William & Mary Bill of Rights Journal

Volume 19 (2010-2011)
Issue 4

Article 5

May 2011

# Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues

Nichole Rustin-Paschal

# ONLINE BEHAVIORAL ADVERTISING AND DECEPTIVE CAMPAIGN TACTICS: POLICY ISSUES

Nichole Rustin-Paschal*

This Essay examines a set of emerging problems in election law—the increased use of online behavioral advertising to target voters, the failure of the law to address deceptive campaign tactics, and the convergence of these two issues in an Internet-based society.[1] The Essay begins with a discussion of voter suppression and deceptive campaign tactics in the context of behavioral advertising. Part II examines the law surrounding voter fraud, intimidation, and suppression, finding that there is a lack of attention to penalizing voter suppression, particularly at the federal level. Though there are some laws at the state level, more can be done. The Essay concludes by examining, in Part III, how political campaigns have put behavioral advertising to use and offers recommendations for moving forward.

## I. ONLINE BEHAVIORAL TRACKING AND THE POTENTIAL FOR VOTER SUPPRESSION

On July 31, 2010, the *Wall Street Journal* (WSJ) began a series investigating how much information advertisers are able to gather about Internet users.[2] The study found, among other things, that "cookies" are no longer the only method for tracking consumers, the profiles compiled from the tracking data are continually refreshed, providing advertisers with a constant stream of data to be bought and sold, and that the tracking technologies used by companies are often never brought to the attention of consumers.[3] Tracking consumers led advertisers, according to the WSJ, to spend twenty-three billion dollars in the previous year.[4] The specificity of the profiles created by advertisers is so exact, that one consumer, confronted with her online profile, commented that it was "unnerving."[5]

---

* Ph.D. (American Studies, New York University, 1999), J.D. (University of Virginia, 2010); EPIC Open Government Fellow. William & Mary Bill of Rights Journal Symposium: Privacy, Democracy, and Elections, October 22, 2010.

[1] This Essay is drawn from my work on the Electronic Privacy Information Center's 2010 report: ELEC. PRIVACY INFO. CTR., E-DECEPTIVE CAMPAIGN PRACTICES REPORT 2010: INTERNET TECHNOLOGY AND DEMOCRACY 2.0 (Nichole Rustin-Pascal & Sharon Gott Nissim eds. Oct. 2010) [hereinafter E-DECEPTIVE] . The full report, including recommendations on defending against e-deceptive campaign attacks, can be found at http://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf.

[2] *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31–Aug. 1, 2010 (Weekend Magazine), at W1.

[3] *Id.*

[4] *Id.* at W2.

[5] *Id.*

The comments about the WSJ story fall into four broad categories—those who find that the WSJ story serves only to stoke the flames of paranoia surrounding threats to privacy,[6] to others finding that people should take the initiative to be more informed about how to protect themselves from privacy invasive technologies,[7] to those who believe that tracking is the quid pro quo for free content,[8] to those who are grateful for the information provided because, though they may be sophisticated readers and consumers, they may not be as technologically literate as they would prefer.[9] Overlaying most of the comments is an awareness that privacy is at risk when people interact on the Internet.[10]

Indeed, that last category of users is precisely the group that concerned Senator John D. (Jay) Rockefeller (D-W.Va.) in a July 2010 hearing by the Committee on Commerce Science & Transportation on Online Consumer Privacy.[11] Before presenting

---

[6] Brandon Adkins wrote, "WSJ, this is one of the most alarmist pieces I've seen from you. This article extremely overstates the privacy issues surrounding cookies. Cookies have been around . . . oh . . . 10–15 years? Stop acting like you discovered them. Such blatant ignorance." Brandon Adkins, Comment to *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (Aug. 7, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[7] William Drose wrote:

> I very much disagree that cleaning cookies/temp files is a hassle, I've done it for years as I browse and it's second nature. Anyone who uses technology of any sort knows maintenance pays dividends. . . .
> Learn your temp folders and get them wired, whatever OS you use. Then teach all of your friends.

William Drose, Comment to *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (Aug. 1, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[8] Walt Kowalski wrote, "By blocking cookies you block the ability of your favorite content providers to make money. Let's face it—you are not going to pay for that subscription." Walt Kowalski, Comment to *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (Aug. 1, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[9] Susan Thomas wrote, "I can't change the past. But going forward, I think this inspires me to quell mindless internet surfing. . . . This article is good incentive to carry out a larger percentage of my life offline." Susan Thomas, Comment to *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (Aug. 3, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[10] *See* Comments to *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 31–Aug. 7, 2010).

[11] *See* Elizabeth Montalbano, *Google, Facebook, Apple Face Privacy Questions From Senators*, INFORMATIONWEEK (July 28, 2010, 3:04 PM), http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=226300182; *see also Consumer Online Privacy Hearing Before the S. Comm. on Commerce, Sci. & Trans.*, 111th Cong. (2010) [hereinafter *Hearing*, Rockefeller] (statement of John D. Rockefeller IV, Chairman), *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235&Statement_id=21f3326d-345f-4aaa-b105-0532997b481e&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2010.

the panel with several questions, Senator Rockefeller described a world in which individuals are continually tracked as they conduct their daily business—information about books purchased and read, stores entered and products bought, prescriptions filled and shampoos chosen becomes revenue generating data.[12] The businesses collecting this data use it to then build a "personality profile" on the user, predicting future purchases, intellectual interests, and medical issues.[13] Though it may seem "fantastic," Senator Rockefeller stated, the truth is that computers are doing this type of extensive profiling on consumers to provide targeted advertising.[14] Though the advertising might be useful, the data used to compile a portrait of the perfect ad could also be used to design a scam directed at a specific user.[15] Senator Rockefeller asked the witness several questions about the notice consumers have about these practices which track consumers online, while they walk public streets, how much of their personal information is being shared with third parties, what benefits consumers get from this tracking, and what recourse they have to demand greater anonymity from advertisers.[16]

Senator Rockefeller concluded his opening statement with several poignant examples of the users whose welfare he thought was being threatened by the increased use of online behavioral tracking:

> I am talking about ordinary Internet users. I am talking about a 55-year-old coal miner in West Virginia who sends an email to his son in college. I'm talking about a 30-year-old mother who uses her broadband connection to research the best doctor she can take her sick toddler to see. I'm talking about a 65-year-old man who just signed up for a Facebook account so he can view photos of his grandson, and reconnect with old friends.[17]

The value of this story to a discussion of e-deceptive campaign tactics is principally drawing our attention as advocates to the reality that consumers are not equally situated when it comes to threats to voter participation. Unsavvy users compose one group for whom e-deceptive campaign practices are a concern. If they are unaware that their online behavior is being tracked (and consequently do not have the knowledge of how to limit that tracking), then they may be susceptible to campaigns which can aggregate information and direct information at them in a way that will discourage their participation in the voting process.

---

[12] *Hearing*, Rockefeller, *supra* note 11.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

As Gilda Daniels has noted, voter deception has an "amorphous and arguably ambiguous definition,"[18] which few scholars and lawmakers have grappled with substantively.[19] Fraud[20] and intimidation[21] remain the primary focus of the law.[22] The Election Assistance Commission (EAC), Daniels explains, usefully defines election crimes, but only in ways that "tangentially include[ ] deceptive acts."[23] Daniels views voter deception as similar to fraud and intimidation, but also quite distinct from them.[24]

In a report the Electronic Privacy Information Center (EPIC) published on e-deceptive campaign practices, EPIC explained:

> Deceptive campaigns are attempts to misdirect targeted voters regarding the voting process or in some way affect their willingness to cast a vote. Deceptive election activities include false statements about poll place opening and closing times, the date of the election, voter identification rules, or the eligibility requirements for voters who wish to cast a ballot.[25]

The rate of deceptive campaign practices surrounding federal elections has been increasing since the 2000 election.[26] In 2004, Election Protection reported over 1,000 complaints about deceptive practices and voter suppression tactics.[27]

---

[18] Gilda R. Daniels, *Voter Deception*, 43 IND. L. REV. 343, 355 (2010).

[19] *See, e.g.*, Jordan T. Stringer, Comment, *Criminalizing Voter Suppression: The Necessity of Restoring Legitimacy in Federal Elections and Reversing Disillusionment in Minority Communities*, 57 EMORY L.J. 1011, 1011–15 (2008).

[20] *See* CRAIG C. DONSANTO & NANCY L. SIMMONS, U.S. DEP'T OF JUSTICE, FEDERAL PROSECUTION OF ELECTION OFFENSES 24 (7th ed. 2007), *available at* http://www.justice.gov/criminal/pin/docs/electbook-0507.pdf ("Election fraud involves a substantive irregularity relating to the voting act—such as bribery, intimidation, or forgery—which has the potential to taint the election itself.").

[21] *See* 42 U.S.C. § 1971(b) (2006). Voter intimidation can include threats, force, or interference in the voting process making voters afraid to exercise their right to vote. *See* 18 U.S.C. § 594 (2006).

[22] *See* Daniels, *supra* note 18, at 361; A. David Pardo, *Election Law Violations*, 45 AM. CRIM. L. REV. 305, 310–29 (2008) (discussing the statutes that govern voter intimidation and voter fraud).

[23] Daniels, *supra* note 18, at 355.

[24] *Id.*

[25] E-DECEPTIVE, *supra* note 1, at 4.

[26] Daniels, *supra* note 18, at 353; *see also* Tova Andrea Wang, *2004: A Report Card*, *in Special Report: Democracy at Risk*, AM. PROSPECT, Jan. 1, 2005, at A4, A7 (describing deceptive actions in Ohio, including falsely informing newly registered voters that if the NAACP or the John Kerry presidential campaign had registered them, they would be ineligible to vote).

[27] ELECTION PROT., SHATTERING THE MYTH: AN INITIAL SNAPSHOT OF VOTER DISENFRANCHISEMENT IN THE 2004 ELECTIONS 7 (2004), *available at* http://www.866ourvote.org/tools/publications_testimony/files/0002.pdf.

Studies have suggested that deceptive campaigns target voters who are likely to vote, but may be swayed by activity, such as robo-calls or misinformation campaigns, not to vote.[28] Voters may be most susceptible to such tactics during elections that are highly contested.[29] Highly contested elections provide a context for pulling in voters who normally do not vote regularly, and potentially discouraging likely voters who find the tenor of a campaign season difficult. Consider the 2008 election when then Senator Barack Obama (D-IL) stood as the Democratic candidate for president. As the first viable African American presidential candidate, Obama attracted a huge African American following.[30] It is well established that African Americans often vote for democratic candidates[31]—since the likelihood of black voters not voting for Obama was so great, deceptive campaigns targeting them, particularly black women who represented for the first time the highest participation of any voting block,[32] would have been reasonable. The goal would have been to keep these voters away from the polls in order to affect the election results. But at the close of polls, researchers found that 95% of black voters voted for Obama.[33]

Suppression campaigns that target African-American voters will likely impact their participation in the electoral process by intimidating them from exercising a constitutional right by affecting their confidence in the electoral process. Suppression campaigns can also affect the success of a party at the polls during a highly contested election.[34] Exercising the right to vote evinces an individual's or a group's stake in fully participating in our democracy as citizens.[35] Suppression tactics effectively turn that desire to participate into skepticism about an individual's or group's value in the democratic process.[36] As Jordan Stringer writes, "[T]he voting system becomes

---

[28] *See* E-DECEPTIVE, *supra* note 1, at 9.

[29] *See id.* at 4.

[30] *See* Claire Cohen, *Breakdown of Demographics Reveals How Black Voters Swept Obama into White House*, DAILY MAIL (Nov. 5, 2008, 6:33 PM) http://www.dailymail.co.uk/news/worldnews/article-1083335/Breakdown-demographics-reveals-black-voters-swept-Obama-White-House.html.

[31] *See* PEW RESEARCH CTR. FOR THE PEOPLE & THE PRESS, THE 2004 POLITICAL LANDSCAPE: EVENLY DIVIDED AND INCREASINGLY POLARIZED 6 (2003), *available at* http://people-press.org/files/legacy-pdf/196.pdf ("Compared with other demographic groups, African Americans are by far the strongest supporters of the Democratic party.").

[32] MARK HUGO LOPEZ & PAUL TAYLOR, PEW RESEARCH CTR. FOR THE PEOPLE & THE PRESS, DISSECTING THE 2008 ELECTORATE: MOST DIVERSE IN U.S. HISTORY 5 (2009), *available at* http://pewresearch.org/pubs/1209/racial-ethnic-voters-presidential-election.

[33] Cohen, *supra* note 30.

[34] *See* Sherry A. Swirsky, *Minority Voter Intimidation: The Problem That Won't Go Away*, 11 TEMP. POL. & CIV. RTS. L. REV. 359, 360 (2002) (noting that voter intimidation efforts "exploit a political culture in which participation by minority, poor and uneducated voters too often has been devalued, even by these voters themselves").

[35] Stringer, *supra* note 19, at 1021.

[36] *See id.*

corrupted not only when laws are repeatedly broken but also when voters *perceive* that they are being victimized by a voting system that is vulnerable to coercive and discriminatory effects."[37]

The primary targets for voter suppression have typically been members of low-income, racial and language minorities, young first-time voters, the disabled, and the elderly.[38] Campaigns which target these communities develop messages that play on their insecurities. For example, people who are undergoing foreclosures may believe deceptive campaign strategies that claim these people are ineligible to vote.[39] This is not the case.[40] Another regularly used tactic is asserting the need to protect against voter fraud.[41] Statistically, voter fraud almost never occurs but, as a scare tactic, it does provide a way to galvanize voters and poll workers to "protect" the integrity of the process.[42] Poll workers might challenge the eligibility of language-minority voters because of fears about who may be voting.[43] The result might be the turning away of eligible voters.[44] Tova Wang has described this "ginning up [the] bogeyman" of voter fraud as a way to "intimidate certain groups of voters and, ultimately, make it harder for minority or disadvantaged groups to exercise their right to vote. It is no accident that these operations have repeatedly focused on minority communities."[45]

Consider some of the following attempts at suppressing minority voter participation. They range from circulating fraudulent ballots,[46] to directing robo-calls

---

[37] *Id.*

[38] *See, e.g.*, BRIAN FREEMAN ET AL., VOTER SUPPRESSION: NEW HAMPSHIRE'S RESPONSE TO A NATIONAL PROBLEM 5–7 (2009), *available at* http://rockefeller.dartmouth.edu/shop/PRS Policy Brief 0809-02.pdf. For a discussion of how voter intimidation tactics are rooted in the racial and class based efforts to limit the vote see TRACY CAMPBELL, DELIVER THE VOTE: A HISTORY OF ELECTION FRAUD, AN AMERICAN POLITICAL TRADITION, 1742–2004, at 133–34 (2005); ALEXANDER KEYSSAR, THE RIGHT TO VOTE: THE CONTESTED HISTORY OF DEMOCRACY IN THE UNITED STATES 258–59 (2000); NAT'L COMM'N ON THE VOTING RIGHTS ACT, PROTECTING MINORITY VOTERS: THE VOTING RIGHTS ACT AT WORK 1982–2005, at 307–10 (2006), *available at* http://www2.ohchr.org/english/bodies/hrc/docs/ngos/lccr2.pdf; PEOPLE FOR THE AM. WAY FOUND., THE LONG SHADOW OF JIM CROW: VOTER INTIMIDATION AND SUPPRESSION IN AMERICA TODAY (2004), *available at* http://www.pfaw.org/sites/default/files/thelongshadowofjimcrow.pdf.

[39] E-DECEPTIVE, *supra* note 1, at 4.

[40] *See id.*

[41] *See generally* JUSTIN LEVITT, BRENNAN CTR. FOR JUSTICE, THE TRUTH ABOUT VOTER FRAUD (2007), *available at* http://www.truthaboutfraud.org/pdf/TruthAboutVoterFraud.pdf.

[42] Tova Andrea Wang, *Voter Fraud Hysteria*, POLITICO (Nov. 1, 2010 10:17 AM), http://www.politico.com/news/stories/1110/44478.html.

[43] *See id.*

[44] *Id.*

[45] *Id.*

[46] *See, e.g.*, News Release, Maryland Attorney General's Office, Attorney General Gansler Obtains Restraining Order to Halt Distribution of Fraudulent Campaign Ballot, (Sept. 7, 2010), http://www.oag.state.md.us/Press/2010/090710.htm; *see also* E-DECEPTIVE, *supra* note 1, at 11.

announcing faulty voter registration information to primarily African-American households,[47] to distributing campaign fliers with altered images and misrepresentations of the policy positions of a candidate to his targeted voters.[48]

Deceptive campaigns often adapt to and follow the technologies available to them. In an increasingly information-based society, deceptive campaigns will likely be launched in ways that take advantage of tools provided by web-based technologies for communicating and organizing.[49] The challenge will be identifying the perpetrators of the campaigns. EPIC identified how computer fraud practices such as "spoofing," "phishing," "pharming," "denial of service," "rumor mongering," and "social engineering," could be used in deceptive campaigns.[50] These tactics rely on voters being unsophisticated computer and Internet users who may have difficulty distinguishing between genuine and fraudulent Internet communications.

During an election period, voters may turn to search engines, social networking sites, and websites to get information about candidates and the issues.[51] Deceptive campaigns could, for example, create websites that misuse government insignia and provide unknowing voters wrong information about registration requirements or polling locations.[52] Alternatively, legitimate sites may be compromised by campaigns that try to overload the system through denial of service attacks, leaving voters without access to important and timely election information.[53] The threat of malware or phishing emails or the exposure of personally identifiable information to identity thieves may discourage voters from participating in organizing efforts or even voting.[54]

## II. THE LEGAL CHALLENGES OF INTERNET ENABLED POLITICAL PARTICIPATION

The decentralized and open nature of the Internet makes it central to contemporary efforts to organize and educate voters.[55] At least 24% of Americans turned to the

---

[47] Bniolet, *Elections Board Hunting Robocaller*, NEWS OBSERVER (Apr. 28, 2008, 4:45 PM), http://projects.newsobserver.com/under_the_dome/elections_board_hunting_robocaller; *see also* E-DECEPTIVE, *supra* note 1, at 12.

[48] Deirdre Fernandes, *Oberndorf Campaign Files Complaint on Sessoms-Obama Flier*, VIRGINIAN-PILOT ( Nov. 29, 2008), http://hamptonroads.com/2008/11/oberndorf-campaign-files-complaint-sessomsobama-flier; Alex Koppelman, *Voter Suppression in North Carolina?*, SALON (May 2, 2008, 4:46 PM), http://www.salon.com/politics/war_room/2008/05/02/robocalls; *see also* E-DECEPTIVE, *supra* note 1, at 12.

[49] E-DECEPTIVE, *supra* note 1, at 12–16.

[50] *Id.* at 14–15.

[51] *Id.* at 16–17.

[52] *Id.* at 17.

[53] *Id.* at 18–19.

[54] *Id.* at 15.

[55] Internet Communications, 71 Fed. Reg. 18,589, 18,590–91 (Apr. 12, 2006) (to be codified at 11 C.F.R. pts. 100, 110, 114); Misha Glenny, *Who Controls the Internet*, FINANCIAL

Internet for information in the 2008 Presidential election.[56] Voters can access the Internet from smart phones and other smart devices such as the iPad, as well from desktop and laptop computers.[57] Information can be disseminated via blogs, texts, tweets, mobile ads and web pages. With over 74% of American adults using the Internet,[58] (many of them from mobile devices)[59] information is portable and easily accessible.

These forms of communication serve not only to bring people together, but to launch deceptive campaigns. Robo-calls, for instance, take advantage of new web-based technology to barrage voters with automated political messages which can be used to misdirect voters.[60] In 2006, voters in Missouri, Virginia, Arizona, and Maryland reported receiving numerous robo-calls falsely informing them that, among other things, their polling places had changed and that their registrations were cancelled making them ineligible to vote.[61]

Because of the fluid and decentralized nature of the Internet, enforcement of laws regulating political activity face a number of challenges. Federal and state laws are not easily mapped onto Internet communications. New strategies are needed to address the gaps. Campaign finance laws, for example, are beginning to be adapted to reflect the limitations of Internet advertising. Florida has recently updated its laws related to political advertising.[62] Prior to the change, Florida state law required that candidates disclose within the ad that it is a political ad, the source paying for the ad, whether the candidate approved the ad, and the office being sought by the candidate.[63] An ad placed in a traditional print medium would provide sufficient space for all of this information. However, Internet-based ads may not. For example, a St. Petersburg mayoral

---

TIMES (Oct. 8, 2010, 11:40 PM), http://www.ft.com/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html.

[56] PEW RESEARCH CTR. FOR THE PEOPLE & THE PRESS, SOCIAL NETWORKING AND ONLINE VIDEOS TAKE OFF: INTERNET'S BROADER ROLE IN CAMPAIGN 2008, at 21 (2008), *available at* http://www.pewinternet.org/Reports/2008/The-Internet-Gains-in-Politics/Summary-of-Findings.aspx.

[57] E-DECEPTIVE, *supra* note 1, at 16.

[58] AARON SMITH, PEW INTERNET &AMERICAN LIFE PROJECT, THE INTERNET'S ROLE IN CAMPAIGN 2008 (Apr. 15, 2009), *available at* http://www.pewinternet.org/Reports/2009/6--The-Internets-Role-in-Campaign-2008.aspx.

[59] LEE RAINIE, PEW INTERNET & AMERICAN LIFE PROJECT, INTERNET BROADBAND AND CELL PHONE STATISTICS (2010), *available at* http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[60] *See* Charles Babington & Alec MacGillis, *It's a Candidate Calling. Again. Republicans Deny Subterfuge as Phone Barrages Anger Voters*, WASH. POST, Nov. 7, 2006, at A8.

[61] ROBIN CARNAHAN, VOTERS FIRST: AN EXAMINATION OF THE 2006 MIDTERM ELECTION IN MISSOURI 17 (2007), http://www.sos.mo.gov/elections/VotersFirst/2006/VoterFirst-Complete.pdf; Deborah Barfield Berry, *Dems To Target Political 'Robo Calls*,*'* USA TODAY (Nov. 11, 2006, 9:21 PM), http://www.usatoday.com/news/washington/2006-11-20-dems-robo-calls_x.htm.

[62] *See* FLA. STAT. ANN. § 106.143 (West 2010).

[63] *See* E-DECEPTIVE, *supra* note 1, at 12.

candidate, Scott Wagman, turned to Google Adwords to advertise his 2009 campaign.[64] Google Adwords links ads and keywords so that a particular ad will appear whenever a search is run using those terms.[65] Wagman linked his ad to search terms including his opponents' names.[66] Wagman was charged with violating Florida's campaign finance laws because the full disclosure was not included in the character-limited Google ad.[67] The lawsuit was thrown out eventually.[68] However, the real result was the Florida legislature amending its disclosure requirement to account for the special context of online advertising.[69]

The efficiency of the early Internet, with its small number of users,[70] did not require much attention to be spent on its security features nor on tight administration of communication flows. The decentralized nature of the Internet, with fluid national and state borders, means that creating laws to govern the Internet remains fraught with numerous tensions.[71] In the context of administering elections, ensuring that eligible voters participate, and policing voter suppression techniques are even more difficult. "The enforcement of campaign regulations regarding political mail and telephone communications would likely be very intrusive in cyberspace unless designed carefully and supported by the active participation of users, nonprofits, governments, and commercial interests."[72] Helping voters get redress against online deceptive campaigns is a difficult task. While voter intimidation has been penalized under the Hatch Act,[73]

---

[64] *Id.* at 12–13.

[65] *Id.* at 12.

[66] *See* Christina Silva, *Scott Wagman to Fight Online Ad Complaint in a Case That Could Set Precedent*, ST. PETERSBURG TIMES (Aug. 11, 2009), *available at* http://www.tampabay.com/news/politics/KYC/scott-wagman-to-fight-online-ad-complaint-in-a-case-that-could-set/1026451; *Internet Campaigning*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=21244 (last visited Apr. 10, 2011).

[67] E-DECEPTIVE, *supra* note 1, at 13.

[68] *Id.*

[69] *See* Kate Kaye, *Florida's New Political Ad Law Could Drive Dollars from State Candidates Online*, CLICKZ (June 2, 2010), http://www.clickz.com/clickz/news/1726249/floridas-new-political-ad-law-could-drive-dollars-state-candidates-online; *see also*, *Internet Campaigning*, *supra* note 66.

[70] *Factsheet: A Brief History of NSF and the Internet*, NAT'L SCI. FOUND. (Aug. 13, 2003), http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050; *see also* Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOCIETY, http://www.isoc.org/internet/history/brief.shtml (last visited Apr. 10, 2011).

[71] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD, at viii (2006).

[72] E-DECEPTIVE, *supra* note 1, at 13–14; *see also Cybersecurity Privacy, Practical Implications*, ELEC. PRIVACY INFO. CTR, http://epic.org/privacy/cybersecurity/default.html (last visited Apr. 10, 2011).

[73] The Hatch Act makes it illegal to intimidate voters in federal elections to:

> [I]ntimidate[ ], threaten[ ], coerce[ ] or attempt[ ] to intimidate, threaten or coerce any other person for the purpose of interfering with the right

there is no federal law making deceptive tactics illegal.[74] Though some steps have been taken to enact legislation addressing this gap in election law, they have ultimately been unsuccessful.

In the 110th Congress, then Senator Barack Obama (D-IL) and Senator Charles Schumer (D-NY) introduced the Deceptive Practices and Voter Intimidation Prevention Act of 2007 which would have criminalized voter deception and increased, for those convicted of voter intimidation, the sentence served from one year to five years or a fine of $100,000, or both.[75] Additionally, the bill provided that private parties could initiate suits in court and required that the Attorney General's office investigate allegations of voter deception.[76] The Attorney General had the additional burden of correcting information for voters who were affected by the deceptive campaign tactic, referring any matter under the Department of Justice's (DOJ) Civil Rights Division to appropriate authorities for prosecution, and referring the case to federal or state authorities for prosecution after the election.[77] The bill prohibited providing misinformation about election times, voter qualifications, voter registration status, political endorsements, and criminal penalties associated with voting.[78]

Following the failure of that bill to move ahead, Representative John Conyers (D-MI) introduced a bill, H.R. 97, in the 111th Congress to address the gap in election protection law.[79] The bill would have required the Attorney General, after determining that there was a reasonable basis to find the occurrence of deceptive practices, to "undertake all effective measures necessary to provide correct information to voters affected by the false information" and to refer all credible allegations to the DOJ's Civil Rights Division and to other federal and state authorities for criminal prosecution or civil action post election.[80] The bill also would have required that the Attorney

---

> of such other person to vote or to vote as he may choose, or of causing such other person to vote for, or not to vote for, any candidate for the office of President, Vice-President, Presidential elector, Member of the Senate, member of the House of Representatives . . . at any election held solely or in part for the purpose of electing such candidate, shall be fined under this title or imprisoned not more than one year, or both.

18 U.S.C. § 594 (2006).

[74] For further discussion of election law offenses and statutes, *see* David Pardo, *Election Law Violations*, 45 AM. CRIM. L. REV. 305, 307 (2008); David C. Rothschild & Benjamin J. Wolinsky, *Election Law Violations*, 46 AM. CRIM. L. REV. 391 (2009).

[75] Deceptive Practices and Voter Intimidation Act of 2007, S. 453, 110th Cong. §§ 1, 3; *see also* Stringer, *supra* note 19, at 1042–43; Seth Stern, *Obama-Schumer Bill Proposal Would Criminalize Voter Intimidation*, N.Y. TIMES (Jan. 31, 2007), http://www.nytimes.com/cq/2007/01/31/cq_2213.html.

[76] Deceptive Practices and Voter Intimidation Act of 2007, S. 453, 110th Cong. § 4.

[77] *Id.* § (4)(b)(1).

[78] *Id.* § (3)(a)(2)(C).

[79] Deceptive Practices and Voter Intimidation Act of 2009, H.R.97, 111th Cong.

[80] *Id.* § 5(b)(1)(A).

General consult with a variety of experts, including voting rights groups, local election officials, and civil rights groups when promulgating rules defining the provision of correct information to voters.[81] However, with the 2010 mid-term elections, a new Congress will be sworn in, requiring that a bill like H.R. 97 be reintroduced.

The Civil Rights Act of 1957 created the Civil Rights Division of the DOJ and authorized it to sue on behalf of black Americans who were being harassed and denied their right to vote.[82] Subsequent enforcement of the Civil Rights Act was inconsistent. "[C]ourts reached different conclusions regarding its application to private individuals' conduct, state elections, and enforcement by private litigants, effectively denying adequate protection to intimidated voters."[83] Congress passed the Voting Rights Act of 1965 (VRA) to address some of the enforcement flaws in the Civil Rights Act.[84] Although the Civil Rights Act provides that no one "shall intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce any other person" by intending to obstruct their right to vote,[85] the VRA prohibits any "voting qualification or prerequisite to voting or standard, practice, or procedure . . . which results in a denial or abridgment of the right of any citizen of the United States to vote on account of race or color."[86] The VRA extends protections beyond elections involving federal candidates to include elections in "any State, Territory, district, county, city, parish, township, school district, municipality, or other territorial subdivision."[87] Nevertheless, the VRA has not been as effective an enforcement mechanism as was hoped.[88] Voter suppression in the form of deceptive tactics remains an untouched violation for the DOJ.[89]

---

[81] *Id.* § 5(b)(2).

[82] *Voting Rights Act Timeline*, AM. CIVIL LIBERTIES UNION, http://www.aclu.org/voting-rights/voting-rights-act-timeline (last visited Apr. 10, 2011); Civil Rights Division, U.S. DEPT. OF JUSTICE, http://www.justice.gov/crt/ (last visited Apr. 10, 2011).

[83] Stringer, *supra* note 19, at 1023.

[84] *Id.* at 1024.

[85] 42 U.S.C. § 1971(b) (2006).

[86] *Id.* § 1973(a).

[87] *Id.* § 1971(a)(1).

[88] *See* Stringer, *supra* note 19, at 1024–25 (noting that the "'flexible, fact-intensive test' allowed courts to exercise considerable discretion" about whether an "invidious purpose" motivated the suppression tactics, whether an invidious purpose was sufficient if there was no showing of compelling discriminatory effects, and that the VRA left no remedies for plaintiffs); *see also* Rogers v. Lodge, 458 U.S. 613, 628 n.10 (1982) (declining to address the VRA claim); NAACP v. Gadsden Cnty. Sch. Bd., 691 F.2d 978, 981 n.4 (11th Cir. 1982) (resolving the case on equal protection grounds and declining to address the VRA's applicability); United States v. Harvey, 250 F. Supp. 219, 237 (E.D. La. 1966) (finding that plaintiffs failed to prove their claim under the VRA); Barbara Arnwine, *Voting Rights at a Crossroads: Return to the Past or an Opportunity for the Future*, 29 SEATTLE U. L. REV. 201, 303 (2005) ("This state of affairs is especially shocking when one considers the hope that existed with the passage of the 1965 Voting Rights Act.").

[89] *See* DONSANTO & SIMMONS, *supra* note 20, at 61.

The DOJ recognizes the significance of voter suppression and defines the elements of voter suppression, even as it notes that there is no federal statute to prosecute voter suppression: "Voter suppression schemes are designed to ensure the election of a favored candidate by blocking or impeding voters believed to oppose that candidate from getting to the polls to cast their ballots."[90] The DOJ Criminal Division prosecutes election offenses under 18 U.S.C. § 241 which makes it a felony to impede the exercise of a right or privilege, such as voting, protected by the Constitution or United States law.[91] If the DOJ brings a case under this statute, it has the burden of proving a "specific intent to violate constitutional rights."[92] Specific intent requires that the violation be the "predominant purpose" of the actions giving rise to the suit.[93] The DOJ has not yet prosecuted a deceptive campaign under this statute, but has successfully prosecuted one party official.[94] The DOJ still has recourse to civil penalties under 42 U.S.C. § 1971(b)[95]

---

[90] *Id.* The examples provided

> include providing false information to the public—or a particular segment of the public—regarding the qualifications to vote, the consequences of voting in connection with citizenship status . . . the date of an election, the hours for voting, or the correct voting precinct. Another voter suppression scheme, attempted recently with partial success, involved impeding access to voting by jamming the telephone lines of entities offering rides to the polls in order to prevent voters from requesting needed transportation.

*Id.*

[91] *See id.* at 37–40 (discussing prosecutions under § 241). The language of the statute reads:

> If two or more persons conspire to injure, oppress, threaten, or intimidate any person . . . in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States, or because of his having so exercised the same . . .
>
> . . .
>
> They shall be fined under this title or imprisoned not more than ten years, or both . . . .

18 U.S.C. § 241 (2006).

[92] United States v. Ellis, 595 F.2d 154, 161–62 (3d Cir. 1979) (citing United States v. Guest, 383 U.S. 745, 753–54 (1966); Screws v. United States, 325 U.S. 91, 101 (1945)).

[93] *See Guest*, 383 U.S. at 760.

[94] *See* Daniels, *supra* note 18, at 362–63 (discussing United States v. Tobin, No. 04-CR -216-01-SM, 2005 WL 3199672, at *1, *3 (D.N.H. Nov. 30, 2005)).

[95] The statute reads:

> No person, whether acting under color of law or otherwise, shall intimidate, threaten, coerce, or attempt to intimidate, threaten, coerce any other person for the purpose of interfering with the right of such other person to vote or to vote as he may choose, or of causing such other person to vote for, or not to vote for any candidate for the office of President, Vice President, presidential elector, Member of the Senate, or Member of the House of Representatives, Delegates, or Commissioners from the Territories or possessions, at any general, special, or primary election

and Section 11(b) of the Voting Rights Act.[96] However, there has been little litigation under these statutes.[97]

Some federal laws may be useful to reach cases in which federal election law has been unsuccessful in combating deceptive campaigns. in. The Phone Harassment Statute prohibits the making of a telephone call or utilization of a telecommunications device "whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications."[98] Additionally, the Phone Harassment Statute criminalizes activity that "makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number."[99] The federal mail-fraud statute criminalizes a "scheme or artifice to defraud" through use of the mails to further the scheme and with the purpose of "obtaining money or property."[100]

Approximately thirty-nine states have, however, passed laws addressing deceptive campaign tactics, such as distributing false information about election administration, candidates or issues, a combination of both or interference with the voting process.[101] For example, Missouri's 2006 law prohibits "Knowingly providing false information about election procedures for the purpose of preventing any person from going to the polls."[102] Arizona makes it unlawful to knowingly, by "fraudulent device or contrivance whatever, to impede, prevent or otherwise interfere with the free exercise of the elective franchise of any voter . . . ."[103] Illinois makes it a felony if an individual or co-conspirator "by force, intimidation, threat, deception or forgery, knowingly prevents

---

> held solely or in part for the purpose of selecting or electing any such candidate.

42 U.S.C. § 1971(b) (2006). Section 1971(c) authorizes the Attorney General to bring civil actions for "preventive relief" against violations of § 1971. *Id.* § 1971(c).

[96] This section reads:

> No person, whether acting under color of law or otherwise, shall intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any other person for voting or attempting to vote, or intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for urging or aiding any person to vote or attempt to vote, or intimidate . . . .

Voting Rights Act of 1965, Pub. L. No. 89-110, 79 Stat. 437, 443 (codified at 42 U.S.C. § 1973i(b) (2006)).

[97] *See* Daniels, *supra* note 18, at 359–61, 363–69.

[98] *See* 47 U.S.C. § 223(a)(1)(C) (2006).

[99] *Id.* § 223(a)(1)(D).

[100] *See* 18 U.S.C. § 1341 (2006).

[101] *See* Daniels, *supra* note 18, at 369.

[102] MO. REV. STAT. § 115.631(26) (LexisNexis 2010); *see also* COMMON CAUSE & DEMOS, VOTING IN 2010: TEN SWING STATES (2010), *available at* http://www.demos.org/swingstate/2010swing_exec_FINAL.pdf.

[103] ARIZ. REV. STAT. § 16-1013(A)(2) (2010).

any person from . . . lawfully voting . . . ."[104] Though the language in these state statutes tends to be broad, the statutes do provide some measure of protection for voters and should be used to combat deceptive campaign tactics.

Election protection efforts have focused on the ways that deceptive campaign tactics used traditional mediums such as "telephone calls, ballot challenges, direct mail, and canvass literature drops" to suppress the vote.[105] These types of campaigns required longer periods to be executed; Internet-based communications makes execution practically instantaneous, and seemingly under the guise of authoritative channels. The hacking of George Mason University's Provost's e-mail on Election Day 2008, advising students that Election Day had been postponed,[106] shows the ease with which trusted networks can be compromised and become the source of suppression tactics.[107]

Some states have laws that address deceptive campaigns that use Internet-based technologies to target a group for voter suppression.[108] These laws could and should be combined with other state statutes to effectively prosecute offenders, for example, with voting rights laws, laws prohibiting false statements and deceptive practices, laws prohibiting tampering with election or campaign materials, laws prohibiting the impersonation of public officials, laws prohibiting the unauthorized use of state seals and insignia, and anti-hacking and computer crime laws.[109] Michigan, for example, has an anti-hacking statute that makes it unlawful for a person to access a computer program, computer, computer system, or computer network to "devise or execute a scheme or artifice with the intent to defraud . . . ."[110]

## III. PROFILING FOR VOTER SUPPRESSION

The Federal Trade Commission (FTC) defines online behavioral advertising as "the tracking of a consumer's online activities over time—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to

---

[104] 10 ILL. COMP. STAT. ANN. § 5/29-4 (LexisNexis 2011); *see also id.* § 5/29-18 (prohibiting conspiracy to prevent voting). Other states with similar laws include Colorado, Kentucky, Louisiana, and Nevada. *See* COLO. REV. STAT. § 1-13-713 (2010); KY. REV. STAT. ANN. § 119.155 (LexisNexis 2010); LA. REV. STAT. ANN. § 18:1461(A)(6) (2010); NEV. REV. STAT. ANN. § 293.710 (LexisNexis 2010). Further discussion can be found in COMMON CAUSE ET AL., DECEPTIVE PRACTICES 2.0: LEGAL AND POLICY RESPONSES (2008), *available at* http://www.commoncause.org/deceptivepracticesreport.pdf [hereinafter DECEPTIVE PRACTICES 2.0].

[105] E-DECEPTIVE, *supra* note 1, at 5 (citing ELECTION PROT., REPORT ON THE LEGAL PROGRAM TO BOARD OF DIRECTORS AND TRUSTEES, STAFF, AND PRO BONO PARTNERS (2006), *available at* http://www.866ourvote.org/tools/publications_testimony/files/0003.pdf).

[106] Thomas Frank & Richard Wolf, *Pranks, Mischief Reach Higher Level at Colleges*, USA TODAY, Nov. 5, 2008, at 10A; Brian Krebs, *GMU E-Mail Hoax: Election Day Moved to Nov. 5*, WASH. POST (Nov. 4, 2008, 10:16 AM), http://voices.washingtonpost.com/securityfix/2008/11/gmu_e-mail_hoax_election_day_m.html.

[107] *See* E-DECEPTIVE, *supra* note 1, at 5.

[108] DECEPTIVE PRACTICES 2.0, *supra* note 104, at 5.

[109] *Id.* at 5–8, 11, 14–15, 18–22.

[110] MICH. COMP. LAWS SERV. § 752.794 (LexisNexis 2011).

deliver advertising targeted to the individual consumer's interests."[111] This definition excludes "first party" advertising where no data is shared with third parties and contextual advertising, which is targeting based on a user's single visit to a single web page.[112] Contextual advertising is to be construed very narrowly—if information is collected and stored for use at a later time, it is no longer contextual advertising.[113]

Further, the FTC found that personally identifiable information (PII) is becoming an increasingly expansive category of data.[114] PII, which links individual consumers to data about online activities, can include wi-fi information, IP addresses, Social Security numbers, and passwords.[115] The FTC proposed four principles for self-regulation of online behavioral targeting, especially when PII data is being collected. The principles include, 1) transparency and control, 2) "reasonable security and limited data retention," 3) "affirmative express consent from affected consumers" before material changes are made to privacy policies, and 4) "affirmative express consent" from the consumer when companies plan to use sensitive data for their advertising.[116]

Enforcement of these principles, the FTC notes, requires industry to do much more to limit the use of PII and the invasiveness of behavioral tracking.[117] "Meaningful enforcement mechanisms" should be the goal of all industry.[118] The report states, "Self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences."[119] Industry self-regulation may have little impact on unscrupulous individuals who are able to buy a company's data on consumers and use that information to suppress voter participation in an election.

The amount of PII circulating on the Internet facilitates the building of profiles of voters for whom targeted political messages can be built and directed.[120] Advertisers and political campaigns often draw on the same types of data to create profiles that illuminate the different aspects of individual lives and identities, including military active duty status, property ownership, and employment status.[121]

> Campaigns collect this data from voter registration applications, voters' history of participation, state-issued professional licenses,

---

[111] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 46 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter FTC REPORT].

[112] *Id.* at 26.

[113] *See id.* at 30.

[114] *Id.* at 22–23; *see also An Interview with David Vladeck of the F.T.C.*, N.Y. TIMES (Aug. 5, 2009, 2:24 AM), http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/.

[115] *See* FTC REPORT, *supra* note 111, at 20–22 & n.47.

[116] *Id.* at 46–47 (capitalization omitted).

[117] *See id.* at 47.

[118] *Id.*

[119] *Id.*

[120] *See* E-DECEPTIVE, *supra* note 1, at 9.

[121] *See id.*

> and low-level elected office holders. Profiles are used to develop expectations regarding the behavior of individuals based on their activities, preferences for a wide range of products and services, personal associations, religious beliefs, past political participation, type of work, neighborhood, place of birth, and level of education.[122]

Until recently, Virginia had limited access to voter information, including PII and history of participation in elections, only to "elected officials, candidates and party chairmen."[123] A court decision found that this state law was unconstitutional under the theory that it limited free expression and violated equal protection of the law principles.[124] The court left undecided whether the information, which the plaintiffs intended to use to target individual voters with their history of election participation as a means of pushing them to the polls, could also be used to let people other than the voter know their record of participation.[125] "Few voters are aware of how much information about the details of their lives is in the hands of third parties."[126]

Greater influxes of cash into elections enable campaigns to drill down into voter interests and new businesses to develop which work under the model of providing the most individualized and expansive lists of voters for targeted messaging.[127] Profiles of consumer behavior are often predictive of future behavior—these profiles are bought and sold between retailers, advertisers, and increasingly, data brokers who may sell the profiles to campaigns.[128] These profiles are often easily linked with the Internet

---

[122] *Id.* (citing Bob Blaemire, *Campaigns and Voter Profiles*, C-SPAN (Dec. 29, 2009), *available at* http://www.c-spanvideo.org/program/290960-3).

[123] Bill Sizemore, *Judge Expands Access to Virginians' Voting Records*, VIRGINIA-PILOT, (Feb. 17, 2011), http://hamptonroads.com/2011/02/judges-ruling-expands-access-virginians-voting-records.

[124] *Id.*

[125] *See id.*

[126] E-DECEPTIVE, *supra* note 1, at 9 (citing T.W. Farnam & Dan Eggen, *Interest-Group Spending for Midterm Up Fivefold From 2006; Many Sources Secret*, WASH. POST, Oct. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/03/AR2010100303664.html).

[127] *See id.* at 9–10 (citing Thomas Fitzgerald, *Parties Pin Hopes on Voter Profiling*, BRADENTON HERALD, Nov. 2, 2006, at 3; Michael D. Shear, *Va. Gubernatorial Candidates Use Data to Zero In on Voters*, WASH. POST, Aug. 28, 2005, at C1; Jacqui Cheng, *Government Relies on Facebook 'Narcissism' to Spot Fake Marriages, Fraud*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2010/10/govt-takes-advantage-of-facebook-narcissism-to-check-on-users.ars (last visited Apr. 10, 2011); *Voter Vault*, FILPAC, http://www.filpac.com/votervault.htm (last visited Apr. 10, 2011)).

[128] *See id.* at 10 (citing Press Release, Markey, Barton Release Responses from Web Sites on Their Tracking of Consumer Behavior (Oct. 8, 2010), http://markey.house.gov/index.php?option=content&task=view&id=4103&Itemid=125; *Behavioral Targeting to Grow: The Mixing and Mining of Audience Data Becomes More Important to Advertisers*, ADWEEK

Protocol (IP) address of the device used to make a purchase, sign a petition, or access a social networking site, making the user personally identifiable.[129]

As EPIC noted in its recent report, the 2008 Presidential Election marked the first time that campaign strategists turned to behavioral targeting and micro-targeting to build their voter profiles.[130] EPIC drew attention to two companies, TargetPoint Consulting and Aristotle.[131] Target Point markets its micro-targeting as a tool "that helps to answer their [customers'] most fundamental questions: Who supports my candidate? Where do I find them? How do I persuade others to support my candidate? When should I talk to them? Who should my messenger be?"[132] Aristotle, the other company highlighted by EPIC, has worked with "[e]very occupant of the White House" for over twenty-five years, and provides voter matching services that allow campaigns to "select and target only the voters [they] need by targeting individuals through a comprehensive selection of demographics including but not limited to: political district, political party affiliation, Super-voters, gender, ethnicity, marital status, wealth, educational level and presence of children."[133]

Internet users are slowly becoming aware of how much of their online activity is being monitored and legislators are increasingly making efforts to address their constituents' concerns about this tracking.[134] Recall Senator Rockefeller's questions

---

(Feb. 28, 2010), http://www.adweek.com/aw/content_display/news/digital/e3iccd499946ba0cc761fcc25e25943c52e; Jennifer Slegg, *What's the Buzz Behind Behavioral Advertising*, SEARCH ENGINE WATCH (May 11, 2006), http://searchenginewatch.com/3605361).

[129] *See* E-DECEPTIVE, *supra* note 1, at 10; Scott Thurm & Yukari Iwatani Kane, *Your Apps are Watching You*, WALL ST. J., Dec. 18, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html?mod=WSJ_hp_LEFTTopStories&om_rid=DlFZ0L&om_mid=_BNDMpyB8WhYZdB#articleTabs%3Darticle.

[130] *Id.* (citing Thomas Fitzgerald, *Profiling is Key to '06 Turnout: Campaigns are Mining Consumer Data for Votes*, PHILA. INQUIRER, Oct. 29, 2006, at A1; Heather Green, *The Candidates are Monitoring Your Mouse*, BLOOMBERG BUSINESS WEEK (Aug. 28, 2008, 5:00 PM), http://www.businessweek.com/magazine/content/08_36/b4098022877194.htm).

[131] *Id.* at 10–11.

[132] *Id.* at 10; *see also MicroTargeting*, TARGETPOINT, http://www.targetpointconsulting.com/system/uploads/14/original/MicroTargeting_101_8-2009.pdf?1249570076 (last visited Apr. 10, 2011). The company provides a "data-rich resource to guide a campaign's strategic decision-making." *To The Point: 4 Ways Data can Change Campaigns*, TARGETPOINT (Aug. 25, 2010), http://www.targetpointconsulting.com/ToThePoint/2010/08/25/4-ways-location-data-can-change-campaigns.

[133] E-DECEPTIVE, *supra* note 1, at 11; *About Aristotle*, ARISTOTLE, http://www.aristotle.com/content/blogsection/8/72 (last visited Apr. 10, 2011); *VoterListsOnline.com*, ARISTOTLE, http://www.aristotle.com/content/view/35/119 (last visited Apr. 10, 2011).

[134] *See Behavioral Advertising: Industry Practices And Consumers' Expectations: Hearing before the Subcomm. on Commerce, Trade, and Consumer Prot. and the Subcomm. on Commc'ns, Tech., and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong. (2010) (statement of Jeffrey Chester, Exec. Dir., Ctr. For Digital Democracy); Press Release, Report Reveals Consumer Awareness About BT (Mar. 26, 2008), http://www.truste.com/about_TRUSTe/press-room/news_truste_consumer_awareness_report.html.

referenced above: "Can consumers demand the same degree of anonymity on the Internet that they have in a shopping mall?"[135] The Federal Trade Commission and the Commerce Department recently published reports calling for increased privacy protections for Internet users.[136] Members of the House are putting forth bills to protect privacy, including "Do Not Track" legislation.[137] The Senate Judiciary committee has created a new subcommittee focused on privacy and the relationship between the individual and the private sector, with jurisdiction over areas including the privacy implications of emerging technologies.[138] These efforts reflect awareness of the need to protect the privacy of Internet users and may also provide ways to think about addressing voter suppression activity that occurs when users' privacy is compromised and used to create profiles based on Internet use.

Political organizations, both grassroots and dominant parties, ought to develop privacy policies about the use of voter information they have collected during the process of getting out the vote, registering voters, and fund-raising. In the 2010 midterm election, Organizing for America, the group which grew out of President Obama's 2008 presidential campaign, created a virtual phone bank.[139] The virtual phone bank provided volunteers helping to get out the vote with detailed information about voters, including name, sex, phone number, city of residence, and address.[140] Volunteers called people on the list to urge them to get out and vote. The problem was the lack of privacy protections built into this virtual phone bank.[141] Anyone who had a computer and could access the Internet, could view this detailed information about voters.[142] Potential volunteers did not have to register or provide any personal information in order to access the data.[143]

Many conservative activists, took advantage of this easy access to use the listings for their own ends.[144] Rubin Stublen explains, "I just called and asked them to vote

---

[135] *Hearing*, Rockefeller, *supra* note 11.

[136] *See* COMMERCE DEP'T, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), *available at* http://ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[137] *See* David Sarno, *'Do Not Track' Internet Privacy Bill Introduced in House*, L.A. TIMES (Feb. 11, 2011), http://articles.latimes.com/2011/feb/11/business/la-fi-do-not-track-20110212.

[138] *See* Cecilia Kang, *Senate Judiciary Names Franken Head of New Privacy, Tech Subcommittee*, WASH. POST (Feb. 14, 2011, 4:34 PM), http://voices.washingtonpost.com/posttech/2011/02/senate_judiciary_names_franken.html.

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

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] *Id.*

for the conservative candidate who was in their area . . . . You don't have to log on and you can get the numbers. I mean, duh."[145] Another conservative activist urged readers to sabotage the Organizing for America's get-out-the-vote effort by pretending to call people on the list but then claim that the voters were deceased or had voted early.[146]

This virtual phone bank example shows the need for enhanced privacy policies as well as illustrates the difficulties discussed earlier of defining deceptive practices and potentially creating legislation that would penalize such activities. The opportunity for advertisers to drill down to the individual interests of particular consumers presents a similar opportunity for activists to target a deceptive campaign at particular audiences. The vulnerability of these audiences suggests that strategies for enhancing digital literacy be designed, the necessity of more stringent regulation of online behavioral advertising, and the adoption of federal and state laws which address deceptive campaign tactics. Voter suppression will become an increasingly potent way to thwart people's active participation in the electoral process. Unless the law evolves to incorporate both civil and criminal penalties for voter suppression, many vulnerable voters will lose the opportunity to have their voices heard.

---

[145] *Id.* In contrast to the ease of access to information in the Organizing for America phone bank, the Republic National Committee required volunteers to register on its website before making a call. The information provided volunteers was limited to the name and state of the voters being called and the call itself was routed through the volunteers' computers, effectively masking the phone numbers of both volunteer and voter. *Id.*

[146] *Id.*