DECEPTIVE PRACTICES 2.0: LEGAL AND POLICY RESPONSES

COMMON CAUSE, THE LAWYERS COMMITTEE FOR CIVIL RIGHTS UNDER LAW AND THE CENTURY FOUNDATION

THE CENTURY FOUNDATION

LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

COMMON CAUSE

This report was written with the enormous pro bono assistance of the law firms Morrison & Foerster L.L.P. and Ropes & Gray L.L.P.. For more information about Ropes & Gray L.L.P., please visit www.ropesgray.com, for more information about Morrison & Foerster, please visit www.mofo.com.

The myriad technological methods by which "e-deceptive practices" might be perpetrated are laid out in tremendous detail in the companion report to this produced by the Electronic Privacy Information Center, available at www.epic.org.

INTRODUCTION

In the last several election cycles, "deceptive practices" have been perpetrated in order to suppress voting and skew election results. Usually targeted at minorities and in minority neighborhoods, deceptive practices are the intentional dissemination of false or misleading information about the voting process with the intent to prevent an eligible voter from casting a ballot. It is an insidious form of vote suppression that often goes unaddressed by authorities and the perpetrators are virtually never caught. Historically, deceptive practices have taken the form of flyers distributed in a particular neighborhood; more recently, with the advent of new technology "robocalls" have been employed to spread misinformation. Now, the fear is deceptive practices 2.0: false information disseminated via the Internet, email and other new media.

In the past, the worst practices involved flyers distributed in predominantly minority communities. The 2004 presidential election cycle provides some particularly vivid examples. In Milwaukee, Wisconsin, fliers purportedly from the "Milwaukee Black Voters League" were distributed in minority neighborhoods claiming "If you've already voted in any election this year, you can't vote in the presidential election; If anybody in your family has ever been found guilty of anything, you can't vote in the presidential election; If you violate any of these laws, you can get ten years in prison and your children will get taken away from you." In Pennsylvania, a letter with the McCandless Township seal on it falsely informed voters that, to cut down on long lines, Republicans would vote on November 2 and Democrats would vote on November 3—the day after the election. Similar fliers were distributed at Ross Park Mall in Allegheny County. In Ohio, a so-called "Urgent Advisory" memo on phony Board of Elections letterhead warned voters that if they were registered by the NAACP, America Coming Together, the Kerry campaign, or their local Congressional campaign, they were disqualified and would not be able to vote until the next election.

More recently, automated calls, known as robocalls in the world of political campaigns, have been the weapon of choice. In 2006, the Secretary of State of Missouri, Robin Carnahan, reported that in one county, "robo-calls reportedly warned voters to bring photo ID to the polls or they would not be allowed to vote. There were also reports on the radio in Kansas City of automated telephone calls telling voters their polling places had been changed and giving incorrect polling place information."[1] According to the National Network for Election Reform, "Registered voters in Virginia, Colorado, and New Mexico reported receiving phone calls in the days before the election claiming that their registrations were cancelled and that if they tried to vote they would be arrested.[2] In Virginia, "Voters in Arlington, Accomack, Augusta, and Northampton counties in Virginia received phone calls on November 6 saying voters would be arrested if they attempted to vote on Election Day. Some of the phone calls also told voters that their polling locations had been moved, although none of the locations had changed."[3]

How might such activities translate online? Emails that appear to come from legitimate sources, such as a campaign, an elections office, a party or a nonprofit organization could be sent in a targeted fashion that contain false or misinformation about the voting time, place or process, or claiming that a poll site has been moved. Just at the time of this writing the first serious instance of email with bogus information came to light in Florida, where voters were receiving emails stating that voters whose ID failed to match a state database on Election Day would be turned away from the polls.[4]

Making matter worse, spyware could be used to collect information on a voter and their online behavior to better target deceptive emails.[5] Partisan mischief-makers with a bit of technological knowledge could spoof the official sites of secretaries of state, voting rights organizations or local election boards and advertise completely wrong information about anything from poll locations to voter identification requirements. Someone could also appropriate website names that are one letter off from the official site name—a typo domain or "cousin domain"—that appear to be an official site, and post phony information. Pharming—hacking into domain name system servers and changing Internet addresses—could be used to redirect users from an official site to a bogus one with bad information on it. As more and more people move from traditional phone lines to internet based calling platforms (known as VOIP or Voice Over Internet Protocol), deceptive robocalls might become even more pervasive as they will be virtually untraceable.

So far in this election cycle, these tactics have already been utilized to spread false information about candidates. Barack Obama has been the most prominent target of these attacks. Several emails have circulated widely which have titles such as "Who Is Barack Obama" and "Can a good Muslim become a good American." The content of the emails has often been the same, highlighting Obama's middle name of "Hussein" and incorrectly claiming he is of Muslim faith. While the Obama Campaign suffers through a seemingly unprecedented level of this activity, in 2004 supporters of Democratic Presidential candidate John Kerry were sent an email that looked almost exactly like official campaign emails, asking for donations. The email actually came from India and was a scam to steal people's money.[6]

Hillary Clinton did not fully escape such tactics either. The NAACP was forced to release on its website a statement from it's chairman Julian Bond stating that an email listing "10 Reasons Not to Vote for Hillary Clinton" supposedly authored by him was a hoax.

This year during the primaries, according to the online publication Wired, a series of false campaign websites materialized that appeared to be legitimate, such as FredThomsonForum.com, RudyGiulianiForum.com, and MittRomneyforum.com. Wired reported that these sites featured posts "under the impersonated names of popular political pundits and bloggers" and "promote misleading links to candidate sites that route to YouTube videos attacking them. Most posts adopt the persona of a supporter of the candidate, while offering views that amount to over-the-top parodies of genuine boosters."[7]

After the primaries, domain names with prospective and actual vice-presidential nominees' names popped up, leading to sites with unexpected information. For example, Obama-Biden.org and Obama-Biden.com diverted people to the website of the American Issues Project, an extremely anti-Obama third party organization. As reported by the Los Angeles Times, the McCain-Romney.com website took viewers to the "official home of the Hundred Year War…and Bush's Third Term!"[8]

An extensive analysis of abuse of campaign domain names found that, "Candidates have not done a good job at protecting themselves by proactively registering typo domains to eliminate potential abuse. In fact, we were only able to find one single typo web site that had been registered by a candidate's campaign - http://www.mittromny.com. All other typo domains were owned by other third parties that appeared unrelated to the candidate's campaign."[9]

This same study also enumerated several specific instances of "typo squatting" of domain names that were meant to look like actual campaign websites, including such gems as "narakobama.com" and mikehukabee.com."[10] These sites were either advertising sites or directed users to sites with "differing political views."[11]

Phony campaign websites have also been created to dupe people into making campaign donations that are really going into someone's pocket, not any campaign. In 2004, phishers (people who use e-mail to fraudulently obtain data from a user) set up a fictitious website purporting to be for the Democrats that stole the user's credit card number, and another site that had users call a for-fee 1-900 number.[12] This year, an Internet site was set up offering to register people to vote for $9.95, a process that is free.[13] In August 2008, the Federal Trade Commission issued a warning to consumers about voter registration scams. Prospective voters were receiving emails and phone calls from people claiming to be affiliated with an election board or civic group and asking for the person's social security number or credit card number to confirm eligibility or registration to vote. The FTC said the purpose was to commit identity theft.[14]

This report seeks to explore how such attacks might take place in the voting rights context and the measures that can be taken to contend with them effectively. The main focus of the report is an investigation into whether our existing state and federal legal structure is sufficiently equipped to deter and punish perpetrators of online deceptive practices. On the state level, we examine current anti-hacking and computer crimes laws, laws regarding the unauthorized use of state seals and insignia and impersonation of public officials, and voting rights laws. Each of these subsections is accompanied by recommendations for ways in which state laws can be improved to better address these types of serious transgressions. We also look extensively at current federal law, including the Voting Rights Act, copyright, trademark, anti-cybersquatting laws, the Computer Fraud and Abuse Act, the Wire Fraud Statute, Section 230 of the Communications Act, and the Can-Spam Act. Again, recommendations for improving federal law are offered.

We conclude with recommendations for those of us who are not prosecutors or technologists, especially elections officials, the campaigns, the media, including online media, voting rights and community groups, and of course, the voters.

STATE LAWS

I. VOTING RIGHTS LAWS

Each of the 50 states and the District of Columbia has laws involving voting rights and the administration of elections. Most states prohibit interference with the election process in some manner, but state statutes vary significantly in scope and application. For example, some state laws focus on interference with the physical act of voting by prohibiting "electioneering" within a certain proximity of the polling place. Others address manipulation of or tampering with ballots, voting machines, or registration logs. Still others outlaw behavior meant to harass, intimidate, or bribe voters. While these categories of laws are critical to ensuring the fair and effective administration of elections, some states have supplemented them with laws generally applicable to interference with the election process or dissemination of false information about voting procedures, candidates, or issues in the election. States that have these more general laws are better equipped to curtail deceptive practices, online or otherwise, in the voting process.

With the advent of online communications, the deceptive tactics once perpetrated through leaflets and phone calls may start to appear in e-mails and on websites. Many state legislatures have recently begun to enact laws that explicitly prohibit false statements or other types of voting fraud perpetrated in cyberspace, but if interpreted broadly, even most older statutes can effectively combat deceptive practices perpetrated online. The following sections detail general trends and important considerations associated with voting fraud laws in all 50 states and the District of Columbia.[15] The state statutes highlighted below are not necessarily models of best and worst practice, but they do provide examples of strong voting fraud provisions that can be used to combat electronic deceptive voting practices now and in the future.

LAWS PROHIBITING FALSE STATEMENTS

Almost all states have laws that prohibit false statements regarding elections, and these laws generally fall within 3 categories:

- ***Laws focused on process***: These laws typically prohibit the dissemination of false information relating to registration qualifications, election day identification requirements, polling place locations, and other procedural matters affecting the vote. For example, the Virginia statute makes it a misdemeanor to "knowingly communicate false election information to a registered voter about the time, date, or place of voting" and "to knowingly communicate false information concerning the voter's precinct, polling place, or a voter registration status." Va. Code Ann. § 24.2-1005.1.
- ***Laws focused on substance***: These laws typically prohibit the dissemination of false information about candidates or issues, rather than election or voting procedures. The Alaska and Wisconsin statutes both prohibit a person from knowingly making a false statement about a candidate that is intended to, or actually does, affect an election. Alaska Stat. § 15.56.14; Wis. Stat. § 12.05.
- ***Laws applicable to both process and substance***: The strongest state laws relating to false statements are those that are broadly applicable to false statements relating to an election, whether it be the procedural issues involved or the substantive issues relating to the candidate or ballot measures. For example, Louisiana law prohibits the distribution or transmission of any "oral, visual, or written material containing a false statement about a candidate. . . or proposition," La. Rev. Stat. Ann. §18:1463, as well as false information about any matter of "voting or. . . registration." *Id.* §18:1461, §18:1461.1.

Although the applicability of false statement provisions is somewhat limited by the process/substance constraints discussed above, these laws likely apply regardless of how the false statement is communicated. The statutes may not explicitly indicate that online or electronic communications are covered, but common terms found in the statutes such as "dissemination," "communicate," or "statement" are broad enough to encompass all forms of communication.

The Tension Between Free Speech and Laws Prohibiting False Statements:

Spotlight on Nevada

A concern surrounding laws dealing with political speech is the possible infringement on First Amendment freedom of speech rights. Accordingly, while voting fraud laws must be inclusive and apply broadly, legislatures must be careful to limit the laws' scope to speech not protected by the constitution. In addition to the content of the speech, due process (i.e., the way in which the law is enforced) concerns must also be considered.

In *Nevada Press Association v. Nevada Commission on Ethics*, the U.S. District Court for Nevada ruled that Nevada's voting fraud law was unconstitutional because the manner in which the law was enforced did not survive the strict judicial scrutiny required by First Amendment jurisprudence. Nevada Revised Statute § 294A.345 "prohibit[ed] any person from making a false statement, with actual malice, about a candidate for political office with the intent and effect of impeding the success of the candidate's campaign." Instead of resolving a claim through the state court system, a candidate claiming to be the victim of a false statement could file a request with the Nevada Ethics Commission within ten days of the alleged false statement. The Commission was required to hold a hearing within fifteen days of the request and give an opinion within three days of the hearing as to whether the statement was true or false. Although the false statement/actual malice framework of the statute survived the court's scrutiny, the court ultimately held the statute unconstitutional because the abbreviated dispute resolution procedure led by the Ethics Commission significantly deviated from civil and criminal standards of due process and greatly increased the chance of an erroneous decision.

In short, *Nevada Press Association* makes two clear points. First, any model statute that could potentially encroach on First Amendment protections should expressly include constitutionally required elements such as "actual malice," and, second, the manner in which a statute is enforced, i.e., due process, must be considered when analyzing the effectiveness and constitutional validity of a voting fraud statute.

LAWS THAT BROADLY PROHIBIT DECEPTIVE PRACTICES

The most effective way to combat online voting fraud is to broadly prohibit deceptive practices relating to an election or the casting of a vote. Many states have implemented laws to combat deception in the voting process, but no state's statute has emerged as a clear model for other states. The following state statutes, however, have provisions that would apply broadly to deceptive practices in the context of online voting fraud and may be useful for other states to consider:

- ***Alabama***: The Alabama statute prohibits "any person . . . by any [] corrupt means, from attempting to influence any elector in giving his/her vote, deterring the elector from giving the same, or disturbing or hindering the elector in the free exercise of the right of suffrage . . . ." Ala. Code § 17-17-38.

- ***Colorado***: The Colorado statute provides: "It is a crime to knowingly make, publish or circulate or cause to be made, published or circulated in any writing any false statement designed to affect the vote on any issue submitted to voters at any election or relating to any candidate for election to public office." Colo. Rev. Stat. § 1-13-109.

- ***Maine***: The Maine statute prohibits "any interference with a voter attempting to cast a ballot, or any attempt to influence a voter in marking his/her ballot." Me. Rev. Stat. Ann. tit. 21-A, § 674(1).

The above statutory provisions are not only broad enough to encompass nearly all *types* of deceptive practices (e.g., dissemination of false registration and polling place information, creation of phony "official" materials, or the spread of unfounded rumors about candidates), but are also expansive enough to cover deceptive practices perpetrated solely online. Also, the statutes featured above apply to deceptive practices generally regardless of whether the tactics are accompanied by bribery, intimidation, or harassment. While it is certainly understandable for state legislatures to focus on the most egregious types of voter interference, voters may also be disenfranchised as a result of simple misinformation disseminated by wrongdoers. Virginia and Missouri also have strong deceptive practices laws on the books.[16]

An Innovative Approach: Spotlight on California

In addition to the broadly applicable laws discussed above, California's "political cyberfraud" law is specifically designed to deter and penalize deceptive practices perpetrated online. Cal. Penal Code §§ 18320-23. California's political cyberfraud law makes it "unlawful for a person, with intent to mislead, deceive, or defraud, to commit an act of political cyberfraud." Political cyberfraud is defined as a knowing and willful act concerning a political website that is committed with the intent to deny a person access to a political website, deny a person the opportunity to register a domain name for a political website, or cause a person reasonably to believe that a political website has been posted by a person other than the person who posted the website, and would cause a reasonable person, after reading the website, to believe the site actually represents the views of the proponent or opponent of a ballot measure.

Political cyberfraud includes, but is not limited to, the following acts:

- Intentionally diverting or redirecting access to a political website to another person's website by the use of a similar domain name, meta-tags, or other electronic measures.
- Intentionally preventing or denying exit from a political website by the use of frames, hyperlinks, mousetrapping, popup screens, or other electronic measures.
- Registering a domain name that is similar to another domain name for a political website.
- Intentionally preventing the use of a domain name for a political website by registering and holding the domain name or by reselling it to another with the intent of preventing its use, or both.

While California's law should be expanded to cover all aspects of online election fraud rather than limiting it to political websites, it provides a fairly comprehensive framework for addressing online voter fraud.

LAWS THAT PROHIBIT TAMPERING WITH ELECTION OR CAMPAIGN MATERIALS

Even states that do not specifically prohibit false statements or deceptive practices perpetrated online may have provisions that combat misinformation in the voting process. Many states, for example, have laws addressing either election or campaign materials, such as prohibitions on the destruction of ballots, ballot box stuffing, or interference with the distribution of election or campaign information. The strongest statutory provisions in this category explicitly include electronic activity.

- ***Illinois***: The Illinois statute not only prohibits tampering with voting machines and placing anything other than a ballot in a ballot box, but it also makes it a felony to "destroy, mutilate, deface, falsify, forge, conceal or remove any record, register of voters, affidavit, return or statement of votes, certificate, tally sheet, ballot, or any other document or computer program . . ." in connection with an election. *See* 10 Ill. Comp. Stat. §§ 5/29-6, 5/29-7.

Not all statutes plainly cover electronic materials; a few are even explicitly restricted to physical materials and contain limiting terms such as "paper" or "card." For the most part, however, statutes that prohibit tampering with election materials can be interpreted to include electronic materials, such as e-mails, databases, documents, and websites. Below are examples of statutes that may be interpreted so as to apply to online tactics.

- ***Arizona***: Arizona law prohibits the delivery or mailing of "any document that falsely simulates a document from the government of this state, a county, city or town or any other political subdivision," where such mailing is done in an attempt to influence the outcome of an election. Ariz. Rev. Stat. § 16-925(A). Although the provision does not explicitly apply to online communications, the terms "mailing" and "document" could easily be interpreted by a creative prosecutor to include e-mails, websites, and the like.
- ***New Mexico***: New Mexico's law prohibits "printing, causing to be printed, distributing or displaying false or misleading" information relating to the voting or election process. N.M. Stat. Ann. § 1-20-9. This law was enacted in 1979, long before online communications, but could encompass printing from a computer rather than with a printing press, posting false information online that someone else subsequently prints, disseminating false information through e-mail, or displaying false information on a website or message board.

In general, a survey of state election laws indicates that most states have provisions that, if creatively applied, could serve to deter and to penalize many of the deceptive practices perpetrated online. Nevertheless, nearly all state laws in this context would benefit from close examination by their state legislatures, which should consider enacting laws to broadly prohibit those deceptive practices that have the potential of interfering with the campaign or election process.

RECOMMENDATIONS

- States *without* laws prohibiting deceptive practices in the context of an election should *enact* laws that explicitly cover such practices perpetrated online.
- States with laws *already* prohibiting deceptive practices in the context of an election should *amend* their laws to explicitly include such practices perpetrated online.
- States with content-specific false statements laws should expand their laws to explicitly include false statements about election and voting procedure.
- States prohibiting only bribes, threats, or other overtly coercive acts should expand their statutes to cover more clandestine practices (such as dissemination of false statements online).

State Laws Regarding Deceptive Voter Practices

State	False Statements Prohibited	Interference with or Fraud in the Election Process Prohibited	No Requirement that Intimidation, Bribery, or Threats be Present	Tampering with Election Materials Prohibited	Voting Laws Explicitly Applicable to Electronic or Online Activity
AL		1			
AK	2				
AZ	3				
AR					
CA					
CO		4			
CT	5				
DE					
DC					
FL					
GA					
HI					
ID					
IL					
IN					
IA					
KS					
KY					
LA					
ME					
MD					
MA				6	
MI	7				
MN					
MS	8				
MO					
MT					
NE		9			
NV					
NH					
NJ				10	
NM					
NY					
NC					
ND					
OH					
OK					
OR					
PA		11			
RI					
SC					
SD					
TN					
TX					
UT					
VT					
VA					
WA					
WV					
WI					
WY					

1. Alabama does not have specific fraud statutes related to the election, but it does prohibit official authorities and employers from unduly influencing voters' ability to vote freely.
2. Alaska's false information laws do not apply to attempts to spread false information about an election or registration; they only apply to false information about a candidate.
3. ARIZ. REV. STAT. §16-925(A) prevents the delivery or mailing of deceptive election documents in an attempt to influence the election.
4. COLO. REV. STAT. §1-13-201 prohibits interference with registration, but does not mention interference with the actual election.
5. Connecticut law prohibits issuing misleading instructions to voters.
6. The Massachusetts statute explicitly deals with voting lists, or registrations, and does not mention the actual election process.
7. This only applies to false statements about candidates.
8. The relevant statute also requires that someone be knowingly defrauded through the use of a false statement.
9. NEV. REV. STAT. §32-1538 prevents the fraudulent assistance of an illiterate voter. There are also statutes dealing with interference with the election process.
10. New Jersey law prohibits the dissemination of false election materials.
11. Pennsylvania primarily prohibits interfering with elected officials.

State	Abbreviation	Statute Reference(s)
Alabama	AL	Ala. Code §§ 13A-11-8, 17-17-4, 17-9-50, 17-5-17, 17-17-38, 17-17-39, 17-17-44, 17-17-45, 17-24-4
Alaska	AK	Alaska Stat. §§ 15-56-14, 15-56-25
Arizona	AZ	Ariz. Rev. Stat. §§ 16-1006(A), 16-1017(6), 16-925(A)
Arkansas	AR	Ark. Code Ann. §5-42-102
California	CA	Cal. Elec. Code §§ 18320, 18500, 18540, 18564
Colorado	CO	Colo. Rev. Stat. §§ 1-13-109, 1-13-112, 1-13-201, 1-13-713
Connecticut	CT	Conn. Gen. Stat. §9
Delaware	DE	Del. Code. Ann. §§ 5161, 5162, 5123, 5116, 5117, 5118, 5125, 5139
District of Columbia	DC	
Florida	FL	Fla. Stat. §§ 104.012, 104.041, 104.0515, 104.061, 104.091
Georgia	GA	Ga. Code Ann. §21-2-567
Hawaii	HI	Haw. Rev. Stat. §§ 19-3, 19-4, 19-6
Idaho	ID	Idaho Code Ann. §§ 18-2305, 18-101
Illinois	IL	Ill. Comp. Stat. §§ 5/29-1, 5/29-2, 5/29-4, 5/29-6, 5/29-7, 5/29-10–13, 5/29-17–18
Indiana	IN	Ind. Code §§ 3-14-3-10, 3-14-3-21.5
Iowa	IA	Iowa Code §39
Kansas	KS	Kan. Stat. Ann. §§ 24-2415, 25-2407, 25-2414, 25-2426, 25-2433
Kentucky	KY	Ky. Rev. Stat. Ann. §§ 119.155, 119.255, 119.275, 119.305, 119.315, 119.345, 119.335
Louisiana	LA	La Rev. Stat. Ann. §§ 18:Et Seq, 18:1463, 18:1461, 18:1461.1
Maine	ME	Me. Rev. Stat. Ann. tit. 17-A, §§ 603, 2931, Me. Rev. Stat. Ann. tit. 21-A, § 674(1)
Maryland	MD	Md. Code Ann., Elec. Law §16
Massachusetts	MA	Mass. Gen. Laws ch. 56, § 29, Mass. Gen. Laws ch. 56, § 42, Mass. Gen. Laws ch. 56, § 39, Mass. Gen. Laws ch. 56, § 43, Mass. Gen. Laws ch. 56, § 10, Mass. Gen. Laws ch. 56, § 23, Mass. Gen. Laws ch. 56, § 30.
Michigan	MI	Mich. Comp. Laws §§ 168.931, 168.932(A), 168.944
Minnesota	MN	Minn. Stat. §§ 204C.06, Subd., 1, 204C.06, Subd., 3, 204C.035
Mississippi	MS	Miss. Code Ann. §§97-13-37, 97-13-39, 97-45-3, 97-13-21
Missouri	MO	Mo. Rev. Stat. §§ 115.631, 115. 633, 115.635, 115.637
Montana	MT	Mont. Code Ann. §§ 13-35-206, 13-35-208, 13-35-217, 13-35-218, 13-35-103
Nebraska	NE	Neb. Rev. Stat. §32
Nevada	NV	Nev. Rev. Stat. §§ 293.700–293.840
New Hampshire	NH	N.H. Rev. Stat. Ann. §§ 652–671
New Jersey	NJ	N.J. Stat. Ann. §§ 2C:28-8, 19:34-29, 19:34-1.1, 19:34-28, 19:34-46, 19:34-66, 19:34-68
New Mexico	NM	N.M. Stat. §1-20-9
New York	NY	N.Y. Elec. Law §17-166
North Carolina	NC	N.C. Gen. Stat. §163-275
North Dakota	ND	N.D. Cent. Code §12.1–14-02
Ohio	OH	Ohio Rev. Code Ann. §3599
Oklahoma	OK	Okla. Stat. §§ 76-3–4, 16-113
Oregon	OR	Or. Rev. Stat. §164.377
Pennsylvania	PA	25 P.S. §§ 3527, 3547
Rhode Island	RI	R.I. Gen. Laws §§ 17-19-42, 19-19-43, 17-19-46, 17-23-1, 17-23-2, 17-23-17
South Carolina	SC	S.C. Code Ann. §§ 7-25-80, 7-25-190, 7-25-180
South Dakota	SD	S.D. Codified Laws §§ 12-26-10-11, 12-26-15, 12-26-12
Tennessee	TN	Tenn. Code Ann. §§ 2-19-142, 1-19-116, 2-19-103
Texas	TX	Tex. Elec. Ann. § 61
Utah	UT	Utah Code Ann. §§ 20A-4-501(1)(C), 20A-3-502(1)(B)
Vermont	VT	Vt. Stat. Ann. tit. 17, §§ 2017, 2019, 1972
Virginia	VA	Va. Code Ann. §24.2-1005.1
Washington	WA	Wash. Rev. Code §29A.8.630
West Virginia	WV	W. Va. Code §§ 3-8-11, 3-9-10
Wisconsin	WI	Wis. Stat. §§ 12.05, 12.09

II. PROHIBITING THE IMPERSONATION OF PUBLIC OFFICIALS

Most states have laws that prohibit the impersonation of public officials/public servants. Notably, certain of these states have impersonation laws directly related to the election process.

GENERAL STATE IMPERSONATION LAWS

Many states have general laws regarding the impersonation of public officials/public servants that merely prohibit such impersonation. Such state laws appear to be quite broad and there appears to be no case law on point addressing whether such laws would apply to impersonation of public officials/public servants in connection with voter deception practices. Presumably, these laws could be applied to online voter deception practices. For example, such laws may apply if an impersonator via a website or email communication deceives voters by 1) impersonating a public official, including an election official, where the impersonator distributes false information relating to polling places, voting requirements, or the like, or 2) creating a website that is made to appear as the official site of a state's Secretary of State or claiming to be the state's Secretary of State. Notably, effective November 1, 2008, New York will have a new law that makes it a violation of its Penal Law to impersonate another "by communication by Internet website or electronic means with intent to obtain a benefit or injure or defraud another, or by such communication pretends to be a public servant in order to induce another to submit to such authority or act in reliance on such pretense." NY Penal Law § 190.25.

STATE IMPERSONATION LAWS SPECIFIC TO THE ELECTION PROCESS

As previously mentioned, there are a few states that have enacted impersonation laws specifically related to the election process. For example, Alabama prohibits fraudulently misrepresenting oneself or other persons/organizations as speaking, printing, acting for or on behalf of a candidate, political campaign committee or political party in a manner that is damaging/intended to damage such person/entity. ala. code § 17-5-16. Maryland prohibits the impersonation of a voter and attiring/equipping someone to give the impression of performing a government function in connection with an election. Md. code ann. elec. law §§ 16-101 and 16-903. Massachusetts prohibits interference with election officials. mass. gen. laws ch. 56, § 48. Impersonation of an election official may qualify as interfering. Nebraska prohibits the impersonation of an elector to register voters. Neb. Rev. stat. § 32-1503. Presumably, such laws may apply to online voter deception practices.

STATES WITH NO LAWS PROHIBITING IMPERSONATION OF PUBLIC OFFICIALS

There are a handful of states that do not have any laws regarding the impersonation of public officials. See the corresponding chart entitled "*State Laws Prohibiting Impersonation of Public Officials*" for the identification of such states.

RECOMMENDATIONS

Based on the existing state laws prohibiting the impersonation of public officials, the following is recommended:

- States *without* laws prohibiting the impersonation of public officials should *enact* laws that cover the impersonation of public officials, explicitly prohibiting the impersonation of public officials a) online or by other electronic means and b) in connection with the election process.

- States with laws *already* prohibiting the impersonation of public officials not expressly related to the election process should *amend* their laws to explicitly prohibit the impersonation of public officials a) online or by other electronic means and b) in connection with the election process.

- States with laws *already* prohibiting the impersonation of public officials in connection with the election process should *amend* their laws to enhance such prohibitions and explicitly prohibit the impersonation of public officials online or by other electronic means.

State Laws Prohibiting Impersonation of Public Officials

State	Fraudulently misrep. self or another/org. as printing, acting for/on behalf of a candidate, political party or committee that damages/ is intended to damage such person/org.	Prohibited from impersonating a public servant or official, i.e. officer/ employee of gov't *(Eff. 11/1/08, NY law will specifically cover comm. by web/electronic means)*	Assuming false identity with intent to defraud; or pretending to be rep. of person/ org. with intent to defraud	Prohibited from impersonating a public officer	General false impersonation with intent to gain a benefit for self or another or to injure, or defraud another	Prohibits impersonating a political party officer
AL	■					
AK		■				
AZ		■	■			
AR						
CA				■		
CO		■			■	
CT						
DE						
DC				■		
FL						
GA				■		
HI						
ID		■				
IL				■		
IN		■				
IA						
KS				■		■
KY		■				
LA					■	
ME		■				
MD						
MA						
MI						
MN				■		
MS		■				
MO						
MT		■				
NE		■	■			
NV				■		
NH						
NJ						
NM						
NY		■				
NC						
ND		■				
OH						
OK						
OR		■				
PA		■				
RI				■		
SC		■				
SD				■		
TN		■				
TX		■				
UT		■				
VT				■		
VA						
WA		■				
WV				■		
WI				■		
WY						

State	Prohibited from impersonating a voter	Prohibited from attiring/ equipping someone to give impression performing gov't function in connection with an election	Prohibited from impersonating state officers	Prohibited from disguising oneself to obstruct law, disguising oneself as an election official to violate election law	Prohibits interfering with election officials	Prohibits impersonation of an elector to register voters	None
AL							
AK							
AZ							
AR							
CA							
CO							
CT							
DE							
DC							
FL							
GA							
HI							
ID							
IL							
IN							
IA							
KS							
KY							
LA							
ME							
MD							
MA							
MI							
MN							
MS							
MO							
MT							
NE							
NV							
NH							1
NJ							
NM							
NY							
NC							2
ND							
OH							3
OK							
OR							
PA							
RI							
SC							
SD							
TN							
TX							
UT							
VT							
VA							1
WA							
WV							
WI							
WY							1

Statute References

State	Abbreviation	Statute Reference(s)
Alabama	AL	Ala. Code § 17-5-16
Alaska	AK	Alaska Stat. Tit. 11, ch. 56, Art. 5
Arizona	AZ	Ariz. Rev. Stat. §§ 13-105(33)(a), 13-2006 and 13-2406
Arkansas	AR	N/A
California	CA	Cal. Penal Code § 538(g)
Colorado	CO	Colo. Rev. Stat. §§ 24-80-902 and 24-80-903
Connecticut	CT	N/A
Delaware	DE	N/A
District of Columbia	DC	D.C. Code § 22-1403
Florida	FL	N/A
Georgia	GA	Ga. Code Ann. § 16-10-23
Hawaii	HI	N/A
Idaho	ID	Idaho Code Ann. §§ 18-3005 and 34-108
Illinois	IL	Ill. Comp. Stat. 5132-5
Indiana	IN	Ind. Code § 35-44-2-3
Iowa	IA	Iowa Code Tit. XVI, Subtit. 1, ch. 718.2
Kansas	KS	Kan. Stat. Ann. §§ 21-3824 and 25-2424
Kentucky	KY	Ky. Rev. Stat. Ann. §§ 519.010(3) and 519.050
Louisiana	LA	La Rev. Stat. Ann. § 14:112
Maine	ME	Me. Rev. Stat. Ann. tit. 17-A, § 457
Maryland	MD	Md. Code Ann., Elec. Law §§ 16-101, 16-201 and 16-903
Massachusetts	MA	Mass. Gen. Laws ch. 56, § 48 and ch. 268 §§ 33 and 34
Michigan	MI	Mich. Comp. Laws § 750.217
Minnesota	MN	Minn. Stat. § 609.475
Mississippi	MS	Miss. Code Ann. § 97-7-43
Missouri	MO	N/A
Montana	MT	Mont. Code Ann. § 45-7-209
Nebraska	NE	Neb. Rev. Stat. §§ 28-608, 28-609 and 32-1503
Nevada	NV	Nev. Rev. Stat. Ann. § 199.430
New Hampshire	NH	N/A
New Jersey	NJ	N/A
New Mexico	NM	N/A
New York	NY	N.Y. Penal Law § 190.25
North Carolina	NC	N/A
North Dakota	ND	N.D. Cent. Code § 12.1-13-04
Ohio	OH	N/A
Oklahoma	OK	N/A
Oregon	OR	Or. Rev. Stat. § 162.365
Pennsylvania	PA	18 Pa. Cons. Stat. § 4912
Rhode Island	RI	R.I. Gen. Laws § 11-14-1
South Carolina	SC	S.C. Code Ann. § 16-17-735
South Dakota	SD	S.D. Codified Laws § 3-1-9
Tennessee	TN	Tenn. Code Ann. § 39-16-301
Texas	TX	Tex. Penal Code Ann. § 37.11
Utah	UT	Utah Code Ann. § 76-8-512
Vermont	VT	Vt. Stat. Ann. tit. 13, ch. 67 §§ 1705 and 3002
Virginia	VA	N/A
Washington	WA	Wash. Rev. Code § 9A.60.040
West Virginia	WV	W. Va. Code § 61-5-27
Wisconsin	WI	Wis. Stat. § 946.69
Wyoming	WY	N/A

1: State law is limited to impersonation of a police officer;
2: State law is limited to impersonation of police officers and emergency personnel;
3: State law is limited to impersonation of state representatives and police officers.

III. THE UNAUTHORIZED USE OF STATE SEALS AND INSIGNIA

Approximately half of the states have laws regarding the unauthorized use of state seals and insignia. Of these states, most of them broadly prohibit the unauthorized use of state seals. Accordingly, such laws could be applied to disenfranchisement efforts such as use of online and digital communications that bear a seal or insignia that is deceptively similar to an official seal in an effort to deceive voters. Certain states have gone even further to specifically address the unauthorized use of a state seal in a political advertisement or campaign. On the other hand, there are a few states that do not broadly prohibit the unauthorized use of a state seal and only prohibit the use of a state seal for advertising or a commercial purpose. The state laws referenced above are summarized in more detail below and in the corresponding chart entitled "*State Laws Regarding Unauthorized Use of State Seals and Insignia.*"

PROHIBITING USE OF STATE SEAL FOR COMMERCIAL V. NON-COMMERCIAL PURPOSE

A few states such as Alaska, Massachusetts, Rhode Island and South Dakota prohibit the use of their state seals for advertising or a commercial purpose. Such state laws do not appear to be applicable to disenfranchisement efforts unless there is some other commercial purpose to such efforts. All of the other states that have laws regarding the unauthorized use of state seals do not limit such laws to prohibiting the use of a state seal for a commercial purpose. Accordingly, the unauthorized use of such a state seal in an effort to disenfranchise voters via websites, email communications or otherwise could presumably fall within these states' statutes.

PROHIBITING USE OF STATE SEAL ON DOCUMENTS V. ELECTRONIC SOURCES

A few states limit their laws regarding the unauthorized use of a state seal to use of the state seal on a document. For instance, in relevant part, Florida prohibits sending any letter, paper or document which simulates the state seal with the intent to mislead. Fla. Stat. § 817.38(1). On its face, Florida's law does not appear to apply to websites or email communications.

A number of states, however, have state laws regarding the unauthorized use of a state seal that broadly prohibit the unauthorized/improper use of such seal and do not appear to be similarly limited. Such state laws presumably would cover disenfranchisement of voters via websites or email communications. For instance, such laws may prohibit the use of a state seal in connection with deceptive online and digital communications that bear a seal or insignia that is deceptively similar to an official seal. Such state laws may be useful tools against false websites or electronic communications that use a state seal in order to convey the appearance of authenticity.

PROHIBITING USE OF A STATE SEAL IN A POLITICAL ADVERTISEMENT/CAMPAIGN

A few states have laws that, under certain circumstances, prohibit the use of a state seal in a political advertisement or campaign. For instance, Washington prohibits the use of the state seal in political campaigns to assist/defeat any candidate. Wash. Rev. Code § 43.04.050. In addition, Texas makes it is a criminal offense for a person other than a political officeholder knowingly to use a representation of the state seal in political advertising. Tex. Elec. Code § 255.006(d), (e) "'Political advertising' is defined as a communication supporting or opposing a candidate for nomination or election to a public office or office of a political party, a political party, a public officer, or a measure that (A) in return for consideration, is published in a newspaper, magazine, or other periodical or is broadcast by radio or television; or (B) appears: (i) in a pamphlet, circular, flier, billboard or other sign, bumper sticker, or similar form of written communication; or (ii) on an Internet website." Tex. Elec. Code § 251.001(16). If any website or electronic communication incorporating the Texas state seal qualifies as political advertising, it would be reached by this statute.

STATES WITH NO LAWS REGARDING UNAUTHORIZED USE OF STATE SEALS

Approximately half of the states do not have any laws regarding the unauthorized use of state seals and insignia. As referenced above, see the corresponding chart entitled "*State Laws Regarding Unauthorized Use of State Seals and Insignia*" for the identification of such states.

RECOMMENDATIONS

Based on the existing state laws regarding the unauthorized use of state seals, the following is recommended:

- States *without* laws prohibiting the unauthorized use of their state seals should *enact* laws that cover the unauthorized use of their state seals, explicitly prohibiting the unauthorized use of their state seals a) online or by other electronic means and b) in connection with a political advertisement or political campaign.

- States with laws *already* prohibiting the unauthorized use of state seals that do not expressly relate to the use of a state seal in a political advertisement or political campaign should *amend* their laws to explicitly prohibit the unauthorized use of their state seals a) online or by other electronic means and b) in connection with a political advertisement or political campaign.

- States with laws *already* prohibiting the unauthorized use of state seals in connection with the use of a state seal in a political advertisement or political campaign should *amend* their laws to explicitly prohibit the unauthorized use of their state seals online or by other electronic means.

State Laws Regarding Unauthorized Use of State Seals and Insignia

State	Cannot use state seal for advertising or commercial purpose, unless obtain written permission	Prohibits persons other than political officeholders from using state seal in political advertising	Cannot use state seal, without obtaining permission, or otherwise allowed by statute	Cannot willfully use insignia of a state with intent of fraudulently impersonating a state	Only Secretary of State can use/affix state seal	Prohibits counterfeiting seal of state, county, etc.
AL						
AK						
AZ						
AR						
CA						
CO						
CT						
DE						
DC						
FL						
GA						
HI						
ID						
IL						
IN						
IA						
KS						
KY						
LA						
ME						
MD						
MA						
MI						
MN						
MS						
MO						
MT						
NE						
NV						
NH						
NJ						
NM						
NY						
NC						
ND						
OH						
OK						
OR						
PA						
RI						
SC						
SD						
TN						
TX						
UT						
VT						
VA						
WA						
WV						
WI						
WY						

State	Cannot send paper document which simulates seal with intent to mislead to obtain more things of value	Prohibits unauthorized / improper use of state seal	Cannot affix state seal on docs	Cannot register mark if it comprises state insignia	Prohibits false alteration of a gov't record and use of/ tampering with a gov't record	Prohibits use of state seal in political campaign to assist/ defeat any candidate	None
AL							
AK							
AZ							
AR							
CA							
CO							
CT							
DE							
DC							
FL							
GA							
HI							
ID							
IL							
IN							
IA							
KS							
KY							
LA							
ME							
MD							
MA							
MI							
MN							
MS							
MO							
MT							
NE							
NV							
NH							
NJ							
NM							
NY							1
NC							
ND							
OH							
OK							
OR							
PA							
RI							
SC							
SD							
TN							
TX							
UT							
VT							2
VA							
WA							
WV							
WI							
WY							

1: New York has a statute that prohibits intentional alteration of object to give it source of authorship it does not actually possess (could apply to creation of phony website or election information)

2: Vermont only has a statute regarding use of state seal for commemorative medals or for public displays not connected with any advertisements.

State	Abbreviation	Statute Reference(s)
Alabama	AL	N/A
Alaska	AK	Alaska Stat. Tit. 44, ch. 9
Arizona	AZ	Ariz. Rev. Stat. § 41-130
Arkansas	AR	N/A
California	CA	Cal. Penal Code § 538(g)
Colorado	CO	Colo. Rev. Stat. §§ 18-5-113 and 18-8-113
Connecticut	CT	Conn. Gen. Stat. ch. 942 § 53-153
Delaware	DE	N/A
District of Columbia	DC	N/A
Florida	FL	Fla. Stat. § 817.38(1)
Georgia	GA	Ga. Code Ann. § 50-3-32(c)
Hawaii	HI	Haw. Rev. Stat. § 5-6
Idaho	ID	Idaho Code Ann. § 18-3603
Illinois	IL	N/A
Indiana	IN	N/A
Iowa	IA	Iowa Code Tit. XVI, Subtit. 1, ch. 718.5
Kansas	KS	N/A
Kentucky	KY	N/A
Louisiana	LA	N/A
Maine	ME	N/A
Maryland	MD	Md. Code Ann., Crim. Law § 8-607
Massachusetts	MA	Mass. Gen. Laws ch. 264, § 5
Michigan	MI	N/A
Minnesota	MN	N/A
Mississippi	MS	N/A
Missouri	MO	N/A
Montana	MT	N/A
Nebraska	NE	N/A
Nevada	NV	Nev. Rev. Stat. Ann. § 235.010
New Hampshire	NH	N/A
New Jersey	NJ	N.J. Stat. Ann. § 52:2-4
New Mexico	NM	N/A
New York	NY	N/A
North Carolina	NC	N/A
North Dakota	ND	N.D. Cent. Code § 47-22-02
Ohio	OH	N/A
Oklahoma	OK	N/A
Oregon	OR	Or. Rev. Stat. § 186.023
Pennsylvania	PA	N/A
Rhode Island	RI	R.I. Gen. Laws § 11-15-4
South Carolina	SC	N/A
South Dakota	SD	S.D. Codified Laws § 1-6-3.1
Tennessee	TN	Tenn. Code Ann. § 39-16-504
Texas	TX	Tex. Elec. Code Ann. §§ 251.001(16) and 255.006(d), (e)
Utah	UT	Utah Code Ann. § 76-8-512
Vermont	VT	N/A
Virginia	VA	Va. Code Ann. § 1-505
Washington	WA	Wash. Rev. Code §§ 43.04.040 and 43.04.050
West Virginia	WV	W. Va. Code § 61-4-2
Wisconsin	WI	N/A
Wyoming	WY	N/A

IV. ANTI-HACKING AND COMPUTER CRIMES LAWS

Each of the 50 states has some form of computer crimes or anti-hacking laws on the books.[17] Most states broadly prohibit any unauthorized access to a computer, for any purpose. Almost without exception, these laws could be creatively applied to hacking or to any use of spyware that would redirect search queries or deny voters access to legitimate websites. There are many ways in which these laws could be expanded, from proscribing harsher penalties to covering different types of electronic devices and deceptive behaviors. Presently, many states reserve their harshest penalties for unauthorized access to a computer that results in damage, involves certain types of malicious intent, or interferes with vital government or public services. It is not always clear whether these laws would apply to online deceptive practices. Finally, 13 states have stand-alone statutes specifically prohibiting the installation and use of spyware.

LAWS PROHIBITING UNAUTHORIZED ACCESS TO A COMPUTER OR NETWORK

The most common form of computer crimes law prohibits, at minimum, any "unauthorized access" to a computer, computer system, or computer network. In most states, the unauthorized access is illegal regardless of the defendant's intentions or damage caused. It seems clear that most spyware and hacking activities would qualify as "unauthorized access" and would be illegal, because this type of online deceptive practice usually involves the clandestine installation of software on the voter's computer.

A small number of states require that the perpetrator actually "use" the victim's computer in some way before triggering a penalty. Even in these states, the installation of software would likely qualify as "use" of the voter's computer, because the perpetrator is using the voter's computer to redirect search queries or domain names. The application of generic "unauthorized access" laws to electronic voting fraud is in question only in a few states. In eight jurisdictions, penalties are available only if the perpetrators intended to cause some type of damage. In these states, prosecutors must prove that the perpetrators' access was not only unauthorized, but that it was accompanied by a specified level of intent (e.g., malicious intent, intent to defraud, etc .).

In addition to the baseline unauthorized access laws, most jurisdictions have also defined several more serious computer crimes. These statutes typically carry enhanced penalties, but it is not always clear whether voter deception tactics would be actionable under these provisions. Categories of computer crime are generally distinguished based on the following considerations:

The perpetrator's mental state (i.e., did the perpetrator act willfully, knowingly, maliciously, or with intent to defraud?).

Whether the perpetrator caused any damage to the computer, or to the computer's owner.

The amount and type of damage caused.

Whether the unauthorized access interfered with certain public services (e.g., medical or emergency services).

Whether the access was designed to facilitate identity theft.

Punishments for unauthorized access vary significantly from state to state and may become more severe based on the above considerations. In general, jurisdictions treat mere "unauthorized access" as a misdemeanor-level offense.

Spotlight on Pennsylvania

Pennsylvania presents a good example of the types of behaviors contemplated by state computer crimes laws. 18 Pa. Cons. Stat. § 7611 prohibits mere unauthorized access or use of a computer. Section 7612, on the other hand, prohibits any scheme to block or impede a user's access to computer services. Other sections prohibit the theft of data (§ 7613), possession of unauthorized copies of computer data (§ 7614), and any unauthorized interference with another person's computer (§ 7615). Someone who hacked into a computer or used spyware to redirect search queries could be prosecuted under any of these sections. Each of these offenses is a third degree felony, subject to up to seven years' imprisonment.

The names used by each state to describe the computer crime laws also vary significantly. Some examples include:

Arizona: "Computer tampering."
Alabama: "Offenses against intellectual property."
Kentucky: "Unlawful access to a computer."
Montana: "Unlawful use of a computer."
Oregon: "Computer crime."
Washington: "Computer trespass."

OPTIONS FOR EXPANDING THE SCOPE OF LAWS ALREADY ON THE BOOKS

Although the great majority of the unauthorized access laws can be applied to deceptive practices based on their plain meaning, a creative prosecutor could interpret the following commonly-used statutory terms so as to enhance the penalties available against perpetrators.

"Scheme or artifice to defraud": This phrase could be defined to include schemes to defraud a voter of his or her constitutional right to vote. At present, most states treat fraud as a purely financial or property-based crime. An expansive interpretation of fraud could include schemes to deprive persons of their *civil* rights as well as schemes to defraud persons of property. In many states, proving a perpetrator's intent to defraud opens the door to much harsher penalties than for mere unauthorized access to a voter's computer.

Spotlight on Ohio

Ohio's "defraud" definition is a model for broad applicability of the computer crimes laws. " 'Defraud' means to knowingly obtain, by deception, some benefit for oneself or another, or to knowingly cause, by deception, some detriment to another." Ohio Rev. Code Ann. § 2913.01(B). There is a strong argument that the loss of one's voting rights would qualify as a detriment to the voter under this definition.

"Computer, computer system, or computer network": This phrase could be defined to include all sorts of electronic devices, including PDAs and cell phones. As the variety of devices capable of connecting with the internet expands, computer crimes laws should be expanded to keep pace with technology.

"Interference with governmental operations": At present, seven states allow for enhanced penalties if unauthorized access to a computer interrupts or interferes with a "governmental operation." At present it is unclear whether an election would be considered a governmental operation. Some states seem to focus on vital public and governmental services such as police, fire and emergency medical services, and will only enhance penalties if the perpetrator's actions put the public at risk.

Another option for strengthening the deterrent effect of the already broad unauthorized access laws is to define each redirected search query or installation of software as a separate, chargeable offense. Very few states define what constitutes a single chargeable event. South Carolina treats each affected computer as a separate violation. S.C. Code Ann. § 16-16-20(5). Tennessee groups all of the violations resulting from any single action and treats them as one chargeable event. Tenn. Code Ann. § 47-18-5204(e). If a prosecutor were willing to take a more expansive view, she could charge each redirected search query or each installation of software as a separate offense. Even though the maximum fines and jail times are generally low for unauthorized access to a computer, these penalties could quickly add up if violators were charged separately for each offense.

Many states reserve the harshest penalties for computer crimes that result in significant financial loss. In these jurisdictions, fines and jail time escalate depending on the amount of monetary damage caused by the perpetrator. Because it is difficult to attach a dollar value to one's voting rights, however, penalties based on the amount of monetary loss are not easily applied to online deceptive practices. Instead, states should expand the harshest penalty provisions to include computer crimes that disrupt elections or interfere with voting rights.

Similarly, many states have laws restricting the creation of false websites, or the transmission of messages from false addresses. At present, these laws focus almost exclusively on the collection of identifying personal financial information (credit card numbers, bank account numbers, etc.), and could not easily be applied to the deceptive practices context. With a little tweaking, however, these laws could be used to prosecute individuals who create phony Secretary of State websites, or send false information about polling places. Because the framework is already there, it is just a matter of expanding these laws to address non-commercial deceptive practices.

Spotlight on Louisiana

Louisiana's Anti-Phishing Law is a good example of a web-crimes statute that is prohibitively limited to the commercial context. La Rev. Stat. Ann. § 2022 prohibits the creation of a web page or a domain name for fraudulent purposes. Unfortunately, the offense is only chargeable if the defendant created the website with the intent to collect identifying information (a term of art, narrowly limited to financial data) about the computer user.

STATES WITH INNOVATIVE LAWS

Several states have stepped outside of the "unauthorized access" computer crimes mold and have enacted innovative electronic "false statements" laws that may be applicable to online deceptive practices other than mere "unauthorized access."

Georgia: Georgia prohibits the transmission of any data over the internet that includes false identification or representation. GA. CODE ANN. § 16-9-93.1 This statute is not limited to the commercial context, and explicitly prohibits the use of a logo or legal or official seal. Prosecutors in Georgia would have no trouble using this law to go after individuals creating phony Secretary of State websites, or individuals who send e-mails purportedly from the Election Board, police department, or other official source. A 1997 United States District Court opinion enjoined the application of this statute on First Amendment grounds (*American Civil Liberties Union of Georgia v. Miller*, 977 F.Supp. 1228 (N.D. Ga. 1997)), but the statute remains on the books and may still be enforceable in Georgia state courts.

Mississippi: Mississippi broadly prohibits the posting of any message through electronic media for the purpose of causing injury to any person. MISS. CODE ANN. § 97-45-17. If spyware is installed on a voter's computer with the intention of causing injury (either by keeping that voter from exercising his or her constitutional right to vote, or by influencing the voter to vote for a candidate through fraudulent means), this statute could be used to prosecute those online deceptive practices.

Ohio: Ohio prohibits tampering with electronic writings or records, and also punishes the transmission or use of falsified electronic documents. OHIO REV. CODE ANN. § 2913.42. At present, this statute has primarily been used to prosecute corruption and schemes to defraud the government (e.g., money laundering and theft in office, submission of false daily activity reports, etc.). But it could conceivably be used to prosecute creators of false official websites or senders of false e-mails from candidates, election authorities, or other official sources.

Pennsylvania: Pennsylvania's generic computer crimes statute contains a prohibition on unauthorized access to a website or telecommunications device. PA. CONS. STAT. § 7611(a)(2). Pennsylvania also prohibits schemes to disrupt service to a website. PA. CONS. STAT. § 7612. This broad definition of unauthorized access covers online deceptive practices without requiring installation of software onto the voter's computer. As hacking techniques evolve and become more sophisticated, this type of broad-based definition may be necessary.

Rhode Island: In Rhode Island, the intentional transmission of false data for any purpose is illegal. R.I. GEN. LAWS § 11-52-7. This law could be used to prosecute anyone who creates a false website or sends an e-mail with false voting information.

Tennessee: It is illegal to duplicate or mimic any portion of a website in Tennessee. TENN. CODE ANN. § 47-18-5203(c). The statute also prohibits false use of a trademark, logo, or name on a website, as well as the creation of false links that redirect users to a different website. This law would easily cover most online deceptive practices that do not involve unauthorized access to the voter's computer.

STATES WITH SPYWARE LAWS

Although spyware could be prosecuted under most states' generic computer crimes laws, 13 states have stand-alone statutes specifically addressing spyware. These statutes generally prohibit installation of software that does one or all of the following things:

- Modifies browser settings.
- Collects personal identifying or financial information.
- Collects keystroke information.
- Prevents removal of the software.
- Misrepresents that the software has been removed.
- Modifies security settings on the user's computer.
- Takes control of the computer in some way.

The uniformity of state law on this issue indicates that many states are following some form of model statute to enact their spyware laws. A representative example of this model statute format is ARIZ. REV. STAT. § 44-7301 *et seq*. An example of a particularly ineffective spyware law is ALASKA STAT. § 45.45-.792 *et seq*. Alaska prohibits only spyware that causes pop-up ads to appear on the user's computer screen.

In general, the states that have spyware laws would be good test-states for prosecuting online deceptive practices involving use of spyware. Although the unauthorized access statutes would likely also cover this deceptive behavior, the statutory violation in states with spyware laws would seem to be easier to prosecute.

RECOMMENDATIONS

- Most states' generic computer crimes laws *could* apply to spyware, but it would be better if this were not left up to prosecutors to decide. States that do not have separate laws could generally benefit from having a separate, well-defined statute prohibiting spyware.

- State fraud statutes should explicitly address fraud related to voting rights (most states focus only on financial harm, not on harm to the victim's constitutional rights).

- Statutory definitions of computers, computer systems, and/or computer networks should be expanded to include cell phones, blackberries, and other portable electronic devices.

- Computer crimes committed with intent to disrupt an election should be subject to harsher penalties than other types of "unauthorized access" to a computer. For example, statutes should provide enhanced penalties for interference with essential government functions and should make clear that an election is included within that definition. The existence of enhanced penalties increases the deterrent effect of these laws.

- Many states have anti-spyware and anti-phishing statutes that apply only in the commercial context. These laws should be expanded to cover non-financial online criminal activity.

- States should enact laws explicitly prohibiting interference with web sites (see e.g. Pa. Cons. Stat. sections 7611(a)(2) and 7612). Current computer crimes laws focus on interference with an actual computer, and may not cover unauthorized access to a website.

State	Unauthorized access prohibited	No additional minimum behavior requirements	Additional protection from online deceptive practices	Enhanced penalties for interference with governmental operations	Private cause of action	Separate spyware statute	No state law
AL	■	■		■			
AK	■					■	
AZ	■	■				■	
AR	■	■	1	■	■	■	
CA	■	■			■	■	
CO	■	■					
CT	■		2		■		
DE	■	■			■		
DC							■
FL	■	■		■	■		
GA	■		3		■	■	
HI	■	■					
ID	■	■					
IL	■	■			■		
IN	■	■				■	
IA	■	■			■	■	
KS	■	■					
KY	■	■					
LA	■	■				■	
ME	■	■					
MD	■	■					
MA	■	■					
MI	■	■					
MN	■	■					
MS	■		4				
MO	■	■			■		
MT	■						
NE	■	■					
NV	■	■		■	■		
NH	■	■				■	
NJ	■	■					
NM	■	■					
NY	■	■					
NC	■	■					
ND	■	■					
OH	■	■	5	■			
OK	■	■			■		
OR	■	■					
PA	■	■	6				
RI	■		7		■	■	
SC	■	■			■		
SD	■	■					
TN	■	■	8		■		
TX	■	■				■	
UT	■	■	9			■	
VT	■	■			■		
VA	■				■		
WA	■	■				■	
WV	■		10		■		
WI	■	■	11	■	■		
WY	■	■		■			

1: Prosecuting attorney may ask for Attorney General's assistance to investigate and/or prosecute this crime. Ark. Code Ann. § 5-41-107.
2: Attorney General may bring a civil enforcement action. Conn. Gen. Stat. § 53-453.
3: Use of a false name, logo, seal, or symbol to identify oneself in a computer transmission is prohibited. Ga. Code Ann. § 16-9-93.1. Attorney General and district attorney have power to investigate computer crimes. Ga. Code Ann. §§ 16-6-108 and 16-9-109.
4: Posting a message in electronic media with the intent to cause injury to another person is prohibited. Miss. Code Ann. § 97-45-17.
5: Falsifying electronic records or writing with intent to defraud is prohibited. Ohio Rev. Code § 2913.42. The computer crimes laws also contain enhanced penalties for falsifying government records or writings.
6: Unauthorized access to a World Wide Web site or telecommunication device is also prohibited.
7: Intentional transmission of false data for any purpose is prohibited. R.I. Gen. Laws § 11-52-7.
8: Unauthorized duplication or mimicking of a website is prohibited. Tenn. Code Ann. § 47-18-5203(c).
9: Individuals have an affirmative duty to report violations of the computer crimes laws. Utah Code Ann. § 76-7-705. Utah also directs the Attorney General, county and district attorneys to prosecute computer crimes laws. Utah Code Ann. § 76-7-704.
10: False documents transmitted via computer can be prosecuted under the forgery laws. W. Va. Code § 61-3C-15.
11: Penalties are enhanced for defendants who conceal that identity and location of their computer.

V. DISTRIBUTION VIA SPAM EMAIL OF FALSE INFORMATION ABOUT VOTING MECHANICS

A majority of states have enacted legislation aimed at curbing unsolicited bulk electronic mail ("e-mail"); however, most of these statutes are designed to protect consumers. Many of these statutes can be found in their respective state's consumer protection laws. These statutes generally prohibit the unsolicited distribution of e-mails that are "commercial" in nature and do not apply to non-commercial activities. Commercial e-mails are generally defined in these statutes as electronic messages with the purpose of promoting real property, goods or services for sale or lease. Accordingly, without some commercial component in the e-mails, it is unlikely that the distribution of spam e-mail used to spread false information about candidates or voting mechanics would violate these statutes.

A number of states have not enacted any legislation regarding unsolicited bulk or commercial electronic mail. These states include Alabama, Hawaii, Kentucky, Massachusetts, Mississippi, Montana, Nebraska, New Hampshire, New Jersey, New York, South Carolina and Vermont. However, many of these states rely on the Controlling the Assault of Non-Solicited Pornography and Marketing Act, or the CAN SPAM Act. The CAN-SPAM Act took effect on January 1, 2004 and requires unsolicited commercial e-mail messages to be labeled (though not by a standard method) and to include opt-out instructions and the sender's physical address. It prohibits the use of deceptive subject lines and false headers in such messages. The Federal Trade Commission is authorized (but not required) to establish a "do-not-email" registry. State laws that require labels on unsolicited commercial e-mail or prohibit such messages entirely are pre-empted, although provisions merely addressing falsity and deception would remain in place. However, the CAN SPAM Act appears to protect individuals from unsolicited commercial e-mails, and therefore is unlikely to apply to the distribution of spam email to spread false information about candidates or voting mechanics.

There are some states, however, whose anti-spam laws may reach non-commercial activity. For example, in Virginia, it is illegal to send unsolicited bulk e-mail containing falsified routing information, if the sender thereby violates a provider's policies, or distributes software designed to falsify routing information. Va. Code §18.2-152.3:1 (Transmission of unsolicited bulk electronic mail). The statute does not distinguish between commercial and non-commercial activity and was amended in April 2003 to increase the penalties for sending a high volume of messages containing falsified routing information.

Nevada is another state whose anti-spam laws are not limited to e-mails that are commercial in nature. In Nevada it is a misdemeanor to willfully falsify or forge any data information, image, program, signal or sound that is contained in the header, subject line or routing instructions of an item of electronic mail with the intent to transmit or cause to be transmitted the item of electronic mail to any Internet or network site or to the electronic mail address of one or more recipients without their knowledge of or consent to the transmission. Nev. Rev. Stat. Ann. §205.492. Furthermore, if a violation of this subsection causes an interruption or impairment of a public service, the person may be guilty of a category C Felony.

Lastly, many states prohibit the unauthorized use of a computer or a computer network to send unsolicited bulk email containing falsified routing information. The unlawful sale or distribution of software designed to facilitate falsification of electronic mail or routing information is also prohibited in many of these states. Persons or entities who distribute spam e-mail to spread false information about candidates or voting mechanics may violate these statutes but only if the sender a) accesses a computer or computer network without authorization, or b) distributes software that is designed to facilitate falsification of electronic mail or routing information. States that have enacted laws similar to these are Connecticut, Iowa, Illinois, Pennsylvania, Rhode Island and Texas.

The statutes referenced above are summarized in more detail in the corresponding chart entitled *"State Anti-Spam Statutes"*.

RECOMMENDATIONS

- Most states do not have adequate or any legislation that address the concerns implicated by deceptive practices and voter intimidation through electronic mail. The states and the Federal Government would benefit greatly by adopting legislation specifically targeted toward addressing these issues.
- New legislation must be tailored to so as to not be pre-empted by the CAN SPAM Act. This is easily accomplished since the CAN SPAM Act revolves around "commercial" activity.
- New legislation must be flexible enough to encompass the various mediums of sending electronic messages such as e-mail, text messages and other forms of digital transmissions over the internet and wireless networks.
- New legislation should also be broad enough to anticipate new forms of electronic distribution.

- The type of prohibited activity should include knowingly distributing false information regarding (1) the time, place, or manner of conducting state elections; (2) the qualifications for or restrictions on voter eligibility for any such election; and (3) false information regarding candidates.
- New legislation should be clearly delineated, preferably, in the state's already existing election laws. Currently, a few state's computer crime laws *may* be broad enough to prosecute those who use spam mail to spread false information about voting mechanics, however, any ambiguity about the application of the laws currently adopted by the states would be cleared up by specifically prohibiting the abuse of false or misleading spam-mail in the states already existing election laws.

State	State has Anti-Spam Legislation Specifically Enumerated in Election Laws	Sate Has Anti-Spam Legislation Enumerated in Computer /Criminal Laws	State Has Anti-Spam Legislation Enumerated in Consumer Protection Laws	State Has No Anti-Spam Laws	Anti-Spam Laws ONLY Prohibit Commercial Activity	Anti-Spam Laws Prohibit Non-Commercial Activity	Statute May Be Used To Prohibit False Information Re: Voting Mechanics*	Prohibits the misrep. of the point of origin or routing information	States that have relied on/ pre-empted by the CAN SPAM Act (Commercial Activity)	General Election Laws May Be Broad Enough To Prohibit Deceptive Spam Re Elections
AL				■						
AK			■		■			■		
AZ			■		■					
AR			■		■			■		
CA			■		■			■		
CO			■		■			■		
CT		■				*	*	■		
DE		■	■		■	*	*	■		
DC				■						
FL			■		■			■		
GA			■		■					
HI				■						
ID			■		■			■		
IL			■		■			■		
IN			■		■					
IA		■				***	***			
KS		■				*	*	■		
KY				■					■	
LA			■		■					
ME			■		■					
MD		■	■		■					
MA				■					■	
MI			■		■					
MN			■		■					
MS				■						
MO			■		■					
MT				■						
NE				■						
NV			■		■			■		
NH				■						
NJ				■						
NM				■						■
NY				■						
NC				■						■
ND		■		■		■	**			
OH			■		■					
OK				■					■	
OR				■						
PA		■				*	*	■		
RI			■		■					
SC				■						
SD			■		■					
TN		■	■			*	*	■		
TX			■		■					
UT				■						
VT				■						
VA		■				*	*	■		
WA			■		■					
WV			■		■					
WI		■								
WY			■		■					

*Requires unauthorized access to a computer network and falsified routing information.
**Statute criminalizes false and misleading emails, however, the false nature of the message must be used to induce the intended recipient to provide property or identifying information ("phishing").
***Requires the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail

Unauthorized access to a computer network is not required to prosecute under this particular statute.

Statute References

State	Abbreviation	Statute Reference(s)
Alabama	AL	N/A
Alaska	AK	Alaska Stat. § 45.50.479 (2008)
Arizona	AZ	Ariz. Rev. Stat. § 44-1372..01(A) (2008)
Arkansas	AR	A.R.S. § 44-1372.01 (2008)
California	CA	Cal Bus & Prof Code § 17529.2 (2008)
Colorado	CO	C.R.S. 6-2.5-103 (2007)
Connecticut	CT	Conn. Gen. Stat. § 53-451 (2008)
Delaware	DE	11 Del. C. § 937 (2008)
District of Columbia	DC	N/A
Florida	FL	Fla. Stat. § 668.602 (2008)
Georgia	GA	O.C.G.A. § 16-9-101 (2008)
Hawaii	HI	N/A
Idaho	ID	Idaho Code § 48-603E (2008)
Illinois	IL	815 ILCS 511/10 (2008)
Indiana	IN	Ind. Code. § 24-5-22-8 (2008)
Iowa	IA	Iowa Code § 716A.2 (2008)
Kansas	KS	K.S.A. § 50-6,107 (2006)
Kentucky	KY	N/A
Louisiana	LA	La. R.S. 51:1741.2 (2008)
Maine	ME	N/A
Maryland	MD	Md. CRIMINAL LAW Code Ann. § 3-805.1 (2008); Md. COMMERCIAL LAW Code Ann. § 14-3002 (2008)
Massachusetts	MA	N/A
Michigan	MI	MCLS § 445.2504 (2008)
Minnesota	MN	Minn. State. § 325F.694 (2008)
Mississippi	MS	N/A
Missouri	MO	§ 407.1135 to 407.1141 R.S.Mo. (2008)
Montana	MT	N/A
Nebraska	NE	N/A
Nevada	NV	Nev. Rev. Stat. An. §§ 41.705 to 41.735 (2007)
New Hampshire	NH	N/A
New Jersey	NJ	N/A
New Mexico	NM	N/A
New York	NY	N/A
North Carolina	NC	N.C. Gen. Stat. § 163-274 (2008)
North Dakota	ND	NDCC § 51-27-10
Ohio	OH	ORC Ann. 2307.64 (2008)
Oklahoma	OK	N/A
Oregon	OR	N/A
Pennsylvania	PA	18 Pa.C.S. § 7661 (2008)
Rhode Island	RI	R.I. Gen. Laws § 6-47-2 (2008)
South Carolina	SC	N/A
South Dakota	SD	SDCL §§ 37-24-41 to 37-24-48 (20008)
Tennessee	TN	Tenn. Code Ann. § 39-14-603 (2008);
Texas	TX	Tex. Bus. & Com. Code § 46.001 (20008)
Utah	UT	N/A
Vermont	VT	N/A
Virginia	VA	Va. Code Ann. § 18.2-152.3 (2008)
Washington	WA	Rev. Code Wash. (ARCW) §§ 19.190.005 to 19.90.110 (20008)
West Virginia	WV	W. Va. Code § 46A-6G-2 (2008)
Wisconsin	WI	Wis. Stat. § 947.0125 (2007)
Wyoming	WY	Wis. Stat. § 947.0125

FEDERAL LAW

There is no clear authority as to whether federal law presently contains criminal penalties against deceptive practices. For example, a classic "dirty trick" is to post fliers in targeted neighborhoods providing incorrect information about the date of an impending election. Even where a person posting such fliers knows that information to be false, and regardless of how many voters are deceived, the current federal law may not subject that person to criminal prosecution or civil injunction.

The most recent version of the Department of Justice's manual for criminal election prosecutions states that:

> 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. Examples 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 dates or qualifications for absentee voting, the date of an election, the hours for voting, or the correct voting precinct. Currently there is no federal criminal statute that expressly prohibits this sort of voter suppression activity.

United States Department of Justice, Criminal Division, Public Integrity Section, *Federal Prosecution of Election Offenses*, Seventh Edition (May 2007) at 61. The manual goes on to state that:

> The Criminal Division believes that the prosecution of voter suppression schemes represents an important law enforcement priority, that such schemes should be aggressively investigated, and that, until Congress enacts a statute specifically criminalizing this type of conduct, 18 U.S.C. § 241 is the appropriate prosecutive tool by which to charge provable offenses.

Federal Prosecution of Election Offenses at 63. Under 18 U.S.C. § 241, it is a felony to "conspire to injure, oppress, threaten, or intimidate any person in any state, territory or district in the free exercise or enjoyment of any right or privilege secured by the Constitution or law of the United States." The right to vote is a right that is protected under 18 U.S.C. § 241. However, while the Department of Justice has brought one prosecution for phone-jamming under this theory, it has not brought any such cases for deceptive practices. The key question would likely be whether a deceptive practice constitutes an injury to the right to vote. The requirement of a criminal conspiracy also limits the reach of this as-yet-untested theory.

In some cases deceptive information may be one aspect of a scheme to intimidate voters in violation of the Voting Rights Act. A prominent example of such a case involved the 1990 re-election campaign of then-Senator Jesse Helms of North Carolina. The Voting Section of the Civil Rights Division in the U.S. Department of Justice brought a case against the Helms campaign under Section 11(b), the principal civil anti-intimidation provision of the Voting Rights Act. The Justice Department charged that the Helms campaign had targeted heavily-black precincts with mailings that provided misleading information threatening criminal prosecution for voting. The case was settled by a consent decree prohibiting such targeted mailings. In the Helms case a deceptive practice was embedded within a larger scheme to intimidate targeted African-American voters. The deceptive practice itself did not constitute a separate claim.

The substantive purpose of digital voter suppression will be the same as its lower-technology counterpart: that is, to furnish misleading information concerning voter qualifications, possible adverse consequences of voting, dates of elections, locations and hours of polling places, and the like. However, the use of the Internet and networked technologies for these purposes raises the possibility of recourse to statutes and regulations, such as the CAN-SPAM Act and the Computer Fraud and Abuse Act, that may not be available when more traditional methods are used. As part of our research concerning statutes and regulations that furnish possible causes of action for digital voter suppression, we identified the following potential federal remedies (apart from violations of federal election laws and civil rights laws): (1) copyright violations; (2) trademark violations; (3) anti-cybersquatting law violations; (4) Computer Fraud and Abuse Act violations; (5) Wire Fraud claims; and the (6) the CAN-SPAM Act. We also considered the availability of Section 230(c)(1) of the Communications Act as a "shield" for liability of Internet service providers ("ISPs") and website operators for legal violations by persons using their facilities or services.

COPYRIGHT VIOLATIONS

A voter suppression campaign that sends emails or posts online information purporting to originate with a government agency or private organization might support a cause of action for copyright infringement.[18] Such an action ordinarily may be brought by any person or entity (whether organized for profit or otherwise) that owns or has license rights to the material that was misappropriated and may include requests for damages and/or injunctive relief, as appropriate.[19] More rarely, violations of copyright are punished under the criminal provisions of the United States Code.

Not all *governmental* organizations, however, may own copyrights and sue for infringement. The Copyright Act expressly disclaims copyright protection for "any work of the United States Government . . .,"[20] and also may prevent state and local governments from claiming protection for statutes or other "edicts of government" to which citizens are entitled to have unrestricted access.[21] However, state or local governments that publish materials other than "edicts of government," along with private organizations (whether or not organized for profit) may bring civil actions under the Copyright Act.

Where allegedly infringing materials are placed on the Internet, an important supplement to traditional copyright remedies is provided by section 512 of the Digital Millennium Copyright Act ("DMCA"), which permits rights holders to ask website hosts and other providers of online services promptly to take down, or disable access to, infringing materials posted to their services by customers or others.[22] Compliance with DMCA requests is not mandatory, but such compliance does give online service providers certain immunity from copyright infringement claims, and most reputable online companies has a policy of complying with DMCA requests. For this reason, and because the DMCA provides an expedited remedy that does not require the claimant to locate and serve the (often-elusive) provider of the misleading information, the DMCA process is a promising tool for stopping a voter suppression campaign that misappropriates copyright material.

Recommendations

Litigation Strategies

Except for the unlikely event of a criminal prosecution, copyright remedies must be sought by the holder of one of the exclusive rights (reproduction, public display, public distribution, etc.) recognized by the Copyright Act. Recommended relief might include a suit for injunctive relief and/or damages. Also, a take-down demand under the DMCA, directed to the website host or other online service provider that made the infringing material available is also an option. The summary DMCA procedure is quick and does not require the Committee or the rights holder to identify and serve a complaint upon the creator of the infringing content.

As noted earlier, copyright claims brought by federal agencies might be dismissed as prohibited by copyright law, but claims on behalf of state and local governmental agencies and private parties are not barred, at least where the materials for which protection is claimed are not statutes or other "edicts of government" published by or on behalf of governmental bodies.[23]

Legislative

The rights granted by the Copyright Act are generally adequate to the purpose of responding to misuse of materials owned by local elections boards, political parties, advocacy groups and other entities for voter suppression purposes. The only significant limitation that might be addressed by statutory amendment is the exception from copyright protection for certain governmental works. This exception, however, is based upon the strong policy concern that tax-payer funded works of authorship should be freely available to the public. Unless a statutory amendment is confined specifically to cases in which a work of government is exploited for fraud or other wrongful purposes, a proposed amendment to the Copyright Act to close this loophole will have little prospect of success.

FEDERAL TRADEMARK RIGHTS

Persons or organizations engaged in online voter deception might use the seals, insignia, names or other devices of governmental organizations, charitable organizations or political parties in order to confuse voters as to the origin of email messages or materials posted on spurious websites. Even where those misappropriations are not sufficiently extensive to support copyright infringement claims, they might give rise to causes of action under trademark law. Trademarks, service marks and trade names are names, symbols and other devices used by makers and vendors of goods to distinguish their products from those made and sold by others.[24] When a person has adopted and used a trademark in commerce, he or she may prevent others from using that trademark in ways that cause confusion as to

the origin of goods or that harm the property rights associated with the trademark. Remedies are available under the common law of unfair competition and under federal law under the Lanham Act.

Recommendations

Litigation

First, federal law precludes trademark registration of "the flag, or coat of arms, or other insignia" of federal, state, local or foreign governments.[25] Accordingly, a phony website that used such governmental insignia to mislead voters would not, on that basis alone, trigger a cause of action for trademark infringement.

However, federal, state and local governments may own and assert infringement of certification marks used to identify the source of government-supplied goods and services.[26] Accordingly, a governmental body might have a federal trademark infringement claim for misuse of a mark associated with a good or service supplied by that agency. Protection under federal trademark and common-law unfair competition law also is available for the names and marks of non-profit charitable groups, political groups and religious institutions.[27]

In some cases brought under federal trademark law, however, courts have denied protection to particular non-profit groups on the ground that those groups' activities did not use their marks "in commerce" or in connection with "goods or services."[28]

Also, even where the "commerce" requirement is satisfied, a claim for trademark infringement by a non-profit organization must satisfy the usual requirements for an infringement claim, including likelihood of confusion.

Legislative

The Lanham Act provides generally that:

> Any person who shall, without the consent of the registrant . . . use in commerce any reproduction, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive, . . . shall be liable in a civil action by the registrant for the remedies hereinafter provided.[29]

The requirement that a mark be used in commerce has caused some confusion as to the trademark rights of political, charitable and nonprofit organizations, especially where those groups do not engage in membership drives or fundraising activities.[30] An amendment to the Lanham Act, providing that use in commerce includes use of a mark to identify an organization engaged in any lawful, ongoing activity, would clarify the availability of trademark protection for nonprofits of all kinds.

ANTI-CYBERSQUATTING VIOLATIONS

An impostor that creates a deceptive website will want to ensure that online searches for the legitimate site will result in "hits" for the phony site. The most effective way to achieve this goal is to register a URL that is similar to that of the legitimate site, or that uses a name or mark similar to that of the organization the impostor seeks to impersonate.

Registration of an Internet domain name that is confusingly similar to a name or mark of an unrelated organization may be challenged in two ways: by a lawsuit brought under the Anticyberquatting Consumer Protection Act ("ACPA"),[31] or by recourse to the Uniform Domain Name Dispute Resolution Policy ("UDRP").[32]

Relief under the ACPA, which requires recourse to the courts, has largely been displaced in practice by the efficient arbitration procedures available under the UDRP. The UDRP is an arbitration-based dispute resolution policy adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"). All persons who apply to register a domain name, or ask a registrar to maintain or renew a domain name registration, are required to warrant that: (a) the statements made in the registration agreement are complete and accurate; (b) that to the registrant's knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) that the registrant is not registering the domain name for any unlawful purpose; and (d) that the registrant will not knowingly use the domain name in violation of any applicable laws or regulations.[33]

Domain name registrants also agree that in the event certain complaints are made concerning their use of a domain name, they will submit to a mandatory arbitration procedure. A finding that the complaint is meritorious may lead to cancellation or transfer of the registrant's domain name.

Recommendations

Litigation

First, there should be no reason for an aggrieved party to use the cumbersome procedure of the ACPA when the UDRP procedure is available. If an organization becomes aware of an apparent misuse of a domain name for voter suppression purposes, it should notify one of the domain name dispute resolution providers approved by ICANN, such as the National Arbitration Forum or the World Intellectual Property Organization.[34]

Second, in stating its complaint under the UDRP, the organization should emphasize any evidence that the bad-faith registrant intended to disrupt the complainant's operations generally or the orderly conduct of an election in particular. The UDRP is tailored primarily to reach misuse of trademarks by competitors for commercial purposes, but permits a general claim of "disrupting the business of a competitor" that at least one arbitrator has upheld as applied to a registrant's attempt to disrupt elections.[35]

Legislative

Both the ACPA and the UDRP are aimed primarily at domain name registrations that exploit trademarks to the detriment of commercial competitors. Both would benefit from amendments that recognize misuse of domain names to mislead and confuse for noncommercial purposes.

Changes to the UDRP procedure, which is nonstatutory and has taken the larger role in domain name enforcement would have an even greater practical effect. Specifically, it would be worthwhile for ICANN to add an additional ground of liability, such as registration "primarily for the purpose of disrupting the right of others to engage in lawful conduct."

COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act ("CFAA") prohibits the hacking into, or the use of worms, viruses and other malware to infiltrate government computers or websites.[36] The CFAA also makes it illegal to hack into private parties' computers, so long as the intrusion causes certain kinds of cognizable harm.[37]

Recommendations

Litigation

The principal limitation on private rights of action under the CFAA is the requirement for proof of more than $5,000 in damages for any one-year period. The Act limits damages for losses to economic loss only (and does not allow recovery for death, personal injury, mental distress, and the like); but "damages for loss of business and business goodwill" are recoverable as economic damages. *Creative Computing v. Getloaded.com, LLC.*[38] Moreover, "[w]hen an individual or firm's money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are 'economic damages.'"[39] Accordingly, it may be that a loss in reputation and business goodwill (perhaps indicated by reduced web traffic?) of a voter registration or information site provides legitimate grounds for a CFAA cause of action. The damages will, however, need to be quantifiable, which may be difficult to prove in the context of nonprofit voter information sites

Legislation

Elimination of the $5,000 damages threshold, or expansion of the categories of damages recognized to include noneconomic harms, would expand the usefulness of the CFAA to public interest groups.

THE WIRE FRAUD STATUTE

The federal crime of wire fraud is codified at 18 U.S.C. § 1343. Mail fraud and wire fraud both are proved by showing a scheme or artifice to defraud, combined with either mailing or electronic communication for purpose of executing the scheme.[40] In addition, the falsehood must be material.[41] Wire fraud has been found to apply to Internet communication.[42]

Recommendations

Litigation

There is no private right of action for violations of the wire fraud statute. Accordingly, any organization aggrieved by voter suppression actions that involve wire fraud would have to refer the matter to law enforcement.

Most frequently, mail and wire fraud apply to attempts to defraud a person of money or property. However, 18 U.S.C. § 1346 extends the category of applicable fraud objectives to the attempt to deprive a person of "honest services" besides property. However, since 1987, all courts but one (*DeFries*, below) have refused to apply wire fraud or this "honest services" argument to prosecutions of election fraud or deprivation of the "right to an honest election" under 18 U.S.C. §§ 1341 or 1343. *See United States v. Turner*, 459 F.3d 775 (2006) (stating that § 1346, adopted after a 1987 Supreme Court case invalidated the use of mail and wire fraud to prosecute election fraud, does not apply in the election fraud context). In fact, there is legislative history supporting the notion that Congress never intended the wire fraud statute to criminalize the deprivation of "inhabitants of a State, or political subdivision of a State, of a fair and impartially conducted election process," since that provision was proposed in the Anti-Corruption Act of 1988 around the time of the § 1346 addition, and was ultimately rejected. 134 Cong. Rec. S16315-01, 1988 WL 177972 (daily ed. Oct. 14, 1988) (statement of Sen. Biden).

There also appears to be no caselaw or legislative history expressly supporting the argument that the wire fraud statute may be used where the fraud deprives a person of the use of their computer equipment or services to receive email messages. Indeed, such limited deprivation may not rise to the appropriate level of materiality. If a problematic election influenced by fraudulent behavior results in additional costs, however, it might satisfy the requisite requirement of harm. *See United States v. DeFries*, 43 F.3d 707 (D.C. Cir. 1995) (holding that a scheme to cast fraudulent ballots in a labor union election tainted the entire election, and was a scheme to defraud the election authority charged with running the election of the costs involved).

SECTION 230 OF THE COMMUNICATIONS ACT

In many cases, the persons who actually create false websites and populate them with deceptive information may be difficult to locate. If the website hosting companies or other online service providers are suspected of complicity with the impostors or of negligence in permitting them to operate, aggrieved parties might usefully consider bringing actions those service providers.

Where such a claim is based upon intellectual property theories, there is no impediment to the claim if the elements of direct, vicarious or contributory infringement can be made out. If the claims are be based upon other grounds of liability, however, Section 230(c)(1) of the Communications Act,[43] which states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" must be taken into consideration. The courts have interpreted this language as providing a comprehensive, if not impregnable, barrier against an online service provider's liability for harmful material posted by others that does not involve violations of copyright or other intellectual property rights.

Recommendations

Litigation

Because of the section 230 exemptions, and because of the cost and delay of litigation generally, an aggrieved party's first approach to a website host or other service provider should be a request to disable or remove offending material voluntarily. Deceptive sites that facilitate voter suppression will be contrary to the terms of use of all or most reputable online service providers, and most businesses will be eager to disassociate themselves from such activity.

In the event that litigation aimed at a service provider appears necessary, the plaintiff should assess the degree of the provider's involvement with creating the offending content, and whether the third-party material involves any colorable intellectual property violations that will not be covered by the section 230 exception. However the complaint is framed, the plaintiff must be prepared to respond to a prompt motion to dismiss under section 230.

Legislative

Section 230, as expansively interpreted by the courts, is a deeply flawed statute that has been persuasively criticized as fostering irresponsible practices by website hosts and online publishers. Section 230 should be amended.

CAN-SPAM ACT OF 2003

Email messages that purport to be from governmental agencies, non-profit organizations that endorse candidates and other senders, but that in fact are sent by persons hoping to mislead voters, should be scrutinized for possible violations of the CAN-SPAM Act of 2003.[44]

Recommendations

Legislative

The CAN-SPAM Act has been widely criticized for its lack of effectiveness in dealing with abusive email marketing practices. Most of those criticisms fault the statute's failure to prohibit all commercial email that recipients have not specifically requested.

With respect to online deceptive practices, the statute's primary flaw is its limitation to messages that promote the sale of commercial products or services. The law should be amended to expand the definition of "commercial electronic mail message," or prohibit misleading practices engaged in by senders and initiators of noncommercial email.

CONCLUSION

In addition to the recommendations made throughout this report, there are steps that can be taken before the election to try to defray the potential damage of online deceptive practices.

First, law enforcement, especially attorneys general, district attorneys and the United States Department of Justice should make clear that these acts will be treated seriously and prosecuted to the full extent of the law. Press statements to this effect should be broadly disseminated before Election Day.

As related at the outset of this report, both Republicans and Democrats have been victimized by e-deceptive practices campaigns. For example, during the primaries a series of false campaign websites materialized that appeared to be legitimate, such as FredThomsonForum.com, RudyGiulianiForum.com, and MittRomneyforum.com. These sites featured posts with misinformation by people impersonating known pundits and promoted links that appeared to be candidate sites that actually routed users to YouTube videos attacking them.[45] The McCain-Romney.com website took viewers to the "official home of the Hundred Year War…and Bush's Third Term!"[46]

Yet, as the most frequent target of viral deceptive information in the context of the political campaign, Barack Obama's operation devised some methods for combating them that may provide voting rights advocates some lessons.

For example, the Obama campaign established a link on its campaign web site that addresses the rumors and fights fraud with fact. On this site www.fightthesmears.com, the Obama campaign provided concise, bulleted points of attack under each summarized smear headline followed by the truth which allows readers to quickly ascertain the facts. From here the reader could continue on and delve into each instance of lies or rumor for a more detailed description of the facts.

Secretaries of State and other election administrators can utilize such methods, as has already been done by the Maryland Board of Elections. At http://www.elections.state.md.us/, the Board has a section on the site called "Rumor Control." The page looks like the following:

RUMOR CONTROL
Get the Facts!

Foreclosure
Rumor: *If my home is in foreclosure, will I be allowed to vote?*
FACT: Maryland's Constitution (Art. I, § 1) guarantees each citizen who is 18 years old and a resident of the State the right to vote. The fact that your home is in foreclosure has no bearing on your right to vote. It may, however, effect where you vote. If you have left your home and taken up a new residence, you will need to update your voter registration (by October 14, 2008) and vote in the election district and precinct for your new residence.
Supporting Documentation:

- Letter from the Attorney General to Linda Lamone regarding reports of voter challenges of persons whose homes have been foreclosed 9-24-2008.

Campaign Merchandise
Rumor: *If I wear a campaign button or t-shirt into the polling place, will I be allowed to vote?*
FACT: A voter may wear campaign paraphernalia (buttons, t-shirts, or stickers) into the polling place while he or she is there to vote (the voter may not linger in the polling place after voting). However, an election judge, challenger and watcher, or other person stationed inside the polling place or within 100 feet of the polling place may not wear or display campaign materials.

Voter Registration Card
Rumor: If the name that appears on the voters registration card does not match exactly as it appears on your driver's license you will not be allowed to vote on November 4th. The authorities at the polls will turn you away, flat out.
FACT: This is not correct for several reasons:

- For voter registration purposes, the voter must use his or her legal name. However, there is no requirement that it be the full legal name. For example, you are not required to use your middle name on your voter registration application.
- Most voters in Maryland are not required to show any identification such as their voter registration card or their driver's license. (Some first time voters and voters who did not provide certain information on the voter registration application are are required to show identification).
- Voters are only required to provide their name when they check in to vote. A pollworker will confirm the voter's identity by having the voter provide his or her month and day of birth.
- No voter in Maryland is simply turned away. Instead, all voters are given the opportunity to vote a provisional ballot.

Rumor: I need my voter registration card to vote.
FACT: You do not need your voter notification card to vote. When you check in to vote, you'll be asked to provide your name, month and date of birth, and address.

College Students
Rumor: If a college student registers to vote at the student's college address the student's parents will not be able to claim the student as a dependent for tax purposes.
FACT: Registering to vote in Maryland alone will not jeopardize a parent's ability to claim a student as a dependent for tax purposes.

Absentee Ballots
Rumor: Election officials **automatically** send out absentee ballot applications to voters who previously voted by absentee ballot.
FACT: Election officials do not automatically send out absentee ballot applications to voters who have previously voted by absentee ballot. Voters can obtain an absentee ballot application on this website or by calling the voter's local election office.

Rumor: Election officials **automatically** send out absentee ballots to voters who previously voted by absentee ballot.
FACT: A voter has the option on the absentee ballot application to request an absentee ballot for a primary election, a general election, or both. A voter who indicated that he or she wanted an absentee ballot for both the 2008 Primary and General Elections will automatically receive an absentee ballot for the upcoming general election. A voter who

only requested an absentee ballot for the 2008 Primary Election will not automatically receive an absentee ballot. He or she will have to submit an absentee ballot application to his or her local election office to receive an absentee ballot for the 2008 General Election.

Registering before each Election

Rumor: Even though you are registered to vote, you still need to register again before the election.
FACT: If you have already registered to vote, you do not need to register again in order to vote in the upcoming General Election. You can check here to make sure you are registered to vote and that your information is up-to-date.

Provisional Voting

Rumor: I can go to any polling place in the State, vote a provisional ballot, and have my vote for President counted.
FACT: If you do not vote at the polling place where you reside, in most cases you will not be voting in your election district or ward and therefore your provisional ballot will not be counted. According to advice from the Office of the Attorney General, a voter must cast his ballot in the election district or ward in which the voter resides.

All chief elections officers should use their websites in this helpful fashion.

In addition to using the website, the Obama campaign utilized the viral nature of the web by encouraging supporters to send emails to their friends debunking the lies and rumors surrounding his candidacy so that the truth may become what is common knowledge. The campaign provided an email address to which anyone who came across an email with phony information could forward it to the campaign so that it could be addressed quickly and correctly.

Common Cause and Election Protection are undertaking a similar project, requesting that anyone who receives an email with false information or sees a spoofed website with misinformation forward that information on to by going to www.commoncause.org/DeceptivePractices or forwarding suspect email messages to DeceptivePractices2008@gmail.com.

There are also several existing websites dedicated to the debunking of misleading statements and rumors on and offline. Such sites include FactCheck.org, PolitiFact.com, and Snopes.com. Snopes has a section specifically dedicated to political myths http://www.snopes.com/politics/politics.asp. BreaktheChain.org is especially dedicated to setting straight email chain rumors spread through forwarded messages. A similar type site could be constructed regarding misleading information about the voting process.

Elections officers too, through whatever other online or offline megaphones they have at their disposal, provide detailed accurate information. They can use the media access available to them to inform people, ahead of time, of their rights and to advise them not to be taken in by any emails they may receive about the process.

They must also be in a position to quickly and loudly debunk false online rumors through the web and the mainstream media, as well as through the networks of voting rights and community organizations, and make sure that accurate information is disseminated through those same mechanisms. Moreover, bloggers and other online journalists can play a role by quickly spotting malicious campaigns and exposing them.

There may be some technology tools that we can use in the future to combat these challenges to our voting system. But for now, it is as it has always been: the best way to fight bad information will be by drowning it out with good information.

ENDNOTES

1 Robin Carnahan, "Voters First: An Examination of the 2006 Midterm Election in Missouri," Report from the Office of the Secretary State to the People of Missouri," Winter 2007, p. 17
2 "Deceptive Practices and Voter Intimidation," National Network for Election Reform, at http://www.nationalcampaignforfairelections.org/page/-/Deceptive%20Practices%20Network%20Issue%20Paper.pdf
3 Lawyers Committee for Civil Rights, "Incidents of Deceptive Practices and Voter Intimidation in the 2006 Elections," Excerpts from "Report on the 2006 Election Protection Legal Program to the Board of Directors and Trustees, Staff and Pro Bono Partners," at http://lccr.3cdn.net/d6af26cb31ff5ee166_vdm6bx6x5.pdf
4 Joy Ann Reid, "Bogus Emails Raise Anxiety About Voter ID Law," South Florida Times, October 3, 2008
5 See Oliver Friedrichs, "Cybercrime and the Electoral System," forthcoming, Symantec Press, p. 28
6 Bob Sulivan, "Kerry Donors Targeted by Fake E-Mail," MSNBC, August 2, 2004
7 Stirland, Sarah Lai. "Decoy Election Websites Pretend to Root for Your Candidate". *Wired* ,July 21 2008. <http://www.wired.com/politics/onlinerights/news/2007/11/ spoof_forums>.
8 Dan Morain, "Misleading Web Addresses Lead to Anti-Obama Site," Los Angeles Times, August 30, 2008
9 Oliver Friedrichs, "Cybercrime and the Electoral System," forthcoming, Symantec Press, p. 10
10 Id. at 11
11 Id. at 15
12 Oliver Friedrichs, "Cybercrimes and Politics," in Crimeware, Markus Jackobsson, Zulfikar Ramzan, eds., Symantec Press, 2008
13 Erik Larsen, "Clerk Warns of Internet Deception," Asbury Park Press, July 29, 2008
14 "FTC Cautions Consumers About Voter Registration Scams," Federal Trade Commission, News Release, August 7, 2008
15 The reference to "states" or "state laws" generally should be understood as including the District of Columbia.
16 Voting in 2008: Ten Swing States, The Century Foundation and Common Cause, September 2008
17 The District of Columbia does not have any form of computer crimes law.
18 17 U.S.C. § 106.
19 *See* Melville B. Nimmer and David Nimmer, *Copyright* §§ 14.01 *et seq.* (1996).
20 17 U.S.C. § 105.
21 *See* Library of Congress Copyright Office, Compendium II, Compendium of Copyright Office Practices § 206.03; *see also* L. Ray Patterson & Craig Joyce, "Monopolizing the Law: the Scope of Copyright Protection for Law Reports and Statutory Compilations," *36 UCLA Law Rev. 719* (1989).
22 Pub. L. No. 105-304, 112 Stat. 2877 (1998), codified at 17 U.S.C. § 512.
23 Copyright plaintiffs also must be prepared for defenses based upon fair use, including the claim that a voter suppression site was merely engaged in parody or comment.
24 15 U.S.C. § 1127.
25 15 U.S.C. § 1052(b).
26 *New York State Office of Parks and Recreation v. Atlas Souvenir & Gifts*, 207 U.S.P.Q. 954 (1980).
27 *Missouri Federation of Blind v. National Federation of Blind, Inc.,* 505 S.W.2d 1 (Mo. Ct. App. 1973); *see also* 1 *McCarthy on Trademarks and Unfair Competition* §§ 9:5-9:7 (West 2008).
28 15 U.S.C. § 1141(1). *See Tax Cap Committee to Save Our Everglades,* 933 F.Supp. 1077, 1091 (S.D. Fla. 1996).
29 *Id.* The anti-dilution and passing-off provisions of the Lanham Act also include a "commercial" requirement. The statute states that "[a]ny person who shall affix . . . a false designation of origin, or any false description, including words or other symbols tending falsely to describe or represent the same, and shall cause such goods or services to enter into commerce . . . shall be liable to a civil action by any person . . . who believes that he is or is likely to be damaged by the use of any such false description or designation." *Id.* § 1125(a).
30 *See* n. 14, *supra.*
31 15 U.S.C. § 1125(d).
32 *See* http://www.icann.org/udrp/udrp.htm.
33 *See* http://www.icann.org/udrp/udrp-policy-24oct99.htm.
34 Under the UDRP, a domain name registrar also many cancel or transfer a registration pursuant to agreement of the parties. In cases where the offending registrant is known and might be amenable to settlement, a demand for voluntary transfer or cancellation might be worth making before, or simultaneously with, notice to the domain name dispute resolution provider.
35 *Citizens Clean Elections Committee v. Schaffer,* 2003 CPRIDR LEXIS 6 (Mar. 24, 2003).
36 The CFAA is codified at 18 U.S.C. § 1030.
37 *Id.*
38 386 F.3d 930, 935 (9th Cir. 2004).
39 *Id.*
40 *VanDenBroeck v CommonPoint Mortg. Co.,* 210 F.3d 696 (6th Cir. 2000).
41 *Neder v United States*, 527 U.S. 1 (1999).
42 *See, e.g., United States v. Curry*, 461 F.3d 452 (4th Cir. 2006).
43 47 U.S.C. § 230(c)(1).
44 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003).
45 Stirland, Sarah Lai. "Decoy Election Websites Pretend to Root for Your Candidate". *Wired* ,July 21 2008. <http://www.wired.com/politics/onlinerights/news/2007/11/ spoof_forums>.
46 Dan Morain, "Misleading Web Addresses Lead to Anti-Obama Site," Los Angeles Times, August 30, 2008

PEOPLE.ACTION.DEMOCRACY.

COMMON CAUSE

1133 19th Street, NW, 9th Floor, NW, Washington, D.C. 20036
Tel 202.833.1200 / Fax 202.659.3716
www.commoncause.org