

specifically authorized. However, lawful exceptions are outlined, allowing such activities for communication service providers, government entities, and law enforcement agencies under certain circumstances, such as in the normal course of business or lawful activities. Additionally, sales for disposal of obsolete or surplus devices are permitted under specified conditions.

Section 4 introduces a new section to KRS Chapter 526, enabling the Attorney General, Commonwealth's attorneys, or county attorneys to seek judicial authorization for wire, oral, or electronic communication interception by investigative or law enforcement officers. This authorization may be granted when interception could provide evidence or has provided evidence of organized crime engagement or criminal gang activity or recruitment. If the interception falls within the lawful parameters outlined in subsection (2) of Section 2 of the Act, no application or order is necessary.

Section 5 establishes protocols for the disclosure and use of information obtained through authorized interception of wire, oral, or electronic communications by investigative or law enforcement officers. It permits officers who have obtained knowledge of such communications or evidence derived from them to disclose or use that information to other authorized officers as necessary for official duties. Additionally, it allows for the disclosure and use of intercepted communication contents or derivative evidence in legal proceedings, provided the disclosure is made under oath or affirmation. It also maintains the privileged character of intercepted communications and allows for the use of intercepted information in cases beyond the specified offenses if approved by a judge after demonstrating compliance with interception regulations.

Section 6 establishes detailed procedures for the application, authorization, and oversight of wire, oral, or electronic communication interceptions by investigative or law enforcement officers. Applications for interception orders must be made in writing, under oath or affirmation, to a judge of competent jurisdiction, providing comprehensive details such as the identity of the applicant, the factual basis justifying the need for interception, and the nature of the communications to be intercepted. The judge may require additional evidence to support the application. If the judge determines probable cause and compliance with interception regulations, an ex parte order may be issued authorizing the interception within specified territorial jurisdictions. The order must specify various details, including the identity of targeted individuals, the nature and location of communications facilities, and the period of authorization. Extensions of interception orders may be granted if justified.

It mandates the recording of intercepted communications, if possible, and strict protocols for the handling, sealing, and retention of recordings and related documents. Judges are required to issue inventories of intercepted communications after the termination of interception orders. The contents of intercepted communications cannot be disclosed in legal proceedings unless all parties have been furnished with relevant court orders and applications.

Furthermore, individuals may move to suppress intercepted communications or evidence derived from them if they believe the interception was unlawful or not conducted in compliance with the law. It also grants the Commonwealth the right to appeal the denial of interception orders.

Section 7 mandates reporting requirements regarding the authorization and implementation of interceptions of wire, oral, or electronic communications. Within thirty days of the expiration or denial of an interception order, the issuing judge must report various details to the Administrative Office of the Courts, including the nature of the order, duration of interceptions, and identifying information about the applying investigative or law enforcement officer and agency. Additionally, in January of each year, the Attorney General, Commonwealth's attorneys, and county attorneys must report detailed information about interceptions made during the preceding year to the Administrative Office of the Courts. This includes data on the nature and frequency of intercepted communications, arrests resulting from interceptions, trials, motions to suppress, convictions, and resource usage. The Administrative Office of the Courts must then compile and transmit a comprehensive report to the General Assembly by March 1 of each year, summarizing the data provided.

Section 8 establishes civil remedies for individuals whose wire, oral, or electronic communications are intercepted, disclosed, or used in violation of the legislation. Such individuals have a civil cause of action against any person involved in the interception, disclosure, or use of the communication. They are entitled to recover actual damages, punitive damages, and reasonable attorney's fees and litigation costs. However, a good-faith reliance on a court order or legislative authorization serves as a complete defense to any civil or criminal action brought under this chapter or any other law.

Section 9 requires law enforcement agencies in Kentucky to register with the Kentucky State Police all devices primarily useful for surreptitious interception of wire, oral, or electronic communications that are owned by them or under their control. Registration must occur within ten days of the effective date of the legislation for existing devices and within ten days of acquiring new devices. The registration information must include agency details and a detailed description of each registered device. The Kentucky State Police will issue a serial number for each registered device, which must be affixed or indicated on the device.

The fiscal impact of HB 725 is indeterminable, though likely negative. The implementation of the bill would have notable fiscal implications for local entities, primarily impacting law enforcement agencies and courts. Initially, local governments would face expenses related to adapting to the new regulations. This includes costs associated with training personnel on the updated procedures and requirements outlined in the legislation. Additionally, ensuring compliance with HB 725 could necessitate investments in administrative resources, such as hiring staff or reallocating existing personnel to handle tasks like reporting and record-keeping. Beyond the initial implementation phase, ongoing operational costs would persist. Local entities would need to allocate resources for activities such as compiling and submitting reports to regulatory

authorities, maintaining accurate records of interception devices, and ensuring legal compliance through training and monitoring efforts.

Sections 2 and 3 changes the conditions of a Class D felony and creates a new Class D felony. When a court denies bail to a Class D felony defendant, the local government is responsible for incarcerating the defendant until disposition of the case in one of Kentucky's 74 full service jails or three life safety jails. While the expense of housing inmates varies by jail, each additional inmate increases facility costs by an average cost to incarcerate of \$44.97, which includes the \$35.34 per diem and medical expenses that the Department of Corrections pays jails to house felony offenders. Upon sentencing, a Class D felon is housed in one of Kentucky's full service jails for the duration of his or her sentence. The Department of Corrections pays a jail \$35.34 per day to house a Class D felon. The per diem may be less than, equal to, or greater than the actual housing cost.

Data Source(s): LRC Staff; Kentucky Department of Corrections

Preparer: Ryan Brown (LG) **Reviewer:** KHC **Date:** 2/28/24