

## Testimony on HB 2084 – Tracking Pre-Paid Communication Device Purchases

Mr. Chairman, Members of the Committee:

**Background:** HB 2084 represents three years of work by law enforcement officers and agencies to address a problem most of us do not see or want to see – the use of pre-paid “throw away” or “burner” phones by persons engaged in human trafficking, drug manufacture and sales, and other illegal activities.

If I have a calling plan through a provider like Sprint, AT&T, Verizon, T-Mobile, and others, and law enforcement officers legally obtain my telephone number, they can contact my service provider and learn my identity, address, and calling information. In other words, they can find me because I have a business relationship with the service provider. The provider sends me a monthly bill at a specific address and I pay it. If they have legal access to my telephone records, they can identify persons with whom I may have been consorting in illegal activities – if those phones also are part of a service provider’s plan.

However, if I purchase a “burner” phone, all I do is register with a service provider to activate the telephone. I can use a false name and address without repercussions because there will be no monthly bill sent out. The service provider has no way of knowing whether Tom Sloan actually purchased and registered the device.

If law enforcement officers legally obtain my “burner” phone’s telephone number, they still cannot identify me because there is no record of who I “really am” and where I live. Similarly, if they have my phone and try to identify the persons to whom I have made calls, if the calls were made to other “burner” phones there is no way to identify the recipient.

Law enforcement officers will provide testimony about why the ability to identify who owns and uses “burner” phones to commit crimes is important. From my perspective, within Constitutional boundaries, I want to help law enforcement officers to protect my family and me and if a crime is committed against my family, to arrest the perpetrator.

**Components of Bill:** Efforts have been made to address the objections and questions from opponents of previous versions of the effort to identify purchasers of pre-paid wireless devices and sim cards. The current bill requires:

- 1) The Secretary of Administration to issue a request for proposals and select a company provider “with demonstrated capabilities of working with law enforcement agencies and PROTECTING CONFIDENTIALITY and ELECTRONIC DATA;
- 2) The provider selected shall provide all necessary equipment, software, and training to the sellers of pre-paid wireless devices. Training shall be at the seller’s location and the equipment, software and training shall be FREE TO THE SELLER of the devices;

- 3) The mobile communications devices identification system shall be a central repository of information received by sellers from purchasers and maintained for the purpose of responding to lawful requests from law enforcement agencies;
- 4) Any information stored in the repository that is not part of an on-going judicial process must be destroyed after two years;
- 5) Information contained in the repository shall be confidential and only used for investigatory or evidentiary purposes and is not subject to the Kansas open records act. Information may only be released to law enforcement officers, prosecutors, and defense counsel.

**Process:** The bill requires:

- 1) Sellers, prior to the completion of any retail sale shall require a purchaser to provide a valid government issued identification card and on equipment/software provided by the vendor FREE to the seller record the purchaser's name, home address, and the mobile equipment identifier;
- 2) The seller shall record all such retail transactions through an electronic filing process;
- 3) Information from the system operator (independent data manager) shall be available to law enforcement officers upon production of a subpoena or other court order. The court order is waived in the event of an emergency situation that involves the risk of death or serious physical harm;
- 4) A seller that knowingly fails to electronically record any such retail transaction shall be liable to the state for a civil penalty not to exceed \$100;
- 5) COSTS OF OPERATING the mobile communications devices identification system may be no greater than one percent of the purchase price;
- 6) SELLER OPTION, the seller may (but is not required to) charge and retain up to a \$2 administrative fee per transaction. This optional fee is separate from the mobile communications devices identification system fee;
- 7) The purchaser, not the seller, is liable for the mobile communications devices identification system fee; and
- 8) The Dept. of Revenue may retain up to \$70,000 the first year to pay for programming and other one-time costs.

**Political Realities:**

- 1) Kansas would be the first state to implement such a law – hence the requirement that the vendor bear the financial costs of establishing and operating the data repository, providing the equipment and software, and training retailers' employees; Some state must be first, just as Oklahoma was the first state to require purchasers of certain pharmaceutical products that can be used to make methamphetamine to show government identification prior to the purchase.
- 2) Only vendors experienced in multi-state programs involving law enforcement and data security and confidentiality will be permitted to respond to the request for proposals;
- 3) This bill/law will not materially impact "grandma" or any other person purchasing a pre-paid wireless device and no one will track teenagers' calls (unless that person is part of a law enforcement investigation);

- 4) We currently require the showing and recording of persons' identities and addresses when purchasing some pharmaceutical products and when selling copper and other metals to recycling centers. The proposal to require identification for purchasers of pre-paid communications devices is no different and no more onerous.

**Summary:**

- a) There are no costs to the State;
- b) There are no costs to the Retail seller of wireless communications devices;
- c) The selected data repository vendor must keep information confidential and available only to law enforcement agencies upon providing a court document;
- d) Retailers may collect a "convenience fee" on each transaction for participating;
- e) Law enforcement agencies will have another tool with which to address organized gangs engaging in human trafficking, illegal drug activities; and other crimes;
- f) This is no more an intrusion into people's privacy than the pharmaceutical purchase and metal sales registries.

Thank you for your attention and consideration, I will be pleased to respond to questions at the appropriate time.