# Kansas State Lodge
## Fraternal Order of Police

Testimony to the
House Committee on Judiciary
House Bill 2191
Detective Dean Brown
Fraternal Order of Police, Kansas State Lodge
February 12, 2019

Mr. Chairman and members of the Committee, thank you for allowing my testimony in support of House Bill 2191. My name is Dean Brown and I am a detective with the Lawrence, Kansas Police Department.

I have been conducting forensic examinations of digital evidence since 2000. During that time, we have largely developed procedure through application of existing statutes which worked well in most cases. In certain situations, this has not worked though. Sometimes the existing statute specifically does not allow us to do what we need to do. This was the case with the search warrant statute, 22-2502, prior to 2012. Prior to the change requested by myself and other people operating in the discipline of digital investigations, securing search warrants from service providers who were headquartered outside of the State of Kansas was not allowed under the existing language. In 2012, the Legislature, after review by this committee, agreed the existing statute had deficiencies when applied to digital investigations and changed the law.

We again, have run across a deficiency and are asking that it be corrected. While the current statute does not specifically deny certain actions, the statute is ambiguous and has been interpreted by some to not allow us to conduct examinations of digital evidence in an efficient manner, and in certain situations, not to complete them at all. House Bill 2191 is focused to address those ambiguities and not to increase the authority of the government to infringe on the rights of its citizens.

House Bill 2191 specifically addresses timing and location of digital examinations. Currently the search warrant statute, with certain exceptions, does not allow searches conducted outside of the 96 hour time limit and does not allow the search to occur outside of the jurisdiction of the authorizing magistrate or district judge who issued the warrant. While a large majority of the state interprets this to mean that as long as items containing digital evidence are under the government's control within 96 hours of the issuance of a search warrant and seized within the jurisdiction of the issuing judge, any subsequent examination of the digital evidence stored within the device can occur outside of the 96 hour limit and occur outside of the jurisdiction of the signing judge.

The rationale for this is that once items containing digital evidence are seized, their contents are generally "frozen" or do not change. This means any evidence which is eventually recovered from the item would have existed when the item was seized. Since the item was seized within 96 hours, this insures all evidence existed in the 96 hour window. Since the purpose of the 96 hour rule is to insure "freshness" of the probable cause,

seizure of the device insures whatever probable cause was provided to the issuing judge would have been fresh for any evidence later discovered. This also insures that any evidence which could later be discovered also existed within the jurisdiction of the authorizing judge when the warrant was signed if the item is seized or is in the jurisdiction of the judge authorizing the warrant when the warrant was signed. All of this, we believe, is consistent with the intent of the law.

The issue is, that the letter of the law does not necessarily reflect that intent. Because of this, there are differing opinions among attorneys arguing these seizures in court, and often law enforcement is directed to operate under the strictest and least favorable interpretation of the law to insure evidence is not later suppressed. The specific consequences of this are that law enforcement must extract information from a device containing digital evidence within 96 hours of issuance of the search warrant and that extraction must occur within the jurisdiction of the judge who signed the warrant. This is not only onerous but in certain situations simply not possible. Examples include current generation locked phones which can take years to unlock and may require the devices being sent to specialized labs outside of Kansas to have the unlocks accomplished.

In general, digital examination equipment and expertise are centralized due to their costs in time to acquire expertise and funds required to purchase equipment. Because of this, evidence often has to be moved, sometime across jurisdictional boundaries for examinations to occur. This also creates a backlog since the number of persons seizing digital evidence exceeds the number of persons examining evidence. While we would argue this does not contradict either the intent of, or the letter of the search warrant statute, it has been argued it does contradict the letter of the search warrant statute. Note this is equivocal since when a search warrant is executed is not defined within the statute.

Current strategies for dealing with the location of where the search occurs in certain counties also require the obtaining of another warrant in the jurisdiction where the examination occurs. In the case of the Heart of America Regional Computer Forensic Laboratory (HARCFL), this means a Clay County, Missouri warrant is obtained. This is duplicitous, and I have never heard of a warrant authorized in Kansas being denied in Clay County, Missouri, but also opens a quagmire of legal issues. Missouri laws are not completely interchangeable with Kansas laws. This also insures that any examination in which a Missouri warrant was obtained, could be legally attacked in two jurisdictions, with a reasonable foreseeable result of a contradictory Missouri and Kansas decision based on the same facts of a case out of Kansas. This goes against state sovereignty where Kansas judges appointed or elected by Kansans determine Kansas cases based on Kansas law.

Analogs for the majority interpretation of the statute also exist in physical evidence. For example, search warrants for DNA evidence do not require that the DNA be examined within the jurisdiction of the authorizing judge, or that the profile of the DNA be extracted within 96 hours so that the comparison to known samples can occur at a later date. The current practice of DNA allows that the substance containing the DNA be seized or be in the possession of the

government within 96 hours of the search warrant being signed and for it to be sent for analysis to labs which may not be within the jurisdiction of the judge who signed the warrant. Seizure of a large number documents likewise does not require the documents be copied by the government within 96 hours and within the jurisdiction of the judge signing the search warrant, just that the documents be in the possession of the government within 96 hours of the search warrant issuing and that they be in the jurisdiction of the signing judge when the warrant is signed.

Kansas is not alone in its need to clarify the search warrant statute. In 2009, the federal government amended Rule 41 of the Federal Rules of Criminal Procedure (Title VIII – Rule 41), to include:

> *(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.*

The state of Texas also amended its search warrant statute, Article 18.07, in 2011 adding the following:

> *(c) If a warrant is issued to search for and seize data or information contained in or on a computer, disk drive, flash drive, cellular telephone, or other electronic, communication, or data storage device, the warrant is considered to have been executed within the time allowed under Subsection (a) if the device was seized before the expiration of the time allowed. Notwithstanding any other law, any data or information contained in or on a device seized may be recovered and analyzed after the expiration of the time allowed under Subsection (a).*

Note this is not an exhaustive list.

In closing, I ask for your support of this measure and that you favorably recommend passage of the bill to the full Senate.

Thank you for allowing testimony today on this very important matter. I am happy to answer any questions.