INTERGOVERNMENTAL ADVISORY COMMITTEE to the FEDERAL COMMUNICATIONS COMMISSION

ADVISORY RECOMMENDATION No: 2015-9

In the Matter of Pre-Paid Wireless Devices in Criminal Activities

The Intergovernmental Advisory Committee ("IAC") to the Federal Communications Commission ("Commission") submits this Advisory Recommendation.

I. Pre-Paid Wireless Communications Devices and Sim Cards

1. Based on law enforcement reports and experiences, the FCC (Commission) should recognize that stolen mobile communications devices (often reported as mobile or cell phones) are frequently used in criminal activities. The Commission's Technological Advisory Council (TAC) is looking into how to prevent thefts by using technological solutions to make stolen mobile devices less valuable to criminals. The IAC commends the TAC and the Commission for addressing the issue of mobile device theft. The IAC believes the Commission should also explore whether pre-paid mobile devices should be registered to the purchaser of the device(s). Currently, when a pre-paid mobile device is purchased at a retail store, the purchaser does not have to register the device. Registering the pre-paid mobile device may prevent its use by criminals by making the device traceable to a particular person.

2. Based on law enforcement experiences, the IAC encourages the Commission to explore the connection between public safety and pre-paid wireless devices and Sim cards. The Kentucky 2014 Commercial Mobile Radio Service Annual Report (page 20) reports that almost one fourth of all wireless phones sold are pre-paid. While the vast majority of such sales are to people unwilling or unable to afford a "Plan," wanting to limit use to emergencies by senior citizens or children, or other legitimate reasons, a significant number of such devices are acquired by criminals. Pre-paid devices are attractive to criminals because of their anonymity. While law enforcement officers are well aware of the use of stolen wireless devices in criminal activities, Commissioners and staff may wish to consider problems law enforcement officers have in protecting the public from persons using pre-paid devices for criminal activities.

3. On behalf of the Atlanta Police Chief and at the request of an IAC member, The Police Chief's Chief of Staff reported that, "We fully support mandatory registration of pre-paid cellular devices." They further stated, "During a recent investigation concerning a series of violent home invasions, the criminals made use of pre-paid cellular phones to communicate with one another. The signatory subscriber was fictitious and the phones were discarded and replace every month. This is indicative of

the fact that criminals are becoming very aware of law enforcement's ability to track phones and develop evidence from the analysis of historical cell site location information."

4. The New York Police Department, at the request of an IAC member, stated: "Issues with pre-paid phones are prevalent and significant in homicide, home invasion, and drug deal investigations."

5. Persons who purchase a cell phone and a service plan provide their name, address, and other identifying information for billing purposes. In testimony before the Connecticut General Laws Committee on February 3, 2015, on Senate Bill 66, CTIA stated: "When a wireless customer enters into a monthly contract to receive wireless service, oftentimes a social security number is requested to serve two purposes: to perform a credit check to ensure the wireless customer will be able to meet the monthly payment obligations; and to verify the customer's identity. Verifying a social security number both authenticates the wireless customer and helps prevent fraudulent subscriptions. This authentication process is beneficial for both wireless companies and consumers by ensuring that companies and consumers are not victims of fraud."

6. For example, Kansas House of Representatives 2015 HB 2084 would require the retailer to provide the information on purchasers of pre-paid mobile devices and Sim cards to a database manager on the same basis that is required by purchasers of some pharmaceutical products and by sellers of metal to recyclers. No government agency would control such information, but it would be accessible to law enforcement officers with an appropriate court order.

7. Kansas' HB 2084 accepts the important and accurate statement that CTIA made in Connecticut, that there is a valid reason to require consumers purchasing wireless devices to provide social security numbers (some form of government-issued identification) for consumer and provider protection.

8. If there is a valid reason for telecommunications providers to collect personal data on some wireless device purchasers for public safety reasons, then clearly obtaining similar data from all purchasers, including those with pre-paid mobile devices, will better serve the public safety interests of consumers and society.

9. Law enforcement officers and retailers report that purchasing Sim cards and replacing those within previously purchased wireless communications devices (those on a Plan or pre-paid) further masks the identity of the device and its user.

10. A Major in the Kentucky State Police summarized crime data contained in the KYOPS System. "In the period 2012 through 2014, nearly 13,000 criminal cases were opened in the Commonwealth related to portable electronic communications. Many of these involved thefts of devices, yet other crimes were of a much more serious nature. Hundreds of crimes related to drug trafficking were logged. During that same period there were 27 murders, 54 rapes, over 800 robberies involving use of force, and 1,500 burglaries **with some tie to portable electronic communications**" (emphasis added).

11. In testimony before the Kansas House Utilities and Telecommunications Committee on February 19, 2015, the representative of the Kansas Chiefs of Police, Sheriffs Association, and Peace Officers

Association reported on a survey of members about their experiences trying to investigate crimes in which pre-paid phones were used. "Drug investigators tell us a majority of drug trafficking cases involve the criminals using these 'drop' phones to conceal their identity. But, these cases involve investigations of phone harassment, stalking, death investigations, child pornography, human trafficking of juveniles in the sex industry, burglaries, thefts, and even homicides." The experiences and problems associated with tracking purchasers of pre-paid communications devices reported by law enforcement officers in Atlanta, New York City, Kansas, and Kentucky are not unique to those states.

12. With proper cause, law enforcement officers can secure a Court order subpoenaing information from a wireless provider for devices included in a Plan when a device represents material evidence in a case (e.g., to identify callers, persons called, timelines). This is not possible when pre-paid phones are registered without subscriber information. Currently persons can purchase multiple pre-paid or "burner" phones and register them using false identification (and if registered from a public library computer, without leaving a trace through an ISP). Without being able to identify the purchaser of a device found in conjunction with a criminal investigation, law enforcement officers have no way to pursue additional information from the telecommunications provider, nor the purchaser, especially for someone who purchases multiple devices for multiple persons.

II. Commission Issues

13. The Commission has jurisdiction over the spectrum used for wireless communications and has jurisdiction over wireless telecommunications providers.

14. The Court decision in *Telecommunications Regulatory Board of Puerto Rico v. CTIA-Wireless Ass'n, 752 F.3d 60, 1st Cir. 2014* stipulated that government agencies may not collect data on the purchasers of telecommunications devices. It does not preclude telecommunications companies, retail vendors, or others within the manufacturing-point of sale supply chain from collecting such data. It also does not prevent law enforcement officers with a proper Court order from securing data from such a repository when investigating a crime. It is also important to note that testimony on Kansas' HB 2084 (2015 HB 2084) established that the technology exists to collect relevant information from purchasers in a very timely manner and without cost to the retailer or telecommunications provider, based on multiple states' success with pharmaceutical and metal sale data repositories.

15. CTIA testified in Connecticut (testimony) that the telecommunications providers can and should maintain customer information databases. The Commission can direct or work with the telecommunications providers to develop and maintain such a database for pre-paid devices and Sim cards on the same or similar basis as they do for devices on a Plan. This database can be developed and maintained directly by the telecommunications providers or through an independent, cyber-secure third party.

16. The Commission's web site notes that the Public Safety and Homeland Security Bureau supports initiatives that strengthen public safety capabilities to assist law enforcement.

17. The Commission thus has a public safety interest in assisting law enforcement officers in protecting the law-abiding citizens who are victims and potential victims of criminals using pre-paid mobile devices that cannot currently be traced to a user. Notwithstanding that the Commission is generally viewed as a policy-making body, there exists an obligation, as with all persons in public service positions, to cooperate with law enforcement officers in whatever manner possible to improve public safety related to these communication devices issues.

18. IAC members are aware that most pre-paid devices are sold to honest citizens and residents, including senior citizens and undocumented residents. Additional devices are purchased by parents for young children to use in emergencies. IAC members reiterate that requiring the recording of data from government issued identifications, including alternatives to drivers' licenses that states readily make available, will not be a burden to customers, retailers, or the telecommunications providers.

19. Similar database collection and management are used to protect against criminals purchasing some pharmaceutical products and selling stolen copper and other metals. This allowed an IAC member who visited several pharmacies to measure the length of time necessary to record the data prior to purchasing restricted pharmaceutical products. In each instance, the clerk required less than 8 seconds to record the data from the individual's driver's license. In a separate "experiment," the information was manually recorded in 30 seconds. Similar visits to scrap metal dealers revealed the same time parameters for recording the relevant information for the database.

20. Testimony provided by a data repository during hearings in Kansas on HB 2084 included that the repository manager provides the hardware and software to pharmacies so that there is no cost to the retailer. The repository also provides employee training to the pharmacies staff members, again so there is no cost to the retailer. Cost of this consumer protection is paid for by a small charge on purchases.

21. IAC members also reiterate that existing databases and the intent of that proposed here require law enforcement officers to secure appropriate court orders before the repository manager can release the data. Unless such a court order is secured, the personal information of purchasers of pre-paid mobile devices and Sim cards will not be accessed by any government agency, and, if a third party repository is developed, the same will be true of telecommunications providers, thus preserving the purchaser's privacy. IAC members believe that constitutionally guaranteed civil rights protections will not be violated by establishing a registry, just as they are not for registering persons selling metal or purchasing pharmaceutical products. IAC members also believe the Commission should always be cognizant of civil rights protection issues.

III. IAC Recommendations

22. The IAC recommends the Commission examine public safety issues related to the purchase and use of prepaid mobile communications devices and Sim cards by criminals. Such examination may include analysis of existing technologies available to cost-effectively and quickly collect relevant identification information on purchasers and store that data in secure repositories independent of government, and potentially telecommunications providers, with access only via valid court orders.

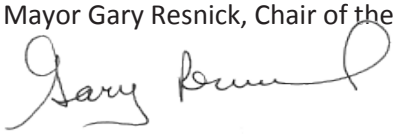
23. The IAC encourages the Commission to include federal and state law enforcement personnel, telecommunications providers, retailers, data repository managers with proven records of maintaining data security, and other parties as deemed appropriate to assess the problem and identify cost-effective policies and programs.

24. The IAC stands ready to assist in this process and to participate as these discussions go forward, to the extent requested by the Commission. As law enforcement officers, telecommunications service providers, and other stakeholders agree that there is a valid public safety requirement to prevent the use of pre-paid wireless devices by criminals, it is reasonable for the Commission to work with and encourage all relevant parties to cost-effectively develop secure databases that protect individual privacy, while permitting legitimate law enforcement activities in the protection and defense of our citizenry.

Thank you for this opportunity to provide these recommendations.

Respectfully submitted,

Mayor Gary Resnick, Chair of the IAC



September 15, 2015