CLEAT
STRENGTH JUSTICE UNITY

NEWS RELEASE

Proudly Serving Texas' Finest

400 W. 14th Street, Suite 100 • Austin, Texas 78701 • (512) 495-9111 • Texas WATS (800) 252-8153

For Immediate Release

REVISED and EXTENDED: 09/10/19

Why Recent Changes To The Texas Public Information Act Should Have All Officers Refusing To Use Their Own Personal Electronic Devices For Work

By: Bob Leonard
CLEAT General Counsel

Recently we have received several inquiries from officers regarding the newly passed SB 944. What is SB 944? SB 944 added several amendments to the Texas Public Information Act (commonly referred to as an Open Records Act). Specifically, the bill amends Section 552.004 of the Texas Government Code by adding subsection (b) that requires a current or former officer or employee of a governmental body who maintains public information on a privately owned device to forward or transfer the public information to the governmental body or a governmental body server to be preserved as required by the Act or to preserve the public information in its original form in a backup or archive and on the privately owned device for the time described in the law.

It should be noted that this was the state of the law before the passage of SB 944 based on previous case law and Attorney General Opinions. Prior to the passage of SB 944, the law did not distinguish between personal or employer-issued devices, but rather focuses on the nature of the communication or document. SB 944 simply clarifies that work related information kept on a privately owned device is public information subject to the Act. It has been CLEAT's longstanding recommendation that officers not use personal electronic devices for work.

One change made by SB 944 has a direct impact on all officers; the law now specifically imposes a duty on the owner of the privately owned device regarding the retention of public information.

In a nutshell SB 944 requires the owner of a privately owned device that contains public information to preserve the information in its original form, both in a backup or archive **AND** preserve the information on the privately owned device unless the information is transferred to the governmental employer or uploaded to a governmental server.

Officers who use personal electronic devices such as cell phones, tablets, or personal computers are subject to the law if those devices are used to store work related information. It covers communications such as texts, tweets, emails, notes and pictures. If the device contains information that is subject to public disclosure under the Public Information Act then the employee or employer must preserve it and make it available for disclosure. It is the information on the device not the type of device or who owns it that controls whether it is subject to the Public Information Act.

What is even more troubling is the new law requires the officer to maintain the information on the device for a defined period unless the information is transferred to the governmental entity for preservation. Failure to preserve the information could result in possible criminal charges. This means if a device is damaged or lost and the information was not backed up, then the officer could be held liable.

Using our personal electronic devices or home computers to assist us in our work has become "the norm." However, given the implications SB 944 presents, it is foolish for officers to continue to utilize their personal electronic devices for official work purposes. Recent case law developing around the country has resulted in more and more criminal defense attorneys who are looking to subpoena officers' phones due to possible evidence on the device. You can see why using your own personal electronic devices for work is a bad idea. If officers require a cell phone or tablet to perform their job, they should request the department issue them one.

Since SB 944 became law, we have had a number of questions that we have been asked regarding specific scenarios. Below is our responses and recommendations regarding those questions.

"Can a department order me to use my personal cell phone for work?"

The answer is generally no. A department can require its officers to maintain a good contact phone number. This could be a home phone or even a simple cell phone without smart phone capability (no e-mail, texting or internet). The only exception would be that you were required as a condition of employment at the time you were hired to purchase a cell phone for use at work. We would have to evaluate the specifics of each case individually to make an absolute determination.
We have been told that some departments provide a cell phone stipend to officers for them to use their personal phone at work. Are you required to accept the stipend? If not, then our recommendation would be to refuse the money and not use your personal device.

If you are ordered to maintain a cell phone for work, we would need to know if there is also a requirement for e-mail or texting capability to be included. If not, our recommendation would be that you purchase a phone without those capabilities for use at work. Even then our concern would be that you are exposed to liability in the event you fail to transfer the information to your employer or do not properly retain the information and then keep it on the secondary phone.
If you are not ordered to purchase or maintain a personal cell phone, our recommendation is that you give notice to your department in writing that you are not using your personal electronic devices (phones, computers, or tablets) for work. Governmental e-mail accounts should be deleted from these devices and you should not text work related information from them. Do not store any work related material on your phone or device, including pictures, notes, reports, or any other document that is subject to the Public Information Act.

IF YOU ARE GIVEN AN ORDER TO USE YOUR PERSONAL ELECTRONIC DEVICE FOR OFFICIAL WORK PURPOSES, FOLLOW THE ORDER AND CALL CLEAT LEGAL IMMEDIATELY.

"Can my department order me to install a software application on my personal phone to back up work related information?"

Would you allow your department to "tap" your phone? Absolutely not. And our recommendation is that you do not install any department software on your phone that also contains personal information, such as banking information or records, personal or family pictures, personal e-mail, or anything else you would want to keep private.
If you are ordered to maintain a phone and install an application for retention of data, we would recommend that you contact us for additional advice. At the very least, you should only install the application on a secondary phone that does not mix work related information with personal information.

"What is my liability or responsibility if I buy a burner phone or secondary phone to use at work?"The law still holds you liable for the retention of any work related material subject to the Public Information Act that is stored on your personally owned device until that material is transferred to the employer or backed up or archived on a governmental server. If you lose the phone, or the data is lost before being transferred or backed up, you are personally liable, not the governmental agency. Once the data is transferred or backed up on a governmental server, the governmental agency is responsible for retention of the information.

As always, CLEAT stands ready to assist our members should you have any questions or run into any problems regarding this new law. We have your six!