Smartphones and Election 2012

Lillie Coney,[*] C. Aaron Cois,[*] and Beth Rosenberg[*]

The increased prevalence of smartphones has the potential to deceive and exploit voters during the 2012 election season. The danger posed to our electoral system will require not only comprehensive voter education and voter protection efforts, but also new regulator and legal rules, as well.

I Introduction and Road Map for the Report

Voters of the 21st Century are experiencing a revolution in political engagement through innovations in communication technology. This report will review the potential for smartphones as vehicles to deliver deceptive messages to voters. Explore specific types of deceptive campaign attacks that would be unique to smartphones and explain why they will work if not addressed. The report will also provide guidance to voters, election administrators, campaigns and election protection efforts on methods that may diminish the impact of e-deceptive campaign practices that target smartphone users.

Elections rely upon successfully reaching voters where they are, and where voters are in 2012 is online. This election year consumer-voters are demonstrating a preference for smartphones that allow them to access online content and services as well as share their original content with others.

II Current Situation

A. 2012 Federal Election Summary

[*] Lillie Coney is Associate Director with the Electronic Privacy Information Center (EPIC) in Washington, DC. Ms. Coney coordinates EPIC's Voting Privacy Project. She contributed to the Brennan Center Taskforces on the Security and Usability of Voting Systems. She also served as a member of the ACM Committee on Guidelines for Implementation of Voter Registration Databases. She contributed to the academic paper "Towards a Privacy Measurement Criterion for Voting Systems. She also authored EPIC's e-Deceptive Campaign Practices Report 2008 and edited the 2010 report.

[*] Dr. C. Aaron Cois is a Software Team Lead for CERT, at the Carnegie Mellon University Software Engineering Institute (SEI) in Pittsburgh, PA. His work includes software development, application security, software architecture, and mobile application development.

[*] Beth Rosenberg is a Technology Fellow at the Electronic Privacy Information Center. She has more than two decades of editing and journalism experience, primarily in the areas of emerging technologies, privacy, and security.

The Federal Election Commission currently regulates campaign telephone banks by stipulating that they must contain disclaimers clearly stating if a committee paid for the communication.[1] However, the regulation explicitly states that it does not regulate Internet communications transmitted over telephone lines. Further, the FEC also regulates corporate communications "for the purpose of influencing" elections that expressly advocate for the election or defeat of a clearly identified candidate. [2]

There are grey areas regarding smartphones and federal campaign regulations because the types of political messages are not limited to voice, but can include, text, apps, video and/or links to online content. The FEC has rules regarding certain types of smartphone campaign related activity that will be discussed later in the report, but the overall many types of campaign messaging are not addressed in federal election law.

B. Regulatory and Legal Framework and the 2012 Election

In 2012, smartphones, most particularly phones running Apple Computer's iOS and the open-source Android operating system, account for at least 40% of the mobile devices used in the United States.[3] Like tablet computers and e-readers, the other fully enabled portable Internet devices,[4] smartphones are increasingly a resource for people to access information,[5] share content, and communicate their views.[6] During the 2012 general election, the smartphone very well may become an essential tool for campaigns and voters.

In the first quarter of 2012, mobile phone consumers spent $109.9 billion, while consumers of landline-telephone service spent $64.4 billion.[7] The Federal Communications Commission

---

[1] Federal Election Commission, Title 11, Chapter 1, Section 100.28 Scope and Definitions, Telephone Bank, (2 U.S.C. 431(24))
http://edocket.access.gpo.gov/cfr_2008/janqtr/11cfr100.28.htm
Federal Election, Title 1, Section 100.17, Scope and Definitions, Clearly Identified (2U.S.C. 431(18)) http://edocket.access.gpo.gov/cfr_2008/janqtr/11cfr100.17.htm

[2] Buckley v Valeo, 424 U.S. 1, 80 (1976); FEC v Massachusetts Citizens for Life, Inc, 479 U.S. 238 248-49 (1986)

[3] *Smartphones Account for Half of all Mobile Phones, Dominate New Phone Purchases in the US*, NIELSONWIRE (Mar. 29, 2012), http://blog.nielsen.com/nielsenwire/online_mobile/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us/.

[4] David Sarno, *Ownership of tablets, e-readers jumps during holiday season*, L.A. TIMES, Jan. 24, 2012, http://articles.latimes.com/2012/jan/24/business/la-fi-tablets-20120124.

[5] *Cross-Platform Report: How We Watch From Screen to Screen*, NIELSONWIRE (May 3, 2012), http://blog.nielsen.com/nielsenwire/online_mobile/cross-platform-report-how-we-watch-from-screen-to-screen/.

[6] PEDRO GIOVANNI LEON ET AL.,CARNEGIE MELLON UNIV. CYLAB, WHAT DO ONLINE BEHAVIORAL ADVERTISING DISCLOSURES COMMUNICATE TO USERS? (2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf .

[7] Bureau of Econ. Analysis, U.S. Dep't of Commerce, National Income and Product Accounts Tables tbl. 2.4.5U (2012), http://www.bea.gov/national/nipaweb/nipa_underlying/TableView.asp?SelectedTable=17&FirstYear=2011&LastYear=2012&Freq=Qtr&ViewSeries=Yes (last revised Apr. 30, 2012).

reports that these figures are only going to become more pronounced in this decade.[8] The U.S. is part of the worldwide trend toward more mobile communication devices and fewer "traditional" computing systems. The Pew Internet & American Life Project reported in March 2012 that 46% of American adults are smartphone users, an 11% increase since 2011.[9] The Pew survey's research revealed the following percentages of smartphone users by age group: 67% of those ages 18-24; 71% of those 25-34; 54% of those 35-44; 44% of those 45-54; 31% of those 55-64 and 13% of those over 65.[10] Additionally, a demographic study of American smartphone users suggests users tend to be financially well-off, well-educated, and under the age of 45.[11]

The Internet has already revolutionized how both campaigns and voters engage in the political process. Election officials use the Internet to enhance the information services provided to voters, while election protection efforts use it to inform voters of their rights, coordinate activities of volunteers, and provide near real time feedback of Election Day activities. Campaigns use the Internet as a more efficient means of targeting voters for messaging and solicitation of contributions. Individual voters are empowered by the Internet to speak directly to fellow members of the electorate, candidates, and policymakers through their own messaging, bypassing traditional media outlets like television, radio and newspapers.

Smartphone use in elections extends this process to the next level. This report explores the novel uses of smartphones during the 2012 election season, and their potential for exploitation and malfeasance.[14] Part I of the report discusses the potential uses and risks smartphone technology will pose during this election cycle, while Part II explores various e-deceptive campaign tactics and terminology and their application. It concludes with recommendations for how both voters and campaigns can protect themselves from "bad actors" who could use the Internet in general and smartphones in particular to disrupt or skew the 2012 election at all levels.

I. Smartphone Technology, Uses, and Risks

---

[8] INDUSTRY ANALYSIS & TECH. DIV. WIRELINE COMPETITION BUREAU, FED. COMMC'N COMM'N, TRENDS IN TELEPHONE SERVICE (2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

[9] *See, e.g.*, Aaron Smith, Pew Internet & Am. Life Project, *Nearly half of American adults are smartphone owners* (Mar. 1, 2012), http://pewinternet.org/Reports/2012/Smartphone-Update-2012/Findings.aspx (finding 41% of adults use some other type of cell phone while only 12% have no mobile phone); Amanda Lenhart, Pew Internet & Am. Life Project, *Teens, Smartphones & Texting* (Mar. 19, 2012), http://www.pewinternet.org/Reports/2012/Teens-and-smartphones/Cell-phone-ownership.aspx.

[10] AARON SMITH, PEW INTERNET & AM. LIFE, 46% OF AMERICAN ADULTS ARE SMARTPHONE OWNERS (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf

[11] AARON SMITH, PEW INTERNET & AM. LIFE, 35% OF AMERICAN ADULTS OWN A SMARTPHONE (2011), *available at* http://pewinternet.org/~/media//Files/Reports/2011/PIP_Smartphones.pdf. Smith's report states that 59% of adults living in a household earning income of $75,000 or more are smartphone owners, as were 48% of those with a college degree. Even among those with a household income of $30,000 or less, smartphone ownership rates for those ages 18-29 are equal to the national average. Additionally, among African-Americans and Latinos, 44% are smartphone users.

[14] *See* RICHARD POWER, CARNEGIE MELLON CYLAB. & MCAFEE, MOBILITY AND SECURITY: DAZZLING OPPORTUNITIES, PROFOUND CHALLENGES (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf (analyzing mobile security and the consumerization of information technology in the workplace).

Before smartphones and other mobile Internet devices, only desk- and laptop computers could deliver Internet-based content to voters. The situation in 2012 has changed dramatically from what it was in 2008. Unlike predecessors (e.g., the Palm), current smartphones have computing and storage capacity that rivals desktop computers of less than a decade ago. The speed and computing power of smartphones are making them a valuable asset for business, personal use, and now political engagement.

According to NielsonWire, almost 50% of mobile technology users own smartphones.[15] A 2011 study reports there are 91.4 million smartphones in use in the United States. Approximately 47% of smartphones in use worldwide are Android-based phones; 29% are iOS-based iPhones; 17% are BlackBerrys; and the rest are divided between Symbian-based and Microsoft Mobile OS-based devices.[16]

The single most important advancement to smartphones also poses the most significant risks: native and third party applications, or "apps."

Smartphones are capable of managing gigabytes of storage and possess powerful processing capacity.[17] Apps harness this power and allow smartphones to access the Web, send and receive email, capture and send digital photos, play games, download music, watch TV, provide two-way live video, and access calendars, address books, and other personal activities within the Internet "cloud".[18] Smartphones are also becoming even "smarter" through multiple radio and network sensor interfaces that enhance users' ability to network with other technologies in their environment (e.g., other "smart" devices, smart-grid-enabled home appliances, entertainment systems, desktop and laptop computers, etc.). The latest smartphones can also provide banking and payment services, and they often have built-in "Near Field Communication" chips that allow users to pay at retail store check-out points by tapping their phone against a sensor.[19]

Smartphones are also intimately associated with their owners and can reveal a great deal about their owners as a result.[20] Researchers who collect cellphone data claim that they can discern "hidden patterns" of social life at home, work, or play that reveal details of life such as travels,

---

[15] *Smartphones Account for Half of all Mobile Phones, Dominate New Phone Purchases in the US*, *supra* note 3.
[16] Anson Alexander, Smartphone Usage Statistics 2012 (Jan. 24, 2012), http://ansonalex.com/infographics/smartphone-usage-statistics-2012-infographic/.
[17] GILES HOGBEN & MARNIX DEKKER, EUR. NETWORK & INFO. SEC. AGENCY, SMARTPHONES: INFORMATION SECURITY RISKS, OPPORTUNITIES AND RECOMMENDATIONS FOR USERS (2010), *available at* http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport.
[18] DEBORAH MORLEY & CHARLES S. PARKER, UNDERSTANDING COMPUTERS: TODAY AND TOMORROW (12th ed. 2009).
[19] Bruce Upbin, *Tap-To-Pay Smartphones: The Coming Near Field Communications Tsunami*, FORBES (Apr. 23, 2012, 2:07 PM), http://www.forbes.com/sites/ciocentral/2012/04/23/tap-to-pay-smartphones-the-coming-near-field-communications-tsunami/; *see also* Patently Apple, *Apple Wins Patent for iWallet: The one that will rule the World* (Mar. 6, 2012), http://www.patentlyapple.com/patently-apple/2012/03/apple-wins-patent-for-iwallet-the-one-that-will-rule-the-world.html (discussing new patent that would allow the implementation and control of a subsidiary financial account on a mobile device).
[20] Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J., Apr. 22, 2011, http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html#articleTabs%3Dvideo (follow video link).

risk of disease—even our political views.[21] Cellphone research suggests that phone use may also reveal those who can influence a person most—the people who are most likely to get someone to change their mind. MIT scientists report that cellphone use data from the 2008 election allowed them to determine that two people were discussing politics without knowing the content of the communication.[22] Typically, smartphones:

- Contain personally identifiable information (PII), including name, address, credit card numbers, banking info, usernames/passwords;
- Contain contacts and social relationship data of the user, such as name/address/phone/relationship information of friends, family, and business acquaintances;
- Are within arm's reach of their owners 24 hours a day;
- Offer applications that can learn from and adapt to users;
- Support applications that monitor the location of users in public spaces;[23]
- Track online activity;
- Host cookies or other computing code that record user engagement with smartphone devices.

This report anticipates that, in 2012, voters will use smartphones as an essential tool for engaging in the political process. We also anticipate that political and election-based apps will promote greater voter engagement.[24] At the same time, however, this election will also create numerous security and privacy risks for smartphone users.[25] These risks include:

- Political or election-centered smartphone apps with misleading, overly complex or inadequate privacy settings;
- "Phishing" attacks promulgated via fake political apps or other digital communications that appear to come from a legitimate campaign;
- Spyware that invades smartphones via political or election apps, either in the app itself, in-app ads (free apps often use these) or on websites or via email;
- Network "spoofing" attacks that take smartphone users to a fake campaign website;
- Location-based surveillance of key campaign staff or officials; campaign volunteers, candidates or their significant others as well as voters;[26]
- Programs that capture keystrokes or log emails or SMS text messages and can capture passwords;

---

[21] Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J., Apr. 22, 2011, http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html.
[22] *Id.*
[23] John Brownlee, *This Creepy App Isn't Just Stalking Women Without Their Knowledge, It's A Wake-Up Call About Facebook Privacy*, CULT OF MAC (Mar. 30, 2012, 3:20 PM PDT), http://www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/.
[24] Michael Scherer, *Complete Coverage of the 2012 Presidential Election*, TIME SWAMPLAND (Mar. 30, 2012), http://swampland.time.com/2012/03/30/the-obama-campaign-tries-out-a-new-cellular-weapon/.
[25] HOGBAN & DEKKER, *supra* note 17.
[26] Hayley Tsukayama, Obama campaign app concerns some privacy advocates, Washington Post, August 7, 2012, http://www.washingtonpost.com/business/economy/obama-campaign-app-concerns-some-privacy-advocates/2012/08/07/548ed7f2-e0b6-11e1-8fc5-a7dcf1fc161d_story.html

- Auto-dial donation sites that use smartphone auto-dialing features to send funds without user permission or knowledge;
- Malware designed to capture campaign credit-card numbers or online banking credentials;
- Smartphone-generated network attacks that overload network capacity during crucial periods of the election season.

A. Profiling and Privacy Risks in Elections

The first rule of privacy protection is to maintain no secret system of records.[27] Secret records disallow individual control over personal and personally identifiable information. The right to correct incorrect information or to know who has accessed information and for what purpose is critical to protecting against abuse or misuse of personal data. Unfortunately, the collection of personal information to create consumer profiles and to influence decisions on consumer opportunities (e.g., employment, credit-worthiness, and educational advancement) is routine in modern society.[28]

Consumer profiles generally link individuals to information that would otherwise not be associated without the effort of collecting data from many sources and placing it in a format that links data to the people it is supposed to represent. For example, credit reports are a well-known type of consumer profile. Credit reports, however, are not secret. The secret profiles that are amassed for commercial purposes, on the other hand, pose privacy risks to consumers.

Consumer profiles are major currency in electronic commerce, where advertisers and marketers use profiles to predict preferences, interests, needs and possible future purchases.[29] Retailers routinely share or sell data on customers and have used that information to improve products and services.[30] Now, retailers are sharing or selling that information to data brokers who use information to create rich profiles on consumers.[31] Data brokers comprise a hidden multi-billion dollar a year industry that buys and sells consumer profile information.[32] In the context of

[27] *See, e.g.*, Electronic Privacy Information Center, Code of Fair Information Practices, http://epic.org/privacy/consumer/code_fair_info.html (last visited May 15, 2012) (citing U.S. DEP'T. OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS § III (1973), *available at* http://epic.org/privacy/hew1973report/c3.htm).
[28] For more information, see EPIC's resource pages: EPIC - E-Verify and Privacy, http://epic.org/privacy/e-verify/ (last visited May 15, 2012); EPIC - Student Privacy, http://epic.org/privacy/student/ (last visited May 15, 2012); EPIC - Privacy and Public Records, http://epic.org/privacy/publicrecords/ (last visited May 15, 2012).
[29] EPIC - Privacy and Consumer Profiling, http://epic.org/privacy/profiling/ (last visited May 15, 2012).
[30] Mike Lennon, *Massive Breach at Epsilon Compromises Customer Lists of Major Brands*, SECURITY WEEK (Apr. 2, 2011), http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands; *see also* EPIC Privacy in the News, *Epsilon Data Breach* (Apr. 7, 2011), http://epic.org/2011/04/epsilon-data-breach-threatens.html.
[31] Lior Levin, *5 New Media Trends That Expand Online Retail Sales*, POWERRETAIL.COM.AU (May 7, 2012), http://www.powerretail.com.au/insights/5-new-media-trends/.
[32] Privacy Rights Clearinghouse, The Proliferation of Online Information Brokers: Noncompliance with Their Own Privacy Policies and Other Problems, December 16, 2008, http://www.privacyrights.org/ar/FTC-InfoBrokers-SummaryWeb-081216.htm (posted Mar. 30, 2009).

smartphones, commercial app developers have every incentive to include hidden features in their apps which collect even more information on users.[33]

Smartphone political apps may prove to be serious challenges to voter privacy. Some political apps combine the collection of near-real-time location information with access to a voter database. The election season is well underway and emotions are running high on and off the campaign trail. Supporters may not mind their candidate or party's campaign knowing all about them, but they may not want others to know their political preferences.[34]

In addition to apps themselves, the technical features of smartphones generate large amounts of personal data about their users. For example, many online generated profiles link to an assigned number or the user's Internet Protocol (IP) addresses. IP addresses are unique numbers that identify a particular computer, but not necessarily any individual user. Smartphones also possess IP addresses; however, IP addresses on smartphones have one major difference from those on other computing devices: On a smartphone, the identity of the smartphone's owner is linked with their location, the data on the phone, and the smartphone use. On a smartphone, it quickly becomes easier to piece together disparate bits of information in order to identify a specific user.

Even when profile data is de-identified it may be possible to re-identify specific individuals by their profile data.[35] This risk became all too real when, in 2006, America Online (AOL) made the search records of 658,000 Americans public. Although the search logs released by AOL had been "anonymized," identifying users only by assigned numbers, news reporters easily matched user numbers with identifiable individuals.[36]

Collecting data of this sort is essential to create voter profiles in order to identify potential targets for messaging. Internet-based deceptive campaign attacks rely on the ability of attackers to effectively identify targets for their deceptions. Voter profiling for targeting campaign messages is nothing new; for decades, campaigns have collected information in order to create voter profiles. This data is gathering comes from voter registration applications, voters' history of participation, state-issued professional licenses, and low-level elected office holders. Many states consider this information to be "public."

Voter profiles are used to understand the behavior of individuals based on their activities, life experiences and preferences for a wide range of products and services.[37] In 2010, the list of voter profiling categories included active military service membership, foreclosure status of a primary home, employment status, as well as subjective views of the US economy based on local gas

---

[33] Connie Guglielmo, *Congress Queries Apple, iPhone App Developers About Privacy*, FORBES (Mar. 22, 2012), http://www.forbes.com/sites/connieguglielmo/2012/03/22/congress-queries-apple-iphone-app-developers-about-privacy/.

[34] Timothy Noah, Bumper Sticker Insubordination A Kerry fan gets fired, and then hired, for her politics, Slate September 14, 2004, http://www.slate.com/articles/news_and_politics/chatterbox/2004/09/bumper_sticker_insubordination.html

[35] EPIC - Re-identification Page, http://epic.org/privacy/reidentification/ (last visited May 15, 2012).

[36] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at C4, *available at* http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63.

[37] Thomas Fitzgerald, *Parties pin hopes on voter profiling*, BRADENTON HERALD (Fla.), Nov. 2, 2006, at 3; *see also* Voter Vault (FILPAC),http://www.filpac.com/votervault.htm (last visited May 15, 2012).

prices or unemployment statistics. Profiles may also include information on personal associations, religious beliefs, political affiliation, support or non-support for causes, past political participation, profession or job held, neighborhood demographics, birthplace, and level of education.[38] Increasingly profiles include more near-real-time activity on consumers such as information on user online behavior, for example, on Facebook, Twitter, or search engine activity. Data aggregators can and do sell this information to campaigns.

Few voters are aware of how much information about the details of their lives is in the hands of third parties. Law enforcement, businesses, and political campaigns are making great progress in mastering the ability to create detailed profiles on individuals. The central committees of both major political parties, as well as and their candidates at the national, state and local levels, are spending billions of dollars to gain greater knowledge of the voters they seek to persuade. In 2006, a report regarding Voter Vault, political software developed by Filpac, a Republican firm, claimed it held data on 160 million Americans.[39] That figure is sure to have increased dramatically over the intervening six years, and smartphones will provide a wealth of new data for these firms to collect.

B. Smartphones and Campaign Engagement in 2012

Voters in 2012, just as they did in 2008 and 2010, can expect to hear early and often from campaigns. Campaign styles and strategies have changed as new technologies and delivery platforms are introduced. Bloggers, Twitter users, and independent campaign efforts are gaining prominence in influencing voters. Whether they approve or not, voters will have their activity online tracked, monitored, and defined by political efforts, and voters who are smartphone users can expect to receive political survey calls, mobile advertisements, and solicitations for contributions on their iPhones, Android devices, and Blackberry smartphones.

Smartphones will provide access to additional voter information such as the real-time collection of voter location data. This data is important because of its potential to reveal relevant activities or interests of voters, which can become a basis for political engagement. Buying gasoline, for example, may prompt the delivery of a political advertisement about the high cost of fuel. If a user went to a major league game or stock car race, visited the local library or participated in a political rally with her smartphone in hand — her location may be in her voter profile. In this election, engaging with voters via smartphones could be lucrative and may be essential. An official Obama 2012 campaign app uses location-based services to identify registered Democrats in the area by first names, last initials, and ages.[40] Meanwhile, the Romney campaign has released an app called "Mitt's VP," which will let users be among the first to know the Republican candidate's choice of running mate. The free app requires users to provide contact information, which will then, presumably, be disseminated to the Romney campaign.[41]

---

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

[39] Jon Gertner, *The Very, Very Personal Is the Political*, N.Y. TIMES MAG., Feb. 15, 2004, http://www.nytimes.com/2004/02/15/magazine/15VOTERS.html?pagewanted=all.

[40] Lois Beckett, "Is Your Neighbor a Democrat? Obama Has an App for That," Aug. 3, 2012, available at http://www.propublica.org/article/is-your-neighbor-a-democrat-obama-has-an-app-for-that.

[41] "Who Will Be Romney's VP?" App available at http://itunes.apple.com/us/app/mitts-vp/id544919187?ls=1&mt=8.

Internet political communications increase the challenge of enforcing existing state and federal laws intended to regulate political activity. In the case of e-deceptive political communications, the challenge of identifying the source — and more importantly, enforcing state and federal laws intended to protect citizens from deceptive election practices — will require new approaches. More state legislatures are amending campaign-financing laws to account for the effect of Internet technology on political advertising.

The adoption of smartphones for political campaign uses may lead to more federal and state regulations on how political advertisements may be used. In 2009, Scott Wagman, a mayoral candidate in St. Petersburg, FL, took advantage of an innovative way to influence voters that was not covered by state campaign laws: Google AdWords. Wagman purchased an AdWords advertisement that appeared on web sites, but did not include a campaign disclaimer. Wagman also purchased the names of his opponents from Google AdWords so any search on an opposing candidate's name was redirected to Wagman's mayoral campaign site.[42] In response, Florida enacted a law in 2010 designed to cope with this new form of political advertising. Florida law describes the attribution requirements for different means of political communication — and now provides for certain exemptions, including paid links so long as there are less than 200 available characters for use in the advertisement.[43]

At the same time, however, the Supreme Court's decision in *Citizens United* to remove both the safeguards against unlimited donations and the transparency usually required for federal election contributions presents additional challenges in the realm of smartphone use.[44] Furthermore, neither President Obama nor Republican Presidential nominee Mitt Romney will take federal funding, which would have limited the ability of both candidates to raise money on their own. As a result, during the upcoming election, large sums of untraceable funds from individuals, corporations, and unions likely will speed the development and deployment of technology designed to raise both large and small contributions. Partisan application development for portable digital devices will be the newest tool to facilitate individual donations to campaigns.

The Federal Election Commission (FEC) places limits on the amount of money individual donors may contribute to a federal election campaigns or political causes.[45] Traditionally, campaigns relied upon a group of routine supporters who gave the maximum amount allowed under law; the introduction of small-dollar donors as a major source of campaign funds did not really begin in earnest until the 2004 presidential election.[46] Online contributions proved to be a

---

[42] *See, e.g.*, Cristina Silva, *Scott Wagman to fight online ad complaint in a case that could set precedent*, TAMPA BAY TIMES, Aug. 11, 2009, http://www.tampabay.com/news/politics/kyc/article1026451.ece.

[43] Technology in Elections Act, 2010 Fla. Laws 167 § 18 (exempting political advertisements "placed as a paid link on an internet website, provided the message or advertisement is no more than 200 characters in length and the link directs the user to another internet website that complies with [disclosure requirements]").

[44] In *Citizens United v. FEC*, 130 S.Ct. 876 (2010), the Supreme Court held that a provision of the Bipartisan Campaign Reform Act prohibiting independent expenditures by corporations and unions violated the First Amendment. *See, e.g.*, Brian Mooney, *Fund-raising Game Upended in 2012 Race*, BOSTON GLOBE, April 8, 2012, http://www.boston.com/news/politics/articles/2012/04/08/fund_raising_game_upended_in_2012_race/.

[45] Fed. Election Comm'n, Contribution Limits Chart 2011-12, http://www.fec.gov/pages/brochures/contriblimits.shtml (last visited May 15, 2012).

[46] INST. FOR POLITICS DEMOCRACY & THE INTERNET, SMALL DONORS AND ONLINE GIVING, A STUDY OF DONORS TO THE 2004 PRESIDENTIAL CAMPAIGN (2006), *available at*

particularly attractive option for young donors in 2004, and Barack Obama's campaign in 2008 further proved the value of reaching small dollar contributors online.

Political contributions online are more cost-effective than contributions by physical mail, both for the contributor and the cause. Internet-based giving also established a model that could optimize issue-generated support in an increasingly 24-hour news cycle. For example, mobile-phone-based contributions toward relief efforts following the Haiti Earthquake totaled over $30 million within a few days.[47]

The FEC is responsible for enforcing federal election rules that govern political advertising, telecommunications, and fundraising activities. One of the FEC's roles is to increase the transparency of campaign efforts in support of candidates for federal elected office. In June 2010, the FEC began to approve a series of "affinity" programs[48] designed to solicit contributions and engage voters via smartphone. Affinity programs were first proposed by businesses that offered to provide contributions to campaigns or legislative advocacy organizations based on consumer consumption or use of products or services.[49] In 2010, Famos LLC received approval from the FEC to offer a Web based Affinity Program to Political Affinity Account Holders.[50] In November 2010, CTIA – The Wireless Association received guidance on an Affinity Program to allow wireless customers to make up to $50 in anonymous contributions.[51] More recently, in June 2012, the FEC unanimously permitted donors to make small contributions to political campaigns via text messaging. While donations are capped at $50 per cell phone number per month, the decision has already been called a "game-changer" for political contributions.[52]

Smartphone users themselves must have tools available to them to let them know that their contributions are going to the candidate or campaign that they intend to support. Many small-dollar donors are supporting campaigns for the first time and likely will use digital means to

---

http://www.cfinst.org/pdf/federal/president/IPDI_SmallDonors.pdf. In 2004, most online donors were ages 18-34, representing all levels of contributions, and Democratic campaigns were more successful overall in soliciting online donations than Republicans.

[47] Stephanie Strom, *Nonprofits Rush to Solicit Donations via Text, but the System Is Flawed*, N.Y. TIMES, Oct. 31, 2010, http://www.nytimes.com/2010/11/01/business/01text.html?_r=2&pagewanted=all.

[48] The FEC uses the term "affinity program" to identify a relationship between a business that offers a product or service and an organization (e.g. fraternal, charitable, religious, professional, or, as in this case, political) that endorses or sponsors the business's product or service to its members, supporters, or other interested persons. *See, e.g.*, FEC Advisory Op. 2010-06 (Famos LLC Web Affinity Program), at 1 n.1, May 27, 2010, *available at* http://saos.nictusa.com/aodocs/AO%202010-06%20final.pdf (citing Advisory Ops. 1979-17 (RNC), 1992-40 (Leading Edge Communications), 2003-16 (Providian National Bank), 2006-34 (Working Assets), and 2008-18 (Mid-Atlantic Benefits).

[49] FEC Advisory Op. 2006-34 (Working Assets Credit Card Affinity Program), Feb. 9, 2007, *available at* http://saos.nictusa.com/aodocs/2006-34.pdf.

[50] FEC Advisory Op. 2010-06, *supra* note 50.

[51] FEC Advisory Op. 2010-23 (CTIA Wireless Association), Nov. 19, 2010, *available at* http://saos.nictusa.com/aodocs/AO%202010-23.pdf. The FEC's vote is available at http://saos.nictusa.com/aodocs/1156216.pdf.

[52] FEC Advisory Op. 2012-17 (Red Blue T LLC, ArmourMedia, Inc., and m-Qube, Inc.), June 11, 2012. *See also* Jack Gillum, *FEC allows campaign donations via text messaging*, AP (June 12, 2012), http://news.yahoo.com/fec-allows-campaign-donations-via-text-messaging-012521250.html.

contribute. First-time contributors also may be unlikely to know that there are federal election donation limits.

C. Internet Globalization and Freedom and Their Effects on E-Campaigns

A primary purpose of the early Internet was to allow researchers to quickly disseminate their results to their peers. Hence, it was designed to be robust and efficient. However, because only a small community of researchers and scientists with well-defined roles used it, security was not a major concern. Even as the Internet became more broadly accessible to users and grew considerably in the nature of its scope and its uses, its intent remained the same: to allow for efficient communication, unhindered by administrative restrictions. The nature of the Internet's "network of networks" makes it particularly difficult for an individual entity to supervise.[55] The fact that smartphone technology is spread across the world provides another challenge to legal regulation. This absence of regulation has served the Internet well in the past, allowing for explosive growth in both content and delivery speed. However, this same lack of regulation has presented problems for consumers to retain control of their personal information.

Similarly, the Internet environment could present problems for enforcing voting rights and thwarting voter suppression efforts that take advantage of this medium. There are no regulations that say a U.S. campaign must be entirely based on American soil. In fact, a tech-savvy and well-resourced campaign might take some of its Internet operations overseas, and the use of cloud computing services alone may make it impossible to guarantee that an entire campaign is U.S.-based. In addition, Super PACs, 527s, and unaligned private efforts are not necessarily required to have U.S.-based services.[56] Even if the FEC investigated foreign elements to an election campaign, it might be impossible for the FEC to make any determination before the election. Furthermore, if any overseas operation were discovered and shut down, another website could easily open up and reroute the old site's Internet traffic, adding enormous complexities to any oversight or regulation.

It is difficult to enforce old campaign laws designed for political mail, radio or television broadcast and landline telephone communications in a broadband wireless global communication environment. As the Internet will probably continue to grow in a largely unsupervised fashion in the near future, users may not be able to rely solely on the strict enforcement of state and federal laws to combat e-deceptive campaign practices. As a result, smartphone users, candidates, campaigns, and election protection efforts will have to rely on their ability to know when something is amiss or seek out reliable sources of information through other means. The good

[55] A phishing site, for example, can shut itself down immediately, leaving very little information about its owner or geographic location.

[56] In January, the Supreme Court affirmed a decision by the D.C. District Court interpreting the 2002 Bipartisan Campaign Reform Act of 2002 as barring foreigners from contributing directly to candidates, making expenditures expressively targeting specific candidates, or making donations to outside groups who use those donations in turn for one of those purposes. However, the court specifically reiterated that the law "does not bar foreign nationals from issue advocacy—that is, speech that does not expressly advocate the election or defeat of a specific candidate." Bluman v. Federal Election Commission, 800 F. Supp. 2d 281, 284 (D.D.C. 2011), *aff'd*, No. 11-275 (Jan. 9, 2012).

news is that, since 2008, several states have taken steps to regulate potentially deceptive online political campaign messages.[57]

II. e-Deceptive Campaign Challenges

The following terms are familiar to computer security and law enforcement experts and will be used to explain the potential for e-deceptive campaign threats in the 2012 election. In the context of deceptive election practices, "spoofing," "phishing," "pharming," "denial of service," "email worms," "malware," "rumor-mongering," and "social engineering" are tactics that can be used to deceive voters and impact voter participation, as illustrated here.

A. Election Online Fraud Terminology

1. Terminology

• *Spoofing* occurs when a website falsely claims to be another, often official, site. For example, a deceptive site claiming to be a state election office might go so far as to appropriate a government's official insignia or seal. The web page's content also might provide deceptive information to voters about polling locations, voter registration rules, or polling dates and times. The recent decision by the Internet Corporation for Assigned Names and Numbers (ICANN) would allow non-Latin characters in Web addresses.[58] This change will open new fronts on spoofing attacks that use internationalized domain names or IDH Homograph Attacks.[59] The Cyrillic letters of A, B, C, E, K, H, P, M, O, T, and X are the visual equivalents of their respective Roman letters. An IDH Homograph Attack could come in the form of an email with a link using any one of or several of these Cyrillic letters. For example, both *http://www.barackobama.com/* and *http://www.mittromney.com/* contain letters which could easily be replaced by Cyrillic characters. An email link containing a Cyrillic character would look visually identical to the actual site's address. When "clicked" the user would land on a page that could look identical to the true website sought, but instead, be a fake or spoofed website.

• *Phishing* in the context of candidates or campaigns might involve sending fake email or text messages to voters, offering assistance with locating polling sites, voter change-of-address requests, new voter registration services, or verification of voter registration status. When the

---

[57] *See, e.g.*, Nichole Rustin-Paschal, *Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues*, 19 WM. & MARY BILL OF RTS. J. 907, 920 (2011); COMMON CAUSE ET AL., DECEPTIVE PRACTICES 2.0: LEGAL AND POLICY RESPONSES 5 (2008), *available at* http://www.commoncause.org/atf/cf/%7Bfb3c17e2-cdd1-4df6-92be-bd4429893665%7D/DECEPTIVE_PRACTICES_REPORT.PDF. Professor Gilda Daniels is less optimistic, arguing that "[o]n the issue of e-deception, a few states include laws that are broadly construed such that they may apply to the traditional means of deception and online voting deception. The litany of statutes and their attributes leads at best to piecemeal enforcement." Gilda R. Daniels, Voter Deception, 43 Ind. L. Rev. 343, 370 (2010).

[58] Press Release, Internet Corporation of Assigned Names and Numbers, ICANN Bringing the Languages of the World to the Global Internet | Fast Track Process for Internationalized Domain Names Launches (Nov. 16, 2009), http://www.icann.org/en/news/announcements/announcement-30oct09-en.htm.

[59] *See, e.g.*, Evgeniy Gabrilovich & Alex Gontmakher, *The Homograph Attack*, COMMUNICATIONS OF THE ACM, Feb. 2002, at128, *available at* http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf; Wikipedia, IDN Homograph Attack, http://en.wikipedia.org/wiki/IDN_homograph_attack (last visited May 15, 2012).

recipient clicks on the links provided, the recipient's computer and computer network are exposed to malware. Phishing can be used in conjunction with spoofing to collect user access rights to a site such as MittRomney.com or BarackObama.com.

• *Pharming* is a variant of phishing, involving the fraudulent use of legitimate domain names and redirecting legitimate Internet traffic to imposter Web sites. Pharming attacks could successfully hijack Get Out the Vote (GOTV), election administration, or election protection web addresses and redirect visitors to imposter web sites. Deceptive campaign techniques may manipulate information stored in a user's computer cache or in the stored registry of domain name system (DNS) addresses. When users visit a web site posing as a legitimate election information resource, malicious software may be installed onto the user's machine without any immediate visible effects. Pharming attacks can be used to trick contributors into donating money or providing personal information or political preferences to fake sites.

• *Denial of Service Attacks* can make voter information sites, GOTV efforts, or voter help hotlines unavailable by clogging up traffic to the web site, thereby overburdening the site's servers and causing the site to shut down. For example, by directing tens of thousands of voters to erroneously contact local election administrators for non-existent voter services such as activating voter registration cards, or known services such as verifying registration status, legitimate sites can crash, leaving voters without access to a critical resource on Election Day. Botnets,[60] collections of computers compromised and controlled by malware distributions, are often directed to perform denial of service attacks. Some botnets include millions of computers, making them a powerful force for this purpose.

• *Email worms and viruses* have been on the decline because of better security practices and heightened response when they are detected. The application of security patches and users' heightened awareness has diminished the damage caused by bogus email. However, smartphones are new territory in 2012.

• *Malware,* or malicious software, can be designed to access campaign staffs' personal email address books or email outboxes. The attack might activate the email application and send itself to the last 50 persons emailed by the user or those listed in the user's e-address book. One infected machine within a computer network can potentially bring down the email application for an entire organization until computers are made immune to the malicious code and it is removed from every infected computer. This type of attack can be disastrous for an election protection or election administration operation in the midst of an election day.

• *Rumor-Mongering* is a term used to cover one form of deceptive campaigning that relies on trusted sources of information to pass along false information. It can involve planting stories that sweep through blogs, on Twitter and Facebook and thus into the mainstream media, causing confusion amongst the electorate. For example, rumors that the election has been cancelled or delayed by a week due to an emergency might keep voters from the polls.

---

[60] John P. Mello Jr, The Case Of The Android Botnet, TechNewsWorld, July 23, 2012, 07/23/12, http://www.technewsworld.com/story/75701.html

• *Social engineering* involves tricking people, through non-technological means, into breaking their normal technology security practices; exploiting individuals who are not technologically savvy into exposing important personally identifiable information; or determining the emotional state of an identifiable block of voters to design messages to discourage participation. During the 2012 election season, social engineering for deceptive campaign purposes could include excessive negative messages directed toward voters disenchanted with the progress of a particular program or government project could be deployed to discourage those voters' participation in an election.

2. Neutral Technologies Used to Facilitate E-Deception

• *Packet sniffers* are specialized software programs typically employed by computer network operators for security and maintenance. Packet sniffers run on computers that are hooked into the network at a location where they can monitor network traffic flowing in and out of systems. These "sniffers" can monitor the entire data stream by searching for keywords, like "Romney" or "Obama;" phrases or strings like IP addresses or email accounts, or collect information on visited web site URLs. The "sniffers" can then record or retransmit anything that fits its search criteria for further review. The header information of IP TCP packets in transit between a requester and an ISP can reveal a packet's source, type, and intended destination.

• *Cookies* save information by storing it in the user's web browser. This allows, for example, a user to remain logged into a web site between browser sessions, as their authentication data could be stored in a cookie in their web browser.

• *Behavioral Targeting* can also be used to manipulate destination and routing of requests sent by Internet users. Web advertising and behavioral targeting techniques can be manipulated to reveal different page views to different users. For example, a viewer identified as a "friendly" voter could see correct information regarding polling locations and times, while an "unfriendly" voter could see a page with inaccurate or deceptive information.

B. E-Deception at Work

The threat posed by these e-deception tactics may present itself across a spectrum of Internet services. In particular, the use of everyday blogs, web pages, and messaging and social networking communication are susceptible to being used to deceive voters and impede their participation in Election 2012.

1. E-Deception via Blogs and Web Pages

Smartphone users find blogs to be great resource for political news and commentary, and are a leading source of news and campaign information for millions of voters. Disseminating campaign news and information is critical to an informed electorate. Campaign and candidate blogs and web pages can accomplish more than simply providing information to visitors to their sites; they are also a resource for campaigns to address issues of concern to their supporters, engage the media, and speak directly to voters on critical issues.

Many political blogs are doing a good, transparent job of engaging voters, but bloggers, readers, and campaigns all must be aware of the potential for deceptive campaign messages through individual blogs and comprehensive webpages. Corporate political speech is virtually unlimited this election cycle. Corporations, acting alone or in conjunction with others, can fund ads and campaigns without financial limit. When deciding whether to act on a message posted to a blog or website, voters should consider how much they trust the site and the information provided. Is the site really a grassroots effort or a marketing tool for a message or opinion clothed as a public or community service organization?

In general, deception in Internet communications is much easier than in physical space because digital theft or misappropriation of graphics, text, and state insignias is much easier to accomplish and may be harder for infrequent visitors to identify as being impersonations of legitimate sites.

2. Threats of E-Deception in Campaign Email, Social Networking and Instant Messaging

National political campaign efforts rely on instant messaging (IM), email, and mobile-device-optimized web sites to manage their communication environment. During the 2008 presidential election, one out of every six Americans received campaign-related emails either directly or forwarded from family or friends, [61] and that percentage is certain to rise significantly in 2012. This fast-paced means of reaching constituents also creates an environment ripe for disinformation or sabotage—particularly amongst younger, less-experienced voters, who are also disproportionately smartphone users.

Deceptive campaign email or text-based attacks may resemble traditional deceptive electioneering tactics by, for example, telling recipients that Democrats vote on one day and Republicans vote on another. However, voters' increasing sophistication and the easy availability of accurate online information will require that an effective attack be creative and well planned. For example, the recipients of a deceptive email may not be the ultimate targets: An attacker may send an email that tells the recipient to call the local election administrator's office to verify registration status or confirm a polling location. Deceptive emails appearing to come from election officials could prompt thousands of simultaneous calls at a time when local election administrators are struggling to open polls and answer legitimate questions from voters.

A more sophisticated deceptive email attack can even prompt well-intentioned users to spread a deceptive message. Any emails received regarding voter identification requirements, straight party voting rules, or other election advice should be viewed with caution. For example, an email stating that voter identification may be required on Election Day may be true, but recommendations that voters should bring a library card, paid parking citation receipt, or motor vehicle registration may seem plausible, but are deceptive messages. Any email message

[61] Andew Kohut, Pew Internet & Am. Life Project, *Social Networking and Online Videos Take Off: Internet's Broader Role in Campaign 2008* (Jan. 11, 2008), http://www.pewinternet.org/Reports/2008/The-Internet-Gains-in-Politics/Summary-of-Findings.aspx.

claiming to have new information applicable to all voters is likely to be false. Each state has its own rules controlling voter participation, including voter identification requirements.[62]

A smartphone attack also might target poll workers, who are essential to the proper conduct of public elections. Messages designed to misdirect poll workers could address their role in opening polling locations, rules regarding voter participation, or the appropriate steps that should be taken when faced with administrative questions during an election.

Social networking also presents a rich set of opportunities for deceptive campaigns, by spreading misinformation or disinformation that may move more quickly than election officials, candidates, and election protection efforts can dispel. These types of deceptions could also drain critical resources and move attention away from real issues or important matters that impact voter engagement at critical times during this election year.

III. Overview and Recommendations

These types of e-deceptive practices have the potential to target smartphone users, and prevention of these practices should be a priority this election year. The challenges of stopping electronic deceptive campaign practices are difficult because the source of the attack can be from any location around the globe, the launch of an attack can be timed to begin within hours of an election, and tracing the source of the attack can be time consuming and may not yield actionable results.

The unique features of smartphones—most specifically their constant proximity to their owners—can allow for shorter time spans to launch some types of attacks. Smartphone attacks may be easier to launch and may spread more quickly through exploits on apps and data already located on the device.

Attacks may be quite specific. Smartphone-based attacks may use software that activates on a significant pre-programmed date and/or time of day. Upon an update, an application may only activate on the morning of Election Day. Visiting certain politically oriented websites or downloading campaign apps, audio, or graphics files may be enough to identify user's political affiliation and attack only those smartphones which have visited or downloaded content about an opposition candidate. Malicious computer software may be used to launch deceptive campaign attacks that cause serious problems on affected smartphones by disabling or manipulating key applications.

Both users and campaigns can protect themselves, however. Attacks that come in the form of false email messages from campaigns—for example, repeated emails claiming that campaign contributions were not processed and need to be sent again—can be verified with the campaign or by checking one's personal bank statement. Meanwhile, campaign web sites should avail themselves of strong authentication and security procedures.

---

[62] Nat'l Conference of State Legislatures, State Voter ID Requirements, http://www.ncsl.org/legislatures-elections/elections/voter-id.aspx (last visited May 15, 2012). For accurate information on the each state's rules regarding voting, visit 866ourvote.org.

In general, smartphone users should take the following precautions

- Learn the rules for voting in your state today by visiting 866ourvote.org;
- Do not use an employer provided cell or smartphone for personal purposes—especially campaign related communications. Employers should not allow the sharing of employee cell or smartphone contact information to political entities (e.g. campaigns, parties or ballot initiatives). This might constitute a campaign contribution that must be reported to the FEC;
- Set smartphone locking features;
- Check the reputation of any app before installing. Download or use apps only from trusted campaign, election administration, election protection sites, or App stores or App Markets. Do not download apps from third-party web sites, as they are a common source of malware;
- Do not click through the installation of apps. Read each decision you are asked to make—some of them may be seeking access to other data hosted on the phone;
- Check the settings and selections for all existing apps on your smartphone;
- Reset and wipe the memory of all smartphones you may be recycling to remove personal information or stored content;
- Maintain good "hygiene" against botnets by ensuring that you have all of the most recent patches and updates for operating system software. Run computer security software to check computers for viruses, worms, Trojans, or active botnet activity. If you have broadband access and are not using your personal computer on Election Day, turn it off. Remember that botnets are not limited to the United States, but can be global. However, botnets cannot use a computer that is turned off.
- Be aware of the conditions for making text contributions to campaigns. Guidelines should be available on campaign websites, read them carefully.
- Links found in emails can be deceptive because of the similarity of certain Latin and Cyrillic letters.

Candidates/campaign staff/election protection entities should also take the following precautions

- Have smartphone apps checked by a third party professional software assessors for flaws or bugs; employ techniques to check both for security weaknesses based on the app itself and the app's interaction with operating systems prior to release;
- Create auditing apps to support security of web sites and application deployment. Those apps should never be ad-supported;
- Regularly clear your smartphone or tablet's cache and cookies;
- Never store sensitive campaign *or* personal information on your smartphone. Only allow access to sensitive personal information if you are using a "non-caching" app;
- For confidential messages use encryption software and SMS encryption software on both ends of the communication;
- Occasionally erase your smartphone using secure deletion techniques and reinstall from a "tested disk image." For added precaution use a desktop or laptop computer that is only

for this purpose. Never connect that computer or laptop to the Internet—but it should have the tested disk image and be kept in a secure location until needed.
- Create checks for text messaging fundraising campaigns that focus on authorization and verification procedures and early warning mechanisms to deal with pharming and phishing threats.

Election Enforcement Agencies (Department of Justice and States Attorneys Generals)

- Consider the importance of resources within the Voting Rights Division that can conduct computer forensics and investigations when evidence may be online.
- Provide for tools within law enforcement divisions to investigate and enforce election laws.

Approaches for Smartphone App Security

- Design apps that limit their capability and rely on users to give permission each time certain transactions are approved;
- Have new apps carefully checked by independent third party professional software assessors for flaws or bugs; employ techniques to check both for security weaknesses based on the app itself and the app's interaction with operating systems prior to release
- Allow remote app removal should apps become compromised;
- Show or remind smartphone users about their devices' backup and recovery features;
- Promote use of smartphones that offer additional layers of authentication or can give users additional protections;[63]
- Use available encryption options for voice calls as well as existing encryption and smartphone security features;
- Diversify the types of smartphones within a campaign or organization, making it more difficult to launch a successful attack against a particular candidate, campaign or party.

The future of campaign and politic communication is on mobile devices.[64] Regardless of the technology used to facilitate U.S. elections, individuals and groups need to protect themselves against online threats to personal autonomy and political freedom until business practices and government oversight functions evolve to meet Internet-based election challenges.

Contact:

Lillie Coney
Associate Director
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009 or http://epic.org
202-483-1140 x 111

[63] HOGBEN & DEKKER, *supra* note 17.
[64] JANNA QUITNEY ANDERSON & LEE RAINIE, PEW INTERNET & AM. LIFE PROJECT, THE FUTURE OF THE INTERNET III (2008), http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_FutureInternet3.pdf.pdf (concluding that the "mobile device will be the primary connection tool to the Internet for most people in the world in 2020").