



**California Special
Districts Association**

Districts Stronger Together

March 24, 2015

Anya M. Binsacca
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004

RE: Request for Comment on Opinion No. 14-1203

Dear Ms. Binsacca,

I am writing on behalf of the California Special Districts Association (CSDA) in response to your solicitation for comments regarding Opinion No. 14-1203. CSDA is a non-profit association representing over 1,000 California independent special districts. Special districts serve a variety of communities and offer essential local services including fire protection, water delivery, sanitation, parks and recreation, airports, ports and harbors, libraries, and public cemeteries. CSDA provides legislative advocacy, education and member services for all special districts. CSDA has identified the issue to be addressed in Opinion No. 14-1203 as of particular importance to special districts.

Special districts are subject to the website agenda posting requirement of California Government Code § 54954.2. Many special districts hold board meetings less frequently than cities or counties, often monthly, bi-monthly, or even quarterly. Meeting postponements and the related need to hold special meetings hampers the public's ability participate. This makes ensuring the reliability and regularity of meetings to be of particular importance to special districts.

Policy Discussion

I. Websites Are Vulnerable to Service Interruptions and Malicious Attack

Technical website problems causing outages or website "downtime" are a common reality of the Internet, even for the most reliable Internet companies and cloud service providers. Google boasted that its email service, Gmail, experienced less than two hours of downtime in 2013.¹ Figures from 2014 show Microsoft's Azure cloud computing service experienced just under 40 hours of downtime for that year while Amazon's Web Services experienced 2.4 hours of downtime.² Many of the most reliable webhosting services available offer 99% uptime guarantees. However, even if these guarantees are met there would still potentially be a combined 3.6 days of website downtime per year. This translates to 100 minutes of

¹ *Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability*, GOOGLE OFFICIAL BLOG (March 20, 2014), <http://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html>

² Brandon Butler, *Which cloud providers had the best uptime last year?*, NETWORK WORLD (Jan. 12, 2015), <http://www.networkworld.com/article/2866950/cloud-computing/which-cloud-providers-had-the-best-uptime-last-year.html>



**California Special
Districts Association**

Districts Stronger Together

downtime per week, or 42 minutes of downtime within any single 72 hour period.³ It is unreasonable to ask districts to maintain constant website uptime.

In addition to normal service interruptions, websites are also often the targets of malicious attacks. One of the most popular forms is the Distributed Denial of Service (DDoS) attack in which a large volume of traffic, often directed by a master computer which controls an "army" of computers infected with malware (a "botnet"), is directed to a website causing it to fail. DDoS attacks are frequent and have brought down websites such as Mastercard, Visa, Paypal⁴, the Central Intelligence Agency⁵, the U.S. Department of Justice⁶, and the entire nation of China⁷. It is unreasonable to ask districts to prevent the types of attacks that have crippled or taken down even the largest and most sophisticated websites in the world. While DDoS attacks are the hardest to prevent, they are also among the easiest to execute. Botnets capable of taking down major websites can be rented for as little as \$100-200 per day.⁸

In contrast to the difficulty in preventing an agency's website from being taken down, physical postings are much easier to protect. For example, an agency could post an agenda in a locked glass case or in the lobby of a police station. An agency's only option in securing the agenda posted on its website is to contract for expensive cyber-security systems. As demonstrated with the examples of attacks on the websites of major corporations, even these measures will have limited impact in preventing DDoS attacks.

This threat of malicious attack against a public agency website isn't just hypothetical. The City of Hawthorne's website was down for nearly a week following a controversial police shooting. The city was forced to postpone its city council meeting due to a concern of violating the Brown Act.⁹ A police source confirmed that the website was down due to a DDoS attack,¹⁰ which many suggest was associated with the activist-hacker group Anonymous.¹¹

³ Additionally, webhosts which offer these guarantees often provide narrow definitions of "downtime" which exclude, for example, scheduled downtime for maintenance, meaning that actual downtime will often be greater than the above figures. A district which contracts with a less expensive, though less reliable provider is likely to experience even longer and more frequent periods of downtime.

⁴ Jaikumar Vijayan, *Update: Mastercard, Visa others hit by DDoS attacks over Wikileaks*, COMPUTERWORLD (Dec. 8, 2010), <http://www.computerworld.com/article/2514804/cybercrime-hacking/update--mastercard--visa-others-hit-by-ddos-attacks-over-wikileaks.html>

⁵ Jeff Hughes, *LulzSec DDoS attacks disrupt CIA and other U.S. agencies' sites*, DIGITAL TRENDS (June 15, 2011), <http://www.digitaltrends.com/computing/lulzsec-hacks-cia-and-disrupts-other-u-s-agencies/>.

⁶ Laurie Seagall, *Anonymous strikes back after feds shut down piracy hub Megaupload*, CNN MONEY (January 20, 2012), http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/.

⁷ *China hit by 'biggest ever' cyber-attack*, BBC NEWS (27 August 2013), <http://www.bbc.com/news/technology-23851041>

⁸ Tim G., *Renting a Zombie Farm: Botnets and the Hacker Economy*, SYMANTEC SECURITY INSIGHTS BLOG (08 Aug 2014), <http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy>

⁹ Heather Navarro, *Hawthorne cancels council meeting after website crashes*, NBC LOS ANGELES (Jul 11, 2013), <http://www.nbclosangeles.com/news/local/Hawthorne-Cancels-Council-Meeting-After-Anonymous-Hack--214795951.html>

¹⁰ Brian Charles, *Hawthorne police purportedly threatened by radical hacking group Anonymous over dog shooting*, LOS ANGELES DAILY NEWS (07/04/13, 12:01 AM PDT), <http://www.dailynews.com/general-news/20130704/hawthorne-police-purportedly-threatened-by-radical-hacking-group-anonymous-over-dog-shooting>

¹¹ *Anonymous hacker takes down police website after officer shot Rottweiler in head*, W3B SECURITY (July 10, 2013), <http://www.w3bsecurity.com/anonymous-hacker-takes-down-police-website-after-officer-shot-rottweiler-in-head-video/>



II. A Conclusion That a Website Must Be Maintained For the Entirety of the 72 Hour Posting Period Could Discourage District Use of Websites and Public Access to Information

A conclusion that the website must be maintained and live for the entire 72 hour period could discourage districts from creating or continuing to maintain websites. A requirement that districts must re-notice meetings due to temporary website downtime, caused by no fault of the district, would postpone district business. Many agenda items are time sensitive by law, policy, or the dynamics of transactions. The district's ability to carry out the public's business would be severely and adversely affected by postponements. Districts may determine temporary interruptions, which would require a meeting to be postponed, to be too burdensome to justify the creation or maintenance of a website. Districts may also fear that a technical violation of the Brown Act could be found after Board action has been taken, thus requiring a new meeting in order to "cure and correct" the violation or the expenditure of district resources to litigate whether the district was in "substantial compliance"¹² with the posting requirements.

Such a conclusion would also incentivize malicious website attacks. As discussed, the tools to take down websites are relatively accessible and low cost. If someone was opposed to a proposed project for financial reasons, for example, he or she could easily delay a vote by forcing the website down for only a few minutes during the 72 hour notice period. This person could repeat this process until the district abandons or removes its website.¹³

Websites are not just for agenda postings. Districts use their websites to accept bill payments and provide detailed account information, communicate with constituents about programs they offer and projects that are underway, provide notices to the community such as suggestions for conserving water or lowering utility bills, contact information for the district and its board members, and many other resources. A district would thus be faced with a choice between utilizing a cost effective method of communicating with and providing services to its constituents or avoiding the uncertainty, burden, and decreased public participation associated with re-scheduling meetings due to routine or maliciously caused website downtime.

The group Anonymous has petitioned the White House to recognize DDoS attacks as a form of legitimate protest - drawing an analogy between the trespass committed by those in the "Occupy" movement with the virtual trespass and occupation of websites by "hactivists" Dara Kerr, *Anonymous petitions U.S. to see DDoS attacks as legal protest*, C|NET (January 9, 2013 8:24 PM PST), <http://www.cnet.com/news/anonymous-petitions-u-s-to-see-ddos-attacks-as-legal-protest/> This illustrates the growing acceptance in some circles of DDoS attacks as a legitimate form of protest against government and private action.

¹² CAL. GOV'T. CODE. § 54960.1(d)(1)

¹³ As will be discussed in greater detail later, if "website" is defined such that the "website" exists, whether or not connected to the Internet, until an agency takes an affirmative action to remove it, then these repeated attacks could paralyze an agency. Repeated attacks could prevent the agency from holding the meeting necessary for the agency to decide to remove the website.



The purposes of the Brown Act are the promotion of openness in how public agencies conduct the people's business and to enable the people to remain informed "so that they may retain control over the instruments they have created."¹⁴ The Brown Act is to be liberally construed to achieve these purposes.¹⁵ An interpretation of the subject provision that requires the postponement of the people's business due to a website error occurring due to no fault of the agency would not promote the goals of the Brown Act. Neither would an interpretation of this provision which discourages agencies from utilizing one of the most cost effective and easily accessible communication tools in existence.

Legal Discussion

I. An Essential Definitional Element of "Website" Is "Connection to and Accessibility Via the Internet"

CSDA believes that a local agency would not violate the agenda posting requirements of Gov'T CODE § 54954.2 if a meeting were held despite the agency website experiencing technical difficulties which cause the website to be disconnected from the Internet. This is because one of the essential definitional elements of "website" is "connection to and accessibility via the Internet." If a collection of files becomes disconnected from the Internet then they fall out of the definition of "website." At such point the agency would no longer have a "website" and the additional "Internet Web site" posting requirements of Gov'T CODE § 54954.2 would not apply.

Website has been defined as:

a set of pages of information on the internet about a particular subject, published by a single person or organization¹⁶

a place on the World Wide Web that contains information about a person, organization, etc., and that usually consists of many Web pages joined by hyperlinks¹⁷

the term "website" means any collection of material placed in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol.¹⁸

¹⁴ CAL. GOV'T CODE § 54950

¹⁵ *San Diego Union v. City Council* (1983) 146 Cal.App.3d 947, 955. See also *Rudd v. California Casualty Gen. Ins. Co.* (1990) 219 Cal.App.3d 948 stating statutory language "must be construed in the context of the statutory framework as a whole, keeping in mind the policies and purposes of the statute."

¹⁶ *English definition of "website"*, CAMBRIDGE DICTIONARIES ONLINE,
<http://dictionary.cambridge.org/dictionary/british/website>

¹⁷ *Web site – Definition and more*, MERRIAM-WEBSTER, <http://www.merriam-webster.com/dictionary/web%20site>

¹⁸ 18 U.S.C. § 2258E(6)



When examining these definitions, it is clear that one of the essential elements of "website" is that it is connected to and accessible via the Internet. This element is essential as it is what differentiates a "website" from any other collection of files stored on a computer or server. Indeed, GOV'T CODE § 54954.2 applies to "Internet Web site[s]" which highlights the centrality of the Internet to the subject of that section.

A collection of files that is not connected to and accessible via the Internet is not a "website." As this applies to the questions presented for an opinion, if, due to a technical difficulty or malicious attack, a collection of files becomes disconnected from the Internet then that collection of files no longer fits the definition of a "website." At such point, an agency, by definition, no longer has an "Internet Web site" and the requirements of GOV'T CODE § 54954.2 at issue would not apply.

Consider an agency which is in the process of creating a website for the first time and is actively compiling files and information and storing it on a server but the site has not yet gone "live." The agency would not be required to post an agenda within this collection of files because the agency does not have a "website."

As another example, an agency has an active website but the agency's contract with its hosting service is set to expire on January 1. The agency has contracted with a new hosting service which will host the existing website files starting January 15. The agency has a scheduled meeting on January 7. Although the website files exist and are stored on a server, because they are not connected to and accessible over the Internet, the agency does not have a "website" during the period between January 1 and January 15.

Finally, consider an example where an agency has a website and posts an agenda on its website. During the 72 hour period, a catastrophic power outage occurs which prevents the servers from connecting to the Internet. The agency postpones the meeting due to a concern of violating the Brown Act. The agency re-notices the meeting through traditional methods but, because the power has not yet been restored and the servers remain inaccessible to the Internet, the agency does not (in fact, cannot) post the agenda on its "website." The agency would not violate the Brown Act by holding this subsequent meeting because the agency would not have a "website."

In this last hypothetical, the agency would not have violated the Brown Act by continuing with the first meeting for the same reason that it would not violate the Brown Act by holding the second meeting. In that hypothetical, the only difference between the first and second meeting was that the "website" was connected to the Internet for some period of time before becoming disconnected. Otherwise, the condition of the files on the server remained the same: isolated files on a computer which were not connected to or accessible via the Internet, and by definition did not constitute a "website."



IV. Alternative Definitions of “Website” Are Inaccurate

Any definition of "website" which does not include as an essential element that files be "connected to and accessible via the Internet" is fundamentally inaccurate. Without this element, any definition would be far too broad, encompassing potentially any file stored on a computer or electronic storage medium.

Additionally without this element there would no requirement that the website be publicly accessible, or even accessible to any other computer. GOV'T CODE § 54954.2 requires the agenda to be posted "in a location that is freely accessible to members of the public and on the local agency's Internet Web site, if the local agency has one." The phrase "freely accessible to members of the public" only qualifies the physical "location" of the posting. Without defining "Internet Web site" to include connection to and accessibility via the Internet, this latter posting requirement contains no provision requiring the "Internet Web site" be freely accessible to the public or even to be accessible via the Internet. Excluding "connection to and accessible via the Internet" from the definition of "Internet Web site" would hinder the purposes of the Brown Act and lead to an absurd result.¹⁹

Similarly, "intent" is an element incompatible with the definition of "website." Most obviously, "intent" alone is a poor determinant of whether something exists. Imagine a definition of "building" which includes as an element the "intent of the owner to have a building". Would the owner be able to deny the existence of the building by simply "intending" it not to be a building (perhaps by "intending" for it to be a chair)? If the building burnt down without the owner's knowledge, would the owner continue in having a building because his "intent" in having the building remained unchanged? Similarly, if an agency's legislative body resolves that it no longer intends to have a website, but fails to disconnect the website from the Internet, is the agency exempt from the requirements of GOV'T CODE § 54954.2 because it no longer has a "website" because there is no longer any "intent" to have the website?

Additionally, a definition of "website" which includes "intent" as an element would offer hackers or other attackers the ability to completely paralyze a public agency. If an agency's legislative body came to a decision to have a website it would also have to come to a decision to remove it. An attacker would need only to briefly interrupt service at some point during the 72 hour notice period to prevent a meeting and could do so during any subsequent 72 hour period noticing the rescheduled meeting. Because the agency would still have the "intent" of having a website it could not simply meet after posting a physical notice. Because the legislative body could not meet it also could not make a decision to remove the website and change its "intent."

¹⁹ "We must also avoid a construction that would produce absurd consequences, which we presume the Legislature did not intend" *People v. Mendoza*, 98 Cal.Rptr.2d 431, 441.



**California Special
Districts Association**

CSDA

Districts Stronger Together

Conclusion

Based on the foregoing, it is CSDA's conclusion that the additional website posting requirements of GOV'T CODE §54954.2 do not apply where a special district's website becomes disconnected from the Internet. An alternative conclusion would provide a serious disincentive for special districts to create or maintain websites and would reduce public access to district meetings by requiring meetings to be rescheduled following routine Internet service interruptions or malicious attacks.

On behalf of CSDA, thank you for the opportunity to comment on this important issue. Please do not hesitate to contact me to further discuss this issue or the comments provided in this letter.

Sincerely,

A handwritten signature in black ink, appearing to read "Nick Clair", is written over a dashed line.

Nick Clair

Legislative Analyst
California Special Districts Association
1112 I Street, Suite 200
Sacramento, CA 95814
877.924.2732
nickc@csda.net