ATPE Opposition to SB 904

Relating to the use of governmental communications systems to distribute political advertising

April 1, 2019

The **Association of Texas Professional Educators (ATPE)** appreciates this opportunity to offer written input in opposition to Senate Bill (SB) 904 by Sen. Bryan Hughes. ATPE believes that SB 904, while well-intentioned, is overly broad, ignores significant limitations of technology, and will result in unintended consequences.

I. Problems with expanding the scope of "electronic communications" for purposes of political advertising laws under SB 904

Current state law, which ATPE supports, prohibits employees or officers of school districts and other political subdivisions from spending public funds on political advertising. Criminal penalties already attach for those who violate this existing law, which constitutes a Class A misdemeanor offense. Fines may also be imposed by the Texas Ethics Commission. Sen. Hughes acknowledges in his bill analysis for SB 904 that current law already prohibits the behavior that his bill seeks to address, but states that government communication systems "are still used" for the purpose of political advertising.

In sections one and two of the bill, SB 904 seeks to add new language to Chapter 255 of the Texas Election Code specifying that the prohibited expenditure of public funds for political advertising as outlined above also includes using government communication systems. The bill further calls for adding an expanded definition of "electronic communications" in section three of SB 904 that would include "any communication facilitated by the use of any electronic device," such as a computer or computer network, as well as communications made "through an Internet website." ATPE believes that this expanded definition is overly broad and will lead to absurd results.

For example, it is well-established that a public employee may use his own personal time and resources to engage in electioneering activity, such as using a personal cell phone to view a campaign website or send a social media message that expresses support for a candidate. If such communications are made using the employee's personal cell phone and on his own personal time, such as during a lunch break, SB 904 would nevertheless criminalize that action if the communications were facilitated using a Wi-Fi network that is provided and paid for by the state or a political subdivision. State agencies, school districts, and other political subdivisions routinely provide computer networks that are often accessible at no charge not only employees but even members of the general public. Visitors to the Texas State Capitol, for instance, routinely use the public Wi-Fi network that is provided by the state and paid for using taxpayer dollars. There is nothing to prohibit such users from engaging in political advertising while using the state-sponsored Wi-Fi network. By making the definition of electronic communications so expansive as to include even computer networks, ATPE believes that SB 904 attempts to criminalize otherwise permissible conduct.

ATPE believes that current state statutes already provide ample guidance and enforcement mechanisms for the attorney general or local prosecutors, as well as the Texas Ethics Commission, to take action against those who violate the law against knowingly using public funds for political advertising. We oppose SB 904's proposed expansion of the law to criminalize certain private, personal communications that may happen to be facilitated by a government-hosted computer network and likely do not result in any actual expenditure of additional public funds.

SB 904 also fails to carve out any exceptions for the legitimate, education-related use of school district-owned computers or other resources to create lesson plans or enable students to view content, including on an Internet website, that may include political advertising. Even the Texas Attorney General's office, when issuing a September 2018 advisory to school districts, acknowledged that the viewing or distribution of campaign materials at school for educational purposes "may not be considered electioneering so long as all sides of an issue, or all candidates involved, are equally and fairly discussed, demonstrating no clear or implied favoritism or preference." ATPE believes that SB 904 is shortsighted in that it fails to recognize certain legitimate circumstances, including the educational example cited in the attorney general's advisory, in which government communication systems are used to access or share political content.

ATPE opposes SB 904 because its expansion of the scope of communications that might trigger a violation of the prohibition on using public resources for political advertising will ensnare certain innocent individuals who are simply exercising their rights to engage in political activities on their own time and at no cost to taxpayers and subject them to criminal penalties. When viewed in the context of other legislation that has been proposed this session to further expand the definition of political advertising, SB 904 is even more troubling. We believe SB 904 has great potential to be enforced selectively and in a manner that is politically motivated; that the bill would have a chilling effect on encouraging political awareness and engagement of our citizenry; and that SB 904 likely infringes on multiple constitutional protections.

II. Problems with third-party liability for "misuse of government resources" under SB 904

With section three of his SB 904, Sen. Hughes also seeks to expand Chapter 255 of the Texas Election Code to prohibit third parties from delivering political advertising messages to an email address issued by the state or a political subdivision, such as a school district. SB 904 would impose a civil penalty against "a person, political campaign, or advocacy group" that violates the prohibition outlined above by sending such email. Again, ATPE believes that SB 904 may be well-intentioned but would produce unintended consequences and unfairly penalize innocent actors.

To illustrate the undesirable effects of SB 904, consider the fact that nearly every member of the legislature maintains a political campaign website in which users can sign up for email updates from the campaign. For example, at the political website BryanHughes.com, operated by or for the benefit of the author of SB 904, one need only type in a name and an email address in order to receive email updates from the campaign. The same is true of many third-party websites operated by advocacy groups or other individuals who may send out email communications of a political nature. Under SB 904, those candidates or advocacy groups would be liable and face harsh penalties if they send such communications to a government email address. The difficulty with SB 904 is that it would be practically impossible for each candidate, individual, or advocacy groups to prevent a government employee from signing up to receive such communications. Under SB 904, if a government employee

uses a state-issued email address to contact a political campaign or candidate and receives an auto-reply message back, it is likely that the political campaign or candidate will be in violation of the law and subject to being fined despite arguably having no actual intent to send a political advertising message to the government employee. Moreover, there is absolutely nothing to prevent a person or group from *falsely* using the name or email address of a government employee to sign up for such updates. ATPE believes it is unreasonable to subject an innocent third party to civil fines and penalties simply for sending email communications at the request of another person, especially if the person who joins the email list does so under false pretenses or with a malicious intent of creating liability under SB 904 for the third party who sends the email.

Texas employs well over a million individuals in state and local government jobs, many of whom have official email addresses assigned to them. SB 904 would impose stiff penalties against any third party that sends a political email message to such an individual or to a state agency. ATPE points out that it would be overly burdensome to expect third party individuals, candidates, or advocacy groups to know whether they are sending communications to a government email address. This is especially true since there is little to no commonality among the domain name formats used for email addresses of state agencies and political subdivisions.

In some cases, it can be impossible to distinguish a government-subsidized email address from one that is paid for by a private individual or group. Among state agencies currently found in Texas that have email addresses for official use, many addresses include the extension ".texas.gov," but there are others that use ".state.tx.us" or ".edu' in the extension of their official email addresses. For school district email addresses, the domain names used from place to place vary even more greatly. Like private email addresses, they may end in ".com," ".org," ".net," or ".us." They may include the name of the school district spelled out in full, or they may use an abbreviation such as "tisd" in the domain name. Given the similarity of so many government email addresses to those used by private entities, confusion abounds. For example, the domain name "tisd.net" belongs to a for-profit company that is an Internet service provider, but the domain name "tisd.org" serves the Temple Independent School District. SB 904 would make it unlawful for a third party to send political email to someone at "tisd.org" but not to someone at "tisd.net."

Furthermore, this section of SB 904 is problematic due to the very nature of electronic communications and the frequency with which email communications are misused. Email spoofing, for instance, has become an omnipresent problem in which an email header is forged so that the message will appear to have been sent by a source that is different from its actual source. Network protocols that provide rules to allow computers to communicate with one another over the Internet, such as through sending and receiving email messages, rarely allow for the actual senders of such messages to be authenticated, and cybercriminals who engage in email spoofing have managed to stay ahead of even the most updated anti-spoofing protections on the market. Through viruses and malware, these cybercriminals will use not only the email address of the innocent person whose account has been compromised or infected, but often will take other emails found in the user's address book and forge those unsuspecting users' email addresses, too, for sending out spoofed and fraudulent email messages. Accordingly, it is extremely difficult in today's environment to prevent one's email address from being hijacked and used without one's knowledge or consent.

Also, once a user's email address has been spoofed, it is seldom used only one time and tends to show up repeatedly in fraudulent email messages. (As one example, the author of this written testimony has repeatedly received spoofed email messages purporting to have been sent by a Texas public school superintendent which are actually originating from a fraudulent source; the messages

have continued to arrive over and over through no fault of the actual superintendent whose name is being used.) This means that even if the alleged "sender" of the email receives only a warning for a first violation, which Sen. Hughes has suggested he might add to SB 904 as a form of safe harbor, it is likely that the spoofed emails will continue to be sent out in the name of the same sender. Therefore, due to the prevalence of email spoofing, ATPE believes it is unrealistic to expect the attorney general and other prosecutors to investigate and impose fines against any third party that appears to have sent a political message (or multiple messages) to a government email address.

ATPE believes it is not feasible, considering the realities of how Internet technology is used and misused in today's world, to impose the sort of "zero tolerance" rule that SB 904 contemplates for third party individuals and groups. Even using the most sophisticated filtering and anti-virus systems that many individuals, candidates, and advocacy groups cannot afford, it would be nearly impossible for any third party to guard against unintentionally sending political email to government-issued email addresses. We also believe it would be a waste of law enforcement resources to try to investigate and enforce such an unrealistic measure as proposed by SB 904.

III. Conclusion

ATPE appreciates the interest of Sen. Hughes in ensuring that state law restrictions on using taxpayer funds for political purposes are respected and enforced. However, we feel that SB 904 takes the wrong approach by criminalizing otherwise permissible activities that may be "facilitated by" government communication resources in an incidental manner. ATPE also believes that the bill's attempt to regulate email communications generated by third parties is unreasonable and will be extremely burdensome, both for prosecutors who would have to investigate alleged violations and for the third parties who would be subject to the law.

For these reasons, ATPE respectfully urges senators to vote **NO** on SB 904. For additional information, contact ATPE Governmental Relations at (800) 777-2873 or government@atpe.org.

The Association of Texas Professional Educators (ATPE) has been a strong voice for Texas educators since 1980. It is the leading educators' association in Texas with 100,000 members statewide. With its strong collaborative philosophy, ATPE speaks for classroom teachers, administrators, future, retired and para-educators and works to create better opportunities for 5 million public schoolchildren. ATPE is the ally and the voice of Texas public school educators.