of its data from political advertisers but mainly is a purveyor of consumer information." Kate Kaye, *Obama's Approach to Big Data: Do As I Say, Not As I Do*, ADVERTISING AGE (Nov. 16, 2012), http://adage.com/article/digital/obama-s-approach-big-d=ata-i-i/238346/.

[111] *See supra* Part II.A.

[112] "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press, 489 U.S. 749, 763 (1989).

[113] 15 U.S.C. § 6501 (2000). "COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age." *Children's Online Privacy Protection Rule ("COPPA")*, FTC, http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (last visited Dec. 19, 2014).

[114] FCRA requires consumer credit reporting companies to adopt procedures for consumer information that are fair and equitable with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information. 15 U.S.C. § 1681 (2006).

[115] HIPAA's "privacy rule" limits the use of "protected health information." *See* 42 U.S.C. § 1320d(1)–(8) (2002).

[116] "The Gramm–Leach–Bliley Act requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data." *Gramm–Leach–Bliley Act*, FTC, http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act (last visited Dec. 19, 2014); *see also* 15 U.S.C. § 6801 (2006).

Act,[117] are either too narrow so as not to apply to computational politics or only apply to governmental data practices.

However, all of these laws safeguard informational autonomy because they incorporate a longstanding principle in federal and state data and computer record-keeping practices known as "fair information practices" (FIPs). The principle was first applied to computer databases in a 1973 report by the U.S. Department of Health, Education, and Welfare (HEW), in which the agency acknowledged potential harms to individuals when they lack control over personal information.[118] The report set forth several "Fair Information Practices,"[119] including that "[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[120] This principle influenced the Privacy Act of 1974,[121] the EU Data Protection Directive of 1995,[122] and others.[123] FIPs vary in definition and implementation, but Professor Paul F. Schwartz helpfully distills them into four basic requirements: "(1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight."[124]

---

[117] "The Privacy Act of 1974 … establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies." *Privacy Act of 1974*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/opcl/privacy-act-1974 (last visited Dec. 19, 2014); *see also* 5 U.S.C. § 552(a) (1988).

[118] SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, PUB. NO. (OS)73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) [hereinafter SECRETARY'S ADVISORY COMM.]; *see also* Lillian R. Bevier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 462 (1995).

[119] Solove, *supra* note 15, at 520.

[120] SECRETARY'S ADVISORY COMM., *supra* note 118; *see also* Solove, *supra* note 15, at 520.

[121] Solove, *supra* note 15, at 520.

[122] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

[123] Solove, *supra* note 15, at 520.

[124] Schwartz, *supra* note 98, at 1614.

FIPs can serve to safeguard democracy by defining the terms of individual participation in social and political life.[125] Schwartz has linked the FIPs to the preservation of democratic order, "by providing access to one's personal data [and] information about how it will be processed," as well as how "the law seeks to structure the terms on which individuals confront the information demands of the community, private bureaucratic entities, and the State."[126]

Applying FIPs in computational politics can remediate harms to informational autonomy and democracy in three ways. First, transparency could mitigate the surreptitious nature of data-gathering in many online and offline scenarios. If computational politicians reveal to voters how their data is gathered, who it is being shared with, and how it is being processed, voters will be more aware of campaign practices that seek to influence or manipulate in ways they may disapprove of. Second, "defined obligations" and "procedural and substantive rights" can afford voters the control necessary to make changes to data once it has been revealed to them, either by correcting false data, removing data that they no longer want on file, or opting out of tracking all together. Lastly, by offering more transparency and control to voters, campaigns can improve upon a system of data collection premised on a legal framework for consent that is more or less a sham. Although voters "voluntarily" disclose their information to campaigns, websites, and many other consumer services, they almost universally fail to appreciate the degree to which companies, campaigns, and political parties retain the right to freely trade their data in an endless chain of secondary and tertiary uses. FIPs can improve this system by informing voters if their data will be traded for secondary uses and allowing them the choice to restrict subsequent uses or even opt out altogether.

C. Informational Privacy Harms

Like Warren and Brandeis's camera, computational politics harms privacy in ways dramatically different from anything pre-

---

[125] Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1564 (2000).

[126] *Id.*

viously possible.[127] Network computing, data storage, and comprehensive records of online behavior[128] all allow private actors to surreptitiously monitor voter information for their own purposes.[129] Privacy experts have connected the loss of informational autonomy with a variety of harms to democracy, including discrimination,[130] the chilling of political speech,[131] and unaccountable "black box" algorithms.[132] This Note will now provide a brief summary of each, and describe how they apply in the context of computational politics.

1. Discrimination

Computational politics can allow companies, parties, and campaigns to distinguish individual members submerged in groups based on granular individual characteristics, preferences, and activities.[133] Algorithms can then crunch the data and allow campaigns and corporations to discriminate based on an infinite number of data points and treat individuals differently on that basis.[134] Predictive privacy harms can and do result when computational politicians discriminate between individuals based on their data profiles.[135] A voter given a particular classification is saddled with any "cascading disadvantages" associated with that particular classification.[136] Disadvantages include "redlining,"[137] where campaigns

---

127 Schwartz, *supra* note 98, at 1610–11.

128 *Id.*

129 *Id.*

130 *See infra* Part II.C.1.

131 *See infra* Part II.C.2.

132 *See infra* Part II.C.3.

133 Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. TELECOMM. & HIGH TECH. L. 351, 355 (2013).

134 See *id.*

135 Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 99 (2014); *see also* PASQUALE, *supra* note 24, at 215.

136 *See* PASQUALE, *supra* note 24, at 32.

137 "Redlining is an old term used to refer to the organizational practice of identifying the parts of a community that are difficult or problematic to serve. Most often the term refers to how organizations decide that some people, by virtue of neighborhood attributes and perceptions, should be offered low standards of service and indenturing obligations. These neighborhoods would be circled in red ink as places where insurance companies would give uncompetitive rates, banks would have more demanding repayment plans, government agencies would make fewer investments, or real estate developers would

use data to ignore voters with attributes that suggest an unlikelihood to vote.[138] According to Philip N. Howard, political campaigns redline when they are "declining to serve a community if it is not part of a sensitive electoral district or declining to serve individuals if they are perceived to be less sensitive to the political issue."[139] For example, Howard argues that the ability to disengage with "unlikely" or "unpersuadable" voters through modeling suggests that campaigns can apply the "swing state" strategy deployed in presidential politics but at the individual level[140]—meaning that "non–voters" can be ignored while others can be flooded with campaign material,[141] introducing a new form of categorical inequality into our politics.[142]

Campaigns are redlining voters with audience segmentation tools provided by political data firms. For example, in 2012, Aristotle partnered with Intermarkets, a digital ad firm and ad sales rep for web publishers. The partnership combines Aristotle's political data with consumer data tracked from Intermarkets' "cookie pool" in order to "[segment] online audiences into groups political advertisers want to target."[143] Another example is TargetSmart—an active Democratic data firm during the 2014 midterms—which segments voters based on data used by consumer marketers in order to model each voter based on a persuadability factor,[144] not unlike the Obama campaign's strategy in 2012.[145] [x+1] Inc.,[146] a company that provides artificial intelligence advertising solutions for

---

refuse to build new ventures." *See* PHILLIP N. HOWARD, NEW MEDIA CAMPAIGNS AND THE MANAGED CITIZEN 132 (2006) (internal quotations omitted).

138 Kreiss, *supra* note 12, at 73–74.

139 *See* HOWARD, *supra* note 137, at 133.

140 *See* Tufekci, *supra* note 39.

141 *Id.*

142 *Id.*

143 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.

144 *The Numbers Behind 'The Persuadables,'* BLOOMBERG POLITICS (Oct. 27, 2014), http://www.bloomberg.com/politics/articles/2014-10-27/the-numbers-behind-the-persuadables.

145 Sifry, *supra* note 26.

146 Now acquired by Rocket Fuel. *See* Press Release, Rocket Fuel, Rocket Fuel to Acquire [x+1] (Aug. 5, 2014), *available at* http://rocketfuel.com/press_release/rocket-fuel-to-acquire-x1.

digital marketers,[147] including some politics and advocacy organizations,[148] accesses massive databases of online behavior gathered through tracking technologies across the web.[149] [x+1] uses this data to help its clients draw assumptions about a target's proclivities and alter displayed ads for each individual based on his or her segment.[150] A test subject during a *Wall Street Journal* investigation was placed in a [x+1] segment called "White Picket Fences," meant for individuals who "live in small cities, have a median income of $53,901, are 25 to 44 years old with kids, work in white-collar or service jobs, generally own their own home, and have some college education."[151]

There is also real concern that these algorithms can result in discriminatory outcomes for members of protected classes. Algorithms can "find strong correlations, which result in discriminatory outcomes while based on neutral factors."[152] For example, FTC Chief Technologist Latanya Sweeney discovered how race can affect what types of ads are served by predictive online advertising.[153] Sweeney discovered a disproportionate likelihood that advertisements for arrest-record searches appeared on websites with distinctly African-American qualities.[154] Her research also demonstrated that these advertisements were 25 percent more likely to show up on a search for distinctively black names when compared to white names.[155] Given the potential for harm,[156] data scientists like Cynthia Dwork have urged algorithms to be subjected to a

---

147 *About Rocket Fuel*, ROCKET FUEL, http://rocketfuel.com/about-rocket-fuel#success_stories (last visited Dec. 19, 2014).

148 *Id.*

149 Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only,* WALL ST. J. (Aug. 4, 2010), http://online.wsj.com/articles/SB10001424052748703294904575385532109190198.

150 *Id.*

151 *Id.*

152 Tene & Polonetsky, *supra* note 133, at 358–59; *see also* PASQUALE, *supra* note 24, at 38–39.

153 Laura Ryan, *Feds Investigate 'Discrimination by Algorithm,'* NAT'L J. (Sept. 15, 2014); *see also* PASQUALE, *supra* note 24, at 38–39.

154 Ryan, *supra* note 153; *see also* PASQUALE, *supra* note 24, at 38–39.

155 Ryan, *supra* note 153; *see also* PASQUALE, *supra* note 24, at 38–39.

156 Wade Henderson & Rashad Robinson, *Big Data is a Civil Rights Issue*, TALKING POINTS MEMO (Apr. 8, 2014), http://talkingpointsmemo.com/cafe/big-data-is-a-civil-rights-issue.

"fairness constraint," through which an algorithm's discriminatory outcomes are tested to see if similar individuals are treated similarly.[157] Civil rights groups have urged for reforms as well, citing a need for individual autonomy over personal information "that is known to a corporation [that] can easily be used by companies and the government against vulnerable populations, including women, the formerly incarcerated, immigrants, religious minorities, the LGBT community, and young people."[158] The White House Report on Big Data also warned that "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[159]

2. Chilling Effects

The knowledge that all consumer, Internet, and political transactions are surveilled, compiled, and sold can alter a citizen's behavior and even chill political association.[160] There are three reasons why associational chilling can occur when voters lose their informational autonomy.

First, consumer data-mining practices are surreptitious, passive, and automatic.[161] Voters are unable to predict when or how their digital dossiers are being compiled and what the data suggests about them.[162] For example, campaigns compile voter lists containing the names and contact information of all voters that have inte-

---

[157] Cynthia Dwork et al., *Fairness Through Awareness* (Nov. 29, 2011), *available at* http://www.cs.toronto.edu/~zemel/documents/fairAwareItcs2012.pdf.

[158] Press Release, The Leadership Conference, Civil Rights Principles for the Era of Big Data (2014), *available at* http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html.

[159] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 1, 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; *see also* PASQUALE, *supra* note 24, at 38.

[160] Evans, *supra* note 10, at 882. For an example of a complainant alleging the chilling of associational rights due to governmental data-gathering, *see* Laird v. Tatum, 408 U.S. 1, 11 (1972); *see also* Nat'l Ass'n for Advancement of Colored People v. State of Ala. *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (stating that associational disclosure can result in economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility).

[161] *See supra* text accompanying notes 19–22.

[162] *Id.*

racted with the campaign online and offline.[163] These lists are then matched with data firms like Aristotle, which lay bare a voter's consumer habits along with models for persuadability or other algorithmic judgments.[164]

Second, because campaigns are subjected to practically no regulation for the repurposing of political data, voters are unable to predict what other campaigns or candidates will benefit from their data in the future. For example, the privacy policies used by both candidates in the 2014 Kentucky Senate race lacked sufficient clarity about potential secondary use of voter data. Democratic candidate Alison Lundergran Grimes's online privacy policy promises not to share a voter's data with third parties except with those "candidates, organizations, campaigns, groups or causes that we believe have similar political viewpoints, principles or objectives,"[165] a policy that tracks with the Democratic National Committee's own policy.[166] Senator Mitch McConnell's online privacy policy does not even acknowledge third-party sharing of personal information,[167] but the Republican party reserves the right to share data with like-minded organizations.[168] Although the policies may be short and comprehensible as is recommended by the FTC,[169] they give little instruction as to what may happen to a voter's personal information once the campaign is over.

---

[163] *See supra* Part I.C.

[164] Aristotle's website advertises a "data matching" service that allows campaigns to "match [their] list to [Aristotle's] voter file and pull out records that [they] may want to exclude from [their] database." *Data Matching*, ARISTOTLE, http://aristotle.com/political-data/data-matching/ (last visited Dec. 19, 2014).

[165] *Privacy Policy*, ALISON FOR KENTUCKY, http://alisonforkentucky.com/privacy-policy/ (last visited Dec. 19, 2014).

[166] *Privacy Policy*, DEMOCRATS, http://www.democrats.org/privacy_policy (last visited Dec. 19, 2014).

[167] *Privacy Policy*, TEAM MITCH, http://www.teammitch.com/privacy_policy (last visited Dec. 19, 2014).

[168] "We may share your information with like-minded organizations. The RNC may share information—that you voluntarily provide us—with like-minded organizations committed to the principles or candidates of the Republican Party, Republican State Party organizations and local Republican groups. The RNC may provide your email address or other personal information to authorized third parties required to deliver a particular service. These third parties may not use said information for any other purpose than to carry out the services they are performing for the RNC." *Terms & Conditions and Privacy Policy*, GOP, https://www.gop.com/privacy/ (last visited Dec. 19, 2014).

[169] FTC REPORT, *supra* note 34, at viii.

Third, fear of discrimination and redlining can cause chilling effects. As discussed earlier, campaigns that engage in computational politics are able to discriminate and profile the electorate in new and powerful ways.[170] Politicians can choose to under serve or ignore particular parts of their constituency based on what an algorithmic model tells them about that group's electoral utility.[171] Although the fear of redlining is nothing new,[172] the addition of computational politics can make the practice a lot more harmful due to its pervasive and surreptitious nature.

3. Black Boxes

Because computational politics involves opaque, latent, and sophisticated computer modeling to carry out highly effective campaigns of persuasion and social engineering, there are justifiable concerns about the further accretion of political influence to a wealthy and powerful few.[173] This accretion of power is enhanced by the loss of an individual's informational autonomy which makes mining the raw material for computational politics dirt cheap.[174] But also, power is solidified due to the opacity of political data firms that operate so-called "black box" algorithms in computational politics.[175]

As discussed earlier, computational politics is conducted surreptitiously and is subjected to little independent oversight.[176] As a result, private data practices are opaque and voters have no ability to control—much less anticipate—when or how their data is collected or how it is used to distinguish them from other voters.[177] Professor Frank Pasquale has discussed at length the potential harms caused by opaque algorithms in search.[178] Pasquale discusses the role of Internet gatekeepers like Google, who operate informational bottlenecks that can "manipulate the flow of informa-

---

170 *See supra* Part II.C.1.
171 *Id.*
172 HOWARD, s*upra* note 137.
173 *See generally* Tufekci, *supra* note 39.
174 *See generally* PASQUALE, *supra* note 24, at 30–34.
175 *See id.* at 9–10.
176 *See supra* Part II.B.
177 *See supra* text accompanying notes 19–22.
178 *See* PASQUALE, *supra* note 24, at 66.

tion … [and suppress] some sources while highlighting others" either because of intrinsic preferences or inducement from others.[179] Lack of informational autonomy and oversight can facilitate manipulation through unaccountable private "black-box"[180] algorithms. Pasquale warns of a "black box society"[181] where private firms can lock away information even when there is a strong public interest for disclosure.[182] In Pasquale's view, unaccountable Internet power can stifle innovation by manipulating the market in order to maintain power and "pick winners" among content and application providers.[183] For example, Facebook has demonstrated that its proprietary algorithms can affect voter turnout,[184] albeit by a slim .39 percent, but enough to swing a close election.[185] Jonathan Zittrain explains how Facebook, or another dominant social network, could in the future affect electoral outcomes in far more insidious ways,[186] by using the Facebook newsfeed to only activate voters that Facebook's algorithms have identified as likely to support the company's favored candidate.[187]

---

[179] Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1165 (2008); *see also* PASQUALE, *supra* note 24, at 67.

[180] *See* Frank Pasquale, *Battling Black Boxes*, MADISONIAN.NET (Sept. 21, 2006), http://madisonian.net/2006/09/21/battling-black-boxes/.

[181] *See generally* PASQUALE, *supra* note 24, at 16–18.

[182] Frank Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines*, 2008 U. CHI. LEGAL F. 263, 286 (2008).

[183] *Id.* at 299; *see also* PASQUALE, *supra* note 24, at 191–92.

[184] Sifry, *supra* note 26.

[185] *See* PASQUALE, *supra* note 24, at 74.

[186] "Now consider a hypothetical, hotly contested future election. Suppose that Mark Zuckerberg personally favors whichever candidate you don't like. He arranges for a voting prompt to appear within the newsfeeds of tens of millions of active Facebook users—but unlike in the 2010 experiment, the group that will not receive the message is not chosen at random. Rather, Zuckerberg makes use of the fact that Facebook 'likes' can predict political views and party affiliation, even beyond the many users who proudly advertise those affiliations directly. With that knowledge, our hypothetical Zuck chooses not to spice the feeds of users unsympathetic to his views. Such machinations then flip the outcome of our hypothetical election. Should the law constrain this kind of behavior?" Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, THE NEW REPUBLIC (June 1, 2014), http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering. *See also* PASQUALE, *supra* note 24, at 74.

[187] *Id.*

Pasquale's critiques of search and social networks can be analogized to computational politics. Political data firms like Aristotle operate as informational gatekeepers and solidify their market dominance with exclusive contractual arrangements to consolidate data with advertising firms,[188] market research firms,[189] and data analytics firms.[190] Market dominance can be used to affect particular political outcomes. In the case of partisan data operations it is clear that computational tools are meant to affect a particular partisan outcome. As for non-partisan firms like Aristotle, there remains a concern that particular kinds of political outcomes or candidates can be prioritized. For example, the corporate leaders in some of these non-partisan firms have deep ties with powerful D.C. partisans,[191] which can inform which clients a firm is willing to take on[192] or what business contracts to enter into.[193] Beyond partisanship, computational politics can privilege a wealthier class of candidates and campaigns that can afford their highly effective and expensive suite of data services[194] or who have spent years investing

---

188 Kaye, *supra* note 143.

189 For example, the market research firm Claritas has an exclusive data-sharing arrangement with Aristotle. Verini, *supra* note 55.

190 Press Release, Evolving Strategies and Aristotle Introduce Groundbreaking Voter Targeting Technology that Could Flip the Senate Next Month (Oct. 8, 2014), http://www.prnewswire.com/news-releases/evolving-strategies-and-aristotle-introduce-groundbreaking-voter-targeting-technology-that-could-flip-the-senate-next-month-278523401.html.

191 "[T]he companies Aristotle does business with have deep ties in Washington. Acxiom's recently retired CEO, Charles Morgan, is a longtime friend of Bill and Hillary Clinton's. Wesley Clark, the retired general and former Democratic presidential candidate, used to sit on Acxiom's board. Catalist, a data-mining firm providing voter lists to the Clinton campaign in the 2008 race, is presided over by Harold Ickes Jr., Bill's onetime deputy chief of staff, and Laura Quinn, who held the same position in Al Gore's office. In 2005, the Department of Justice alone bought $19 million worth of records from data miners, according to the Government Accountability Office." Verini, *supra* note 55.

192 "F.E.C. filings from 2006–7 show, however, that the majority of Aristotle's client candidates were and are Republicans. Among them are former House majority leader Tom DeLay and former California congressman Duke Cunningham. The National Rifle Association was once Aristotle's biggest client." *Id.*

193 *See* Press Release, *supra* note 190.

194 *See* ISSENBERG, *supra* note 62, at 174–75 (describing the cost of commercial data services from the country's largest commercial data warehouses like InfoUSA, Acxiom, and Experian).

in expensive in-house data operations[195]—a problem that is compounded given the ever-increasing price of post-Citizens United campaigning.[196]

III. UNDERSTANDING HOW TO REFORM COMPUTATIONAL POLITICS

A. Challenges

Given the role computational politics plays in influencing important political outcomes for all Americans, it is essential that voters are afforded some insight into and control over these systems. Fundamentally, partisan and non-partisan political data firms are in the business of information about voters and how they behave, and that kind of information is only valuable if it is exclusive, and remains exclusive through the full power of copyright protections.[197] Trade secrets make it impossible to test the fairness, validity, or honesty behind algorithms used in computational politics.[198] Successful firms in computational politics will not be evaluated for the fairness, validity, or honesty behind their voter data,[199] and instead can only be judged on a reputation built on past successes.[200] Meanwhile, the voters that make the system possible with their data will have no insight into or control over these important algorithms. In order to prevent the aforementioned privacy harms,[201]

---

[195] "The Republican National Committee, which had already invested in a national ground game, built an in-house data and analytics infrastructure. They tested their model universe, making thousands of calls each week to voters in order to better refine their targeting assumptions. And they used the special election in March in Florida's 13th Congressional District to quietly test their smartphone apps." Ashley Parker, *Chastened Republicans Beat Democrats at Their Own Ground Game*, N.Y. TIMES, Nov. 7, 2014, http://www.nytimes.com/2014/11/08/us/politics/republicans-beat-democrats-at-their-own-ground-game.html.

[196] *The Money Behind the Elections*, CENTER FOR RESPONSIVE POLITICS, https://www.opensecrets.org/bigpicture/ (last visited Dec. 19, 2014); Ian Vandewalker, *Outside Spending and Dark Money in Toss-Up Senate Races Post-Election Update*, BRENNAN CTR. FOR JUSTICE (2014), http://www.brennancenter.org/sites/default/files/blog/Post_Election_Spending.pdf.

[197] *See* PASQUALE, *supra* note 24, at 215.

[198] *Id.* at 217.

[199] *Id.* at 217–18.

[200] *Id*.

[201] *See supra* Parts II.C.1–3.

regulatory regimes must be put in place to allow voters some access to the data and algorithms behind computational politics.

But legislating strong data privacy protections is very difficult.[202] Many proposals to regulate data are overly restrictive, under-protective, or both.[203] In some cases, sophisticated data firms will find a way to circumvent new restrictions and in so doing make their services more valuable.[204] Also, because legislating political data protections necessarily implicates the First Amendment,[205] restrictions that outright forbid tracking a citizen's political beliefs—similar to the EU Privacy Directive—are simply not workable.[206]

---

[202] "Of all reputation systems … credit scores are by far the most regulated. Yet regulation has done little to improve them. Penalties for erroneous information on credit reports are too low to merit serious attention from credit bureaus." PASQUALE, *supra* note 24, at 191.

[203] *Id.*; *see also* Evans, *supra* note 10, at 893–94.

[204] "Johnson et al. recommend making donor data 'read only' to increase the cost of importing such data into political databases. This would seem to only bar outsider candidates with limited resources from using the data, while professional political data-miners will quickly find a way to work around the nuisance—making their service even more valuable. They also propose limiting the lifespan of contributor data, but again, professional data-miners could quickly find a work-around and mark up the cost of their services." *See* Evans, *supra* note 10, at 893–94.

[205] "[P]rivacy concerns give way when balanced against the interest in publishing matters of public importance. As Warren and Brandeis stated in their classic law review article: 'The right of privacy does not prohibit any publication of matter which is of public or general interest' …. One of the costs associated with participation in public affairs is an attendant loss of privacy." Bartnicki v. Vopper, 532 U.S. 514, 534 (2001); *see also* Philip N. Howard & Daniel Kreiss, *Political Parties and Voter Privacy: Australia, Canada, the United Kingdom, and United States in Comparative Perspective*, 15(12) FIRST MONDAY (Dec. 6, 2010), *available at* http:// firstmonday.org/htbin/cgiwrap/bin/ojs/ index.php/fm/article/view/2975/2627 ("On First Amendment grounds, provided they remain non-state actors candidates and parties enjoy broad latitude with respect to their data practices.").

[206] "The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited." Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

B. Reform Skeptics

Reform skeptics may understandably protest the regulation of a lawful data industry. Citizens are freely giving away their informational autonomy. And why not—especially if more data results in higher turnout,[207] more relevant political ads,[208] or if the private data used by campaigns was given away in exchange for a service like a discount at a supermarket check-out[209] or for the use of a social network.[210] Others may even question whether computational politics truly predicts a voter's actual behavior or reveals the "truth" behind their behaviors or motivations; that "truth" may not exist in any case.[211]

Indeed, computational politics can boost voter turnout. Facebook has demonstrated this with its experiments during the 2010 midterm election.[212] Also, it is true that with more data, campaigns can craft better appeals to individual voters and even motivate previously disengaged voters.[213] An example of this from the 2012 Obama campaign was the use of Facebook to match supporters with their friends living in swing states. Supporters were prompted with a picture of their friend and were told to click a button to automatically urge those targeted voters to register to vote, vote early, or get to the polls.[214] According to the campaign, 1 in 5 people contacted by a Facebook friend acted on the request, in large part because the campaign was able to match supporters with people they knew and

---

[207] *See supra* text accompanying notes 39–44.

[208] *Id.*

[209] Donna Ferguson, *How Supermarkets Get Your Data—and What They Do with It*, THE GUARDIAN (June 8, 2013), http://www.theguardian.com/money/2013/jun/08/supermarkets-get-your-data.

[210] Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Mar. 9, 2014), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

[211] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1406 (2000).

[212] Micah L. Sifry, *Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012*, MOTHER JONES (Oct. 31, 2014), http://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout.

[213] *See* Evans, *supra* note 10, at 896.

[214] 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/2/.

deliver targeted appeals based on personal information received through the campaign's Facebook app.[215]

Although Facebook's voting experiment appeared to be a great public service, without better insight into the black boxes that conduct these experiments, there is no guarantee that future social networks will be so benevolent. Also, the issue is not whether insights afforded by data are accurately portraying reality or if voters are indeed receiving more relevant campaign ads. Rather, the issue is who controls those modes of prediction,[216] whether it works well enough to affect outcomes, and whether that mechanism has any obligation to remain accountable to the individuals whose data serves as its raw material. This inquiry is more relevant because at bottom, the point of political data is not to help campaigns become more congenial to the attitudes of voters. The goal is to win elections—and the data suggests that it is helping.[217] Data-driven targeting is not meant to merely enable choice by the target market; rather it means to effectuate choice by the marketer.[218] When a communication is framed in order to become more attractive by reflecting a target's desires, it does not necessarily make the communication less manipulative.[219] Manipulation can also be enhanced by the lack of meaningful consent on the part of voters. Voters may consent to the initial use of their political information, but most would not have consented to its continuous aggregation and applications in unexpected ways.[220]

---

215 *Id.*

216 Cohen, *supra* note 211, at 1406.

217 "[Campaigns] develop predictive models that produce individual-level scores that predict citizens' likelihoods of performing certain political behaviors, supporting candidates and issues, and responding to targeted interventions. The use of these scores has increased dramatically during the last few election cycles. Simulations suggest that these advances could yield sizable and electorally meaningful gains to campaigns that harness them." Nickerson & Rogers, *supra* note 38, at 27.

218 Cohen, *supra* note 211, at 1407.

219 *Id.*

220 Philip N. Howard, *Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy*, 597 ANNALS AM. ACAD. POL. & SOC. SCI. 153, 166 (2005).

C. Applying the Fair Information Practices and First Amendment Concerns

So if information wants to be free,[221] how do we regulate it? On what basis do legislators and regulators impose additional obligations on computational politicians—especially when the data was acquired with consent, albeit passively? Answering this question will require a return to the identifiable privacy interest at stake in computational politics: informational autonomy.[222]

Informational autonomy advocates argue that individuals assert a property interest over their personal information.[223] With a property interest, an individual can assert control over use and protect against misuse.[224] The extent to which individuals ought to effect control over data is disputed. On the one hand, enforcing privacy rights as vigorously as copyright law may make progress in protecting privacy,[225] but would also result in the blocking of the free flow of data across the Internet, a proposition that raises clear First Amendment concerns.[226] No doubt, the proper regulatory regime exists somewhere between these extremes.

Applying FIPs to computational politics would be the best way to balance these competing concerns for two reasons. First, FIPs

---

[221] Steward Brand, *Keep Designing: How the Information Economy is Being Created and Shaped by the Hacker Ethic*, WHOLE EARTH REV. 44 (May 1985).

[222] Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2190 (2004).

[223] "To note that privacy talk is embedded in the discourse of property, of course, is to beg the question whether reality is similarly embedded. Some philosophers argue that privacy has meaning only to the extent that it is reducible to a property interest." Cohen, *supra* note 211, at 1379; *see also* Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 333–34 (1995) (describing a "quasi-property" interest in informational privacy theory).

[224] Lawrence Lessig, CODE VERSION 2.0 229 (2006).

[225] *Id.* Moreover, algorithmic processes are premised on smooth, fast, and efficient transactions; introducing reforms will probably slow things down and incur additional expenses. PASQUALE, *supra* note 24, at 213.

[226] Schwartz, *supra* note 223, at 333; *see also* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 760 (2000) (describing desirous uses of personal information without prior consent and the First Amendment concerns of limiting use through individual consent). Most scholars addressing the cyber-property controversy concur, arguing that property-rule protection for network resources is wholly inappropriate; this line of argument guided the court's decision in *Intel Corp. v. Hamidi*. Bellia, *supra* note 222, at 2190.

do not take away a private actor's ability to speak in violation of the First Amendment. FIPs one,[227] two,[228] and four[229] regulate only business practices of private entities without silencing speech.[230] For example, FCRA imposes a defined transparency regime that requires data companies to provide information used to evaluate a consumer's credit upon his request.[231] Paul Schwartz has likened FIP statutes like FCRA to regulating other uses of information in the private sector such as food labeling,[232] in that the regulation of private sector information in order to ensure the goals of transparency, like fairness and accuracy, is an uncontroversial regulation of speech. Second, the FIPs have enjoyed longstanding use in federal, state, and international information privacy protection law for decades[233] and have survived First Amendment challenges.[234] Their use is battle-tested and uncontroversial.

IV. PROPOSALS FOR FEDERAL AND STATE LEGISLATIVE AND REGULATORY REFORM

A. Regulatory Implementation of the Fair Information Practices

As stated earlier, implementing FIPs can foster individual autonomy in computational politics by promoting political data trans-

---

[227] "(1) defined obligations that limit the use of personal data." *See supra* text accompanying note 124.

[228] "(2) transparent processing systems." *See supra* text accompanying note 124.

[229] "(4) external oversight." *See supra* text accompanying note 124.

[230] Schwartz, *supra* note 125, at 1561–62.

[231] 15 U.S.C. § 1681(d) (2006). "No prevention of speech about anyone takes place, for example, when the Fair Credit Reporting Act of 1970 requires that certain information be given to a consumer when an 'investigative consumer report' is prepared about her." Schwartz, *supra* note 125, at 1562.

[232] "The First Amendment does not prevent the government from requiring product labels on food products or the use of 'plain English' by publicly traded companies in reports sent to their investors or Form 10-Ks filed with the Securities and Exchange Commission." Schwartz, *supra* note 125, at 1562.

[233] *See supra* Part II.B.

[234] The Federal Trade Commission's ban on the sale of target marketing lists under FCRA was not a violation of the credit reporting agency's First Amendment rights under intermediate scrutiny because "protecting the privacy of consumer credit information is substantial." *See, e.g.*, Trans Union Corp. v. FTC, 245 F.3d 809, 818 (D.C. Cir. 2001).

parency and encouraging choice on the part of voters.[235] There are plenty of statutes that have implemented FIPs that could serve as a model for implementation in the computational politics context.[236] For example, COPPA emphasizes transparency and choice for parents by requiring operators of any website that knowingly collects personal information from children to provide notice on the site of what information is collected, how the data is used, and whether the data is shared with third parties.[237] The Act also grants parents the power to request their child's data and block a website from surveilling their child's online activities in the future.[238] COPPA is instructive of how regulators could implement a regime that promotes transparency of data, gives voters choices about what to do with their data, and provides options to opt out of future data gathering.

1. Transparency and Choice Portal

Fairness, in the collection of personal information, dictates that the subject of the collection have at least as much information as the entity collecting it.[239] In order to foster fairness, voters need a right to access the black box data behind computational politics. A "right to access" is an uncontroversial FIP,[240] which has been accepted by both government and private entities and is incorporated into federal and state law as well as private business practices.[241]

Of course, a right to access would be meaningless without a corresponding right to delete or correct data or disable future tracking.[242] One such proposal would be a one-stop web portal where computational politicians disclose voter data and offer voters a

---

[235] INTERNET POLICY TASK FORCE, U.S. DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

[236] *See supra* text accompanying notes 113–17.

[237] 15 U.S.C. § 6502(b)(1)(A)(i-ii) (2002).

[238] 15 U.S.C. § 6502(b)(1)(B)(i-iii) (2002).

[239] Preston N. Thomas, *Little Brother's Big Book: The Case for A Right of Audit in Private Databases*, 18 COMMLAW CONSPECTUS 155, 182 (2009).

[240] *Id.* at 183.

[241] *Id.*

[242] "Merely being aware of the contents of a dossier provides little comfort or help to an individual troubled by potential inaccuracies or misuses of that information." *Id.*

chance to correct or delete data or disable tracking. The regime could mirror COPPA's language and target websites and online services that collect a voter's data with knowledge and for political purposes.

Also, centralized data clearinghouses spurned by government regulation are not new. In response to the Fair and Accurate Credit Transactions Act of 2003's (FACTA)[243] requirement that a consumer reporting agency offer free annual credit reports for consumers,[244] a group of the largest consumer data firms (Equifax, Experian, and TransUnion) created AnnualCreditReport.com,[245] the official, centralized source of free credit reports.[246] A similar website could be used to disclose data used for computational politics, including what kind of data is being gathered, what it reveals, and who it is being shared with. Also, to ensure meaningful compliance, regulators could impanel "data auditors," government employees charged with understanding commercial and political data practices and detecting and deterring behaviors that violate FIPs or result in harmful discriminatory outcomes.[247]

In a 2012 consumer privacy report, the Federal Trade Commission recommended that consumer data brokers maintain websites where they could identify themselves to consumers, describe how they collect and use consumer data, and detail the access rights and other choices they provide with respect to the consumer data they maintain.[248] A similar website, but centrally operated by a federal agency, could be an effective tool in order to foster FIPs in a computational politician's data policies.

---

[243] 15 U.S.C. § 1681(j) (2006).

[244] 15 U.S.C. § 1681(j) (2006).

[245] ANNUALCREDITREPORT.COM, https://www.annualcreditreport.com/ (last visited Dec. 19, 2014).

[246] Thomas, *supra* note 239, at 191.

[247] PASQUALE, *supra* note 24, at 151; Thomas, *supra* note 239, at 172 (arguing that a "right to audit" exists in the FIPs).

[248] FTC REPORT, *supra* note 34, at v. Acxiom maintains such a website, allowing consumers to access their data profiles and even stop future tracking. Katy Bachman, *Confessions of a Data Broker: Acxiom's CEO Scott Howe Explains How Self-Regulation Can Work*, ADWEEK (Mar. 25, 2014), *available at* http://www.adweek.com/news/technology/confessions-data-broker-156437.

A centralized government-operated website has many benefits over the self-regulation policy adopted by the FTC and seen in FACTA. For instance, Experian, in a comment to the FTC,[249] voiced privacy and security concerns regarding a right to access and correction of data files, explaining that in order to identify a user's rights, a company engaging in self-regulation will need additional sensitive PII in order to authenticate a user's request for data.[250] If the government acts as the trustee and intermediary between trackers and voters, private companies will not need to maintain sensitive records for authentication purposes. Also, many commentators maintain that data is not always sold to third-party companies with information that could individually identify any one person.[251] With a centralized hub, the government could verify a voter's identity using sensitive PII (e.g. Social Security number) and aggregate all records maintained on that individual across all political data companies that track him or her. In cases where the data was sold to a third-party broker and later re-identified, such information would then be available for the voter when the third-party broker discloses. Once a voter's data is disclosed, the portal could allow voters to make decisions about future tracking. This could come in the form of centralized and user-friendly "do-not-track" (DNT) mechanisms.[252] The FTC has recommended that consumer data brokers use DNT mechanisms but has decided

---

[249] FTC REPORT, *supra* note 34, at 7 n.32 (citing Comment of Experian).

[250] "One commenter raised concerns about granting access and correction rights to data files used to prevent fraudulent activity, noting that such rights would create risks of fraud and identity theft. This commenter also stated that companies would need to add sensitive identifying information to their marketing databases in order to authenticate a consumer's request for information, and that the integration of multiple databases would raise additional privacy and security risks." *Id.* at 64.

[251] "[C]ommenter pointed out that many marketers do not maintain records about data sold to other companies on an individual basis. Thus, marketers have the ability to identify the companies to which they have sold consumer data in general, but not the third parties with which they may have shared the information about any individual consumer." *Id.* at 65.

[252] In order to define DNT, one must first understand what "tracking" entails. According to the Center for Democracy and Technology, "tracking" is defined as "the collection and correlation of data about the Internet activities of a particular user, computer, or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or compliance with law enforcement requests." CTR. FOR DEMOCRACY & TECH., WHAT DOES 'DO NOT TRACK' MEAN? 3, 5 (Jan. 31, 2011), *available at* http://www.cdt.org/files/pdfs/CDT-DNT-Report.pdf.

against a legal mandate.[253] Instead it issued guidelines and principles urging that industry create an "easy to use, persistent, and effective Do Not Track system."[254] However, a centralized DNT approach may be necessary in order to gain meaningful compliance. For example, the European e-Privacy Directive in 2002 mandated that users must be given "clear and comprehensive information" about data tracking and a right to refuse it.[255] This resulted in data trackers allowing users to reject cookies if they could find the instructions to disable a tracking tool burrowed in a website's privacy policy.[256]

2. Regulatory Implementation

It is not clear if any federal agency currently has the authority to implement a centralized transparency and choice portal for political data. The FTC could regulate consumer data brokers and trackers under Section 5 of the Federal Trade Commission Act.[257] However, once the consumer data is sold off to a campaign or political data firm and matched with voter lists, it is not clear that the resulting data would be regulable under the FTC's Section 5 power

---

[253] "[T]he FTC will focus its policy efforts … on vigorously [enforcing] existing laws, [working] with industry on self-regulation, and [continuing] to target its education efforts on building awareness of existing data collection and use practices and the tools to control them." FTC REPORT, *supra* note 34, at ix.

[254] *Id.* at v.

[255] Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37 (July 31, 2002), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

"Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller." *Id.*

[256] The European e-Privacy Directive was later amended to call for opt-in consent. Omer Tene & Jules Polonetsky, *To Track or 'Do Not Track:' Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 308 (2012).

[257] *See* 15 U.S.C. § 45(a)(1) (1994) ("[U]nfair or deceptive acts or practices in or affecting commerce are . . . declared unlawful.").

to regulate "commerce."[258] The Federal Election Commission may also lack jurisdiction. The agency was created to enforce federal campaign finance law[259] through powers specific to campaign finance enforcement.[260] When the FEC regulates in novel areas the courts have applied heightened scrutiny to the action.[261] Regardless, the FEC is notorious for gridlock and dysfunction[262] and may not be a good regulator on that basis alone.

The FTC would be the best agency to regulate computational politics, but doing so will require jurisdictional expansion by Congress. In the past, Congress has expanded the FTC's jurisdiction to enforce privacy under FCRA and COPPA.[263] Today, the FTC's small privacy division only enforces COPPA.[264] Despite the narrow jurisdictional grant, the agency has a good reputation as the de facto federal privacy agency,[265] and given the dysfunctional nature of the FEC, it would be the best candidate for the job.

---

[258] *Id.* The act is only addressed to commercial practices.

[259] "The Commission shall administer, seek to obtain compliance with, and formulate policy with respect to, this Act and chapter 95 and chapter 96 of Title 26. The Commission shall have exclusive jurisdiction with respect to the civil enforcement of such provisions." 52 U.S.C. § 30106(b)(1) (2012).

[260] 52 U.S.C. § 30107 (2014).

[261] "This novel extension of the Commission's investigative authority warrants extra-careful scrutiny from the court because the activities which the FEC normally investigates differ in terms of their constitutional significance from those which are of concern to other federal administrative agencies whose authority relates to the regulation of corporate, commercial, or labor activities." Fed. Election Comm'n v. Machinists Non-Partisan Political League, 655 F.2d 380, 387 (D.C. Cir. 1981).

[262] "The chairwoman of the Federal Election Commission says she's largely given up hope of reining in abuses in raising and spending money in the 2016 presidential campaign and calls the agency she oversees 'worse than dysfunctional.'" *FEC Chair Ann Ravel Says Agency is 'Worse Than Dysfunctional' At Regulating Money in Politics,* HUFFINGTON POST (May 2, 2015), http://www.huffingtonpost.com/2015/05/03/fec-ann-ravel-dysfunctional_n_7197360.html; *see also* Jonathan Backer, *Gridlock and Dysfunction on Display at FEC Oversight Hearing,* BRENNAN CTR. FOR JUSTICE (Nov. 4, 2011), http://www.brennancenter.org/blog/gridlock-and-dysfunction-display-fec-oversight-hearing.

[263] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 602 (2014).

[264] *Id.*

[265] "Today, the FTC is viewed as the de facto federal data protection authority. A data protection authority is common in the privacy law of most other countries, which designate a particular agency to have the power to enforce privacy laws." *Id.* at 600.

B. State Voter Privacy Protections

States enjoy broad authority to regulate access to their public records.[266] In response to the growing data trade, states have implemented some restrictions to public records.[267] Often states exclude access for the commercial uses of soliciting business or marketing services or products.[268] Because state voter registration data is an invaluable resource for political micro-targeters,[269] states are in a position to condition access to records on implementation of basic privacy protections. This could be a useful interim stop-gap to mitigate the harms caused by computational politics while Congress is in legislative dysfunction.[270] Also, in the interest of national uniformity, should Congress choose to legislate in this area, it could easily preempt these laws in the same way that FACTA preempted state credit data laws.[271]

1. State Voter Registration Databases

In response to the 2000 presidential election and Florida recount, Congress passed HAVA,[272] mandating improvements to outdated election procedures across the states. One such mandate was the statewide computerized voter registration list, along with uniform procedures for processing registration data.[273] In the past, voter registration lists were maintained by a patchwork of state and local offices with little computerization, standardization, or real-time access.[274] In some cases, access to voter lists required the right

---

266 Solove, *supra* note 64, at 1169.

267 *See id.*

268 *Id.*

269 *See supra* Part I.C.

270 Thomas Mann & Norman Ornstein, *Yes, Congress is That Bad,* FOREIGN POLICY (Nov. 26, 2012), http://foreignpolicy.com/2012/11/26/yes-congress-is-that-bad/.

271 "Congress chose to permanently extend the preemptions that were established under the 1996 reforms to the FCRA and to institute additional preemptions in areas in which the states had previously been free to regulate." Michael Epshteyn, *The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers?*, 93 GEO. L.J. 1143, 1144 (2005).

272 42 U.S.C. §§ 15301–15545 (2012).

273 Kele Williams, *Key Provisions of the Help America Vote Act*, BRENNAN CTR. FOR JUSTICE (June 20, 2004), http://www.brennancenter.org/sites/default/files/analysis/HAVA%20Fact%20Sheet.pdf.

274 *See* ISSENBERG, *supra* note 62, at 245.

connections—or a willingness to pay.[275] HAVA liberalized access by requiring standardized databases, network computing, and real-time lists accessible by any election official in the state.[276] Easily accessible and electronic records were a significant boon for parties and political data firms.[277] Firms like Voter Vault, Catalist, and Aristotle rely on data to make their targeting and profiling services relevant and up to date,[278] and they offer a suite of comprehensive national voter lists comprised of state voter lists.[279]

2. Conditioning Access to State Voter Databases

States are in a unique position to require basic data protections in exchange for use of voter data. Many states have already implemented prohibitions on the commercial use of voter registration records.[280] For example, "California [allows] voter registration lists [to] be released to candidates, political committees, or for 'election, scholarly, journalistic, political, or governmental purposes.'"[281] However, this likely would not place any restrictions on political data firms accessing data.[282] States could release voter lists on the condition that campaigns and political data firms adopt some privacy protections that will minimize harms caused by a loss

---

[275] "While technically public information, these lists were often jealously controlled by local party bosses. To gain access, a candidate had to have the right connections—or be willing to pay." Verini, *supra* note 55.

[276] Leonard M. Shambon, *Implementing the Help America Vote Act*, 3 ELECTION L.J. 424, 430 (2004).

[277] "As records are increasingly computerized, entire record systems rather than individual records can be easily searched, copied, and transferred. Private sector organizations sweep up millions of records from record systems throughout the country and consolidate those records into gigantic record systems." Solove, *supra* note 64, at 1152; *see also* Nick Judd, *In Year of Political 'Big Data,' NationBuilder Makes Voter Data Free*, TECH PRESIDENT (Sept. 13, 2012), http://techpresident.com/news/22856/year-political-big-data-nationbuilder-makes-voter-data-free; *see also* Evans, *supra* note 10, at 883.

[278] Evans, *supra* note 10, at 883.

[279] Robert L. Mitchell, *Campaign 2012: Mining for Voters*, COMPUTERWORLD (Oct. 29, 2012), http://www.computerworld.com/article/2492578/big-data/campaign-2012—mining-for-voters.html?page=2.

[280] *See* Howard, *supra* note 220, at 166.

[281] Deborah G. Johnson, Priscilla M. Regan, Kent Wayland, *Campaign Disclosure, Privacy and Transparency*, 19 WM. & MARY BILL RTS. J. 959, 965 (2011) (quoting CAL. ELEC. CODE § 2194(a)(2)).

[282] Solove, *supra* note 64, at 1144 n.15

of informational autonomy. Regulations could implement FIPs or a centralized, state-run transparency and choice portal.[283] Or, states could require each political data tracker to adopt a DNT mechanism[284] or require minimum standards for third-party sharing of voter information and the reporting of data breaches.

a) Federal Constitutional Limitations on State Voter Data Protections

The Supreme Court has held that the First Amendment mandates a "right of access" to government documents.[285] In general, the right of access has only been applied to records from criminal proceedings. For example, in *Globe Newspaper Co. v. Superior Court*, the facts involved a Massachusetts law that protected the privacy of juvenile victims of sexual assault by closing all criminal trial proceedings to the public.[286] The Supreme Court held that a "major purpose" of the First Amendment is "to protect the free discussion of governmental affairs."[287] To determine whether the right of access applies, the Court delivered a two-prong test: (1) examine whether the record has "historically . . . been open to the press and general public;" (2) determine whether access "plays a particularly significant role in the functioning of the judicial process and the government as a whole."[288] Lower courts today typically apply the *Globe Newspaper* two-prong test.[289]

The Court has not squarely articulated whether the right of access applies to other state documents and proceedings.[290] However, that is no guarantee that the *Globe Newspaper* test does not extended to other state records.[291] Because the right of access directly implicates the right to knowledge about the government as

---

283 *See supra* Part IV.A.1.

284 *Id.*

285 Solove, *supra* note 64, at 1201 (citing Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980)).

286 Globe Newspaper Co. v. Super. Ct. for Norfolk Cnty., 457 U.S. 596, 598 (1982).

287 *Id.* at 604 (citing Mills v. Alabama, 384 U.S. 214, 218 (1966)).

288 Solove, *supra* note 64, at 1201 (2002) (citing *Globe Newspaper Co.*, 457 U.S. at 605).

289 *See* El Vocero de Puerto Rico (Caribbean Int'l News Corp.) v. Puerto Rico, 508 U.S. 147, 149 (1993) (applying the *Globe Newspaper* test); *see also* United States v. Index Newspapers LLC, 766 F.3d 1072, 1096 (9th Cir. 2014); Solove, *supra* note 64, at 1202.

290 Solove, *supra* note 64, at 1203.

291 *Id.*

an essential component of discourse,[292] the doctrine could easily apply to state voter records. Therefore, in order to survive the *Globe Newspaper* test, a state law that limits access to voter data will need to be narrowly tailored to apply to particular uses[293] and articulate a compelling governmental interest.[294]

Protecting a voter's informational privacy could be a compelling governmental interest. The Constitution requires certain responsibilities for the way the government uses the information it collects.[295] In *Whalen v. Roe*, the Court extended the right to privacy[296] to include personal information collected by the government.[297] At issue in *Whalen* was whether New York State was permitted to record, in a centralized computer database, all of the names and addresses of persons who have been prescribed certain drugs.[298] The plaintiffs argued that the collection and aggregation of personal information on its face violated their right to privacy,[299] but the Court disagreed.[300] However, the Court did clearly articulate that the "zone of privacy" extends to both decisional privacy, defined as "independence in making certain kinds of important decisions,"[301] and informational privacy, defined as "individual interest in avoiding disclosure of personal matters."[302] The Court emphasized that accumulation of vast amounts of personal information in government computerized databases can be a clear threat to an individual's privacy.[303] As a result, states that engage in collection and aggregation of personal information are obligated to avoid embarrassing, harmful, and unwarranted disclosures.[304] Al-

---

292 *Id.*
293 *Id.*
294 *Id.*
295 *Id.*
296 *Id.* at 1204–05.
297 429 U.S. 589, 605 (1977).
298 *Id.* at 591.
299 "Appellees contend that the statute invades a constitutionally protected 'zone of privacy.'" *Id.* at 598.
300 *Id.* at 600.
301 *Id.* at 599–600.
302 *Id.* at 599.
303 *Id.* at 605.
304 "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." *Id.*

though a majority of the circuit courts have now accepted the constitutional right to informational privacy,[305] the right has not developed much since *Whalen*.[306]

However, if a state's voter data limitations are too burdensome, they may potentially be struck down as a violation of the right to vote.[307] In order to determine if a state law is too burdensome on the right to vote, the Supreme Court has employed a balancing test, weighing "the character and magnitude of the asserted injury" against "the precise interests put forward by the State" while considering "the extent to which those interests make it necessary to burden the plaintiff's rights."[308] The Court has explicitly rejected strict scrutiny;[309] instead, it has accepted "reasonable, nondiscriminatory restrictions" as constitutional if the state demonstrates an "important regulatory interest."[310]

States can balance the rights of access and privacy in crafting appropriate voter data protections. As discussed earlier, computational politics can harm a voter's informational privacy, autonomy, and self-determination.[311] As seen in *Whalen*, protecting a citizen's informational privacy can be a valid constitutional prerogative for states. Burdens on the right to vote aside, a state can constitutionally limit access to voter records in exchange for privacy protections. Overall, a state voter data protection regime will have to balance three constitutional interests: (1) the right to access information that plays a significant role in the function of the government; (2)

---

[305] Solove, *supra* note 64, at 1205 n.413.

[306] *Id.*

[307] The Court's fundamental rights jurisprudence has located the right to vote in the Fourteenth Amendment. "The Supreme Court has identified various rights as fundamental based on their importance to ensuring individual liberty and self-governance …. These rights include the right to marry, the right to procreate, the right to interstate travel, and, supposedly, the right to vote." Joshua A. Douglas, *Is the Right to Vote Really Fundamental?*, 18 CORNELL J.L. & PUB. POL'Y 143, 147–48 (2008).

[308] Burdick v. Takushi, 504 U.S. 428, 434 (1992) (citing Anderson v. Celebrezze, 460 U.S. 780, 788 (1983)).

[309] "Election laws will invariably impose some burden upon individual voters. Each provision of a code, whether it governs the registration and qualifications of voters, the selection and eligibility of candidates, or the voting process itself, inevitably affects—at least to some degree—the individual's right to vote and his right to associate with others for political ends." *Id.* at 433.

[310] *Id.* at 434.

[311] *See supra* Parts II.C.1–3.

the right of citizens to be free from harm caused by the dissemination of public records that contain their personal information; (3) the right to be free from unreasonable and discriminatory restrictions on the right to vote.

b) Federal Statutory Limitations on State Voter Data Protections

Limitations on voter list access will not likely run afoul of federal statutory protections. Burdens on the constitutional right to vote aside,[312] states enjoy broad power to regulate the time, place, and manner of elections[313]—which includes the registration and qualifications of voters.[314] However, the federal government may proscribe this authority with new law,[315] and it has frequently done so. Laws like the Voting Rights Act (VRA),[316] HAVA,[317] and the National Voter Registration Act (NVRA)[318] all limit state authority to legislate in this area.

Most relevant for our purposes are the NVRA's requirements that states disclose materials used to produce voter lists. In part, the NVRA requires that states make available for public inspection "all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters."[319] Whether this provision applies to voter lists comprised of active voters—the kind of data sold to campaigns and political data firms[320]—was addressed in *True the Vote* v. *Hosemann*[321] during the 2014 midterm elections.

True the Vote involved a run-off election in the Mississippi Republican primary for U.S. Senate. A tea party challenger appeared

---

312 *See supra* Part IV.B.2.a

313 U.S. CONST. art. I, § 4, cl. 1.

314 Burdick v. Takushi, 504 U.S. 428, 433 (1992).

315 U.S. CONST. art. I, § 4, cl. 1.

316 52 U.S.C. § 10301 (2014).

317 52 U.S.C. § 20507 (2006).

318 52 U.S.C. §§ 20501–11 (2005).

319 52 U.S.C. § 20507(i) (2006).

320 *See supra* Part I.B.

321 No. 3:14-CV-532-NFA, 2014 WL 4273332, at *1 (S.D. Miss. Aug. 29, 2014).

poised to unseat Thad Cochran in the run-off.[322] However, Senator Cochran maintained his seat by a few thousand votes with the help of predominantly African-American Democratic crossover votes.[323] Suspicious of voter fraud, True the Vote (TTV), a Texas-based conservative voter integrity group, sought to inspect Mississippi's election records,[324] including active voter lists.[325] Mississippi law confines inspection of cast ballots to candidates and representatives, but makes no mention of other election materials.[326] Without clear statutory authority, Mississippi's officials refused TTV access in most cases.[327] TTV sued Mississippi under the "public disclosure" provision of the NVRA to gain access and lost.[328] The district court's opinion in part found that the NVRA did not apply to voter lists containing active voters.[329] The court in *Project Vote/Voting for America v. Long* noted that the NVRA's plain meaning and statutory purpose only required disclosure of materials relevant to the carrying out of voter registration activities because they are "the means by which an individual provides the information necessary for the Commonwealth to determine his eligibility to vote."[330] Lists of active voters are not used for maintaining accurate official lists of voters because "[w]hether a voter in 'active'

---

[322] Rebecca Green, *Rethinking Transparency in U.S. Elections*, 75 OHIO ST. L.J. 779, 822–23 (2014).

[323] Nate Cohn & Derek Willis, *More Evidence That Thad Cochran Owes Runoff Win to Black Voters*, N.Y. TIMES, July 15, 2014, http://www.nytimes.com/2014/07/15/upshot/more-evidence-that-thad-cochran-owes-runoff-win-to-black-voters.html.

[324] Emily Wagster Pettus, *US Judge: Voters' Birthdates Are Not Public Record*, WASH. TIMES (Sept. 2, 2014), http://www.washingtontimes.com/news/2014/sep/2/us-judge-voters-birthdates-are-not-public-record/.

[325] *Id.*

[326] MISS. CODE. ANN. § 23-15-271(1) (2012) ("The state executive committee of any political party authorized to conduct political party primaries shall form an election integrity assurance committee for each congressional district.").

[327] "When TTV representatives sought access to election materials at county election clerks' offices, they were met with mixed results. Some counties denied TTV access altogether." Green, *supra* note 322, at 824.

[328] True the Vote v. Hosemann, No. 3:14-CV-532-NFA, 2014 WL 4273332, at *1 (S.D. Miss. Aug. 29, 2014).

[329] *Id.* at *17.

[330] 682 F.3d 331, 336 (4th Cir. 2012) (citing Project Vote/Voting for Am., Inc. v. Long, 752 F.Supp.2d 697, 707 (E.D. Va. 2010)).

status voted or failed to vote in a particular election does not affect that voter's eligibility to vote in future elections."[331]

True the Vote is instructive as to whether the NVRA will preempt state voter data protection laws that limit access to lists of voters. The district court's opinion suggests that a state could limit or even deny access to voter data, so long as the data is not relevant to a state's list maintenance procedures.[332] Whether a state's data is used for list maintenance appears to be factually determined.[333] So long as a state limits or gives conditional access to pure lists of registered voters that can vote on Election Day, there will not likely be an NVRA problem.

CONCLUSION

Computational politics has grown in lockstep with "Big Data" practices seen in advertising and commercial industries that track individuals online and offline with increasing efficiency and effectiveness. As a result, campaigns and the firms they hire are now in possession of a massive trove of PII on hundreds of millions of American voters. In the absence of regulatory oversight, these databases and the tools used to assemble them can harm a voter's informational privacy by allowing campaigns to craft substantial informational asymmetries that make it difficult for voters to predict

---

[331] "Voter statuses do not change as a result of the State's processing of poll books. Whether a voter in 'active' status voted or failed to vote in a particular election does not affect that voter's eligibility to vote in future elections." *True the Vote*, 2014 WL 4273332, at *17.

[332] "Thus, to be subject to disclosure under the NVRA, a record must ultimately concern activities geared towards ensuring that a State's official list of voters is errorless and up-to-date." *True the Vote*, 2014 WL 4273332, at *14; *see also Project Vote*, 682 F.3d at 336 ("The requested applications are relevant to carrying out voter registration activities because they are the means by which an individual provides the information necessary for the Commonwealth to determine his eligibility to vote.") (internal quotations omitted).

[333] *See, e.g., Project Vote*, 682 F.3d at 336 ("[T]he registration applications requested by Project Vote are clearly 'records concerning the implementation of' this 'program and activit[y]' . . . because they are 'the means by which an individual provides the information necessary for the Commonwealth to determine his eligibility to vote' . . . [w]ithout verification of an applicant's citizenship, age, and other necessary information provided by registration applications, state officials would be unable to determine whether that applicant meets the statutory requirements for inclusion in official voting lists.").

when they are being tracked, who is tracking them, and which information has been gathered. This can create serious harms to privacy and democracy in the form of discrimination, redlining, chilling effects on political association, and unaccountable black boxes.

Adopting FIPs and expanding the FTC's jurisdiction to explicitly include political data can minimize these harms. Once given the jurisdictional grant, the FTC can require campaigns and the political data firms they employ to disclose their data at a one-stop-shop web portal designed to disclose what data campaigns have on voters and allow voters to initiate a DNT mechanism. States are also free to craft voter data protection laws due to the immense power they wield in administering and maintaining official lists of voters. When political campaigns and political data firms purchase these lists, the states can condition use on adoption of FIPs or a web portal that discloses data and offers a DNT mechanism. Whether states may freely regulate access to their voter lists will depend on federal constitutional and statutory concerns that could prevent the state from regulating in this area. Overall, states are likely not to run afoul of the federal constitution or laws if their regulations foster transparency and choice and do not implement outright bans on particular uses of political data.