INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief Mark Marshall

President
International Association of Chiefs of Police

Before the

Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

United States House of Representatives

February 17, 2011

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning Mr. Chairman and Members of the Subcommittee,

My name is Mark Marshall and I serve as the Chief of Police in Smithfield, Virginia and I also serve as the president of the International Association of Chiefs of Police. I am here today representing over 20,000 of IACP's members who are law enforcement executives in over 100 countries throughout the world. I am pleased to be here this morning to discuss the challenges currently confronting the U.S. law enforcement community on electronic surveillance issues.

In the United States, there are more than 18,000 law enforcement agencies and well over 800,000 officers who patrol our state highways and the streets of our communities each and every day. A great number of those officers also use electronic surveillance as they investigate crimes. Each day, state, local, tribal and federal law enforcement agencies use lawful electronic surveillance as a critical tool for enforcing the nation's laws and protecting the citizens they serve. Moreover, electronic evidence is now a routine issue in all crimes and at most crime scenes.

The IACP believes that lawful interception of voice and data communications is one of the most valuable investigative tools available to law enforcement in identifying and crippling criminal and terrorist organizations. Understandably, there is an increased volume and complexity of today's communication services and technologies. And, the evolution and development of communication devices has had a significant impact on law enforcement's ability to conduct electronic surveillance, as well as to recover valuable evidence from communication devices. Additionally, legal authorities and mandates have not kept pace with changing technology. CALEA or, the Communications Assistance for Law Enforcement Act, for example, does not cover many types of services that are routinely used by criminals.

The advanced features of today's phones can process more information about where people have been, who they know and are calling, what they are texting, pictures they have and are sending, as well as larger amounts of data than ever before. Information

recovered can also produce connections to other media like Facebook and Twitter, contact lists, call history, calendars, GPS waypoints and email. If properly recovered, this sort of stored data on communication devices has great investigative and intelligence value to assist law enforcement with investigations.

Many agencies that need to be able to conduct electronic surveillance of real time communications are on the verge of "Going Dark" because they are increasingly unable to access, intercept, collect and process wire or electronic communications information when they are lawfully authorized to do so. This serious intercept capability gap often undercuts state, local, and tribal law enforcement agencies' efforts to investigate criminal activity such as organized crime, drug-related offenses, child abduction, child exploitation, prison escape, and other threats to public safety.

This must change—law enforcement must be able to effectively use lawful electronic surveillance to combat terrorism and fight crime. Law enforcement needs the federal government to generate a uniform set of standards and guidelines to assist in this exploration. In order for law enforcement to maintain its ability to conduct electronic surveillance, laws must be updated to require companies that provide individuals with the ability to communicate too also provide law enforcement with the ability to lawfully intercept those communications in a timely and cost effective manner.

In September of 2010, the Law Enforcement Executive Forum (LEEF), comprised of law enforcement executives, including many from the IACP, released a plan to address the spectrum of issues related to electronic surveillance and to law enforcement's ability to recover and process data stored on communication devices. This plan, National Domestic Communications Assistance Center (NDCAC) Proposal, calls for a strategy to be created to address issues related to maintaining law enforcement's ability to conduct court authorized electronic surveillance. For instance, to determine if a solution within the law enforcement community exists and promote knowledge-sharing among law enforcement agencies and groups regarding technical, legal, policy, and other issues.

The Proposal also calls on Congress and the Administration to make funding available to establish the National Domestic Communications Assistance Center. The Center would leverage the research and development efforts of the law enforcement community with respect to lawful electronic surveillance capabilities and the ability to obtain communications device information. The Center would also facilitate the sharing of technology between law enforcement agencies. Finally, the Center would partner with industry to develop CALEA-related technical standards for services beyond those already being addressed by the FBI. The IACP fully supports The Proposal.

The IACP believes that carriers must be required to install, deploy and make available to law enforcement a solution to assist with lawfully authorized electronic surveillance of telecommunication services prior to or concurrent with the release of communications products to the public. The IACP also strongly urges that telecommunications carriers provide law enforcement agencies service for cost and not retail value.

The IACP calls on Congress to take into account the National Domestic Communications Assistance Center (NDCAC) Proposal and use the Proposal's recommendations to create a national strategy to assist state, local and tribal law enforcement in addressing the technical developments and issues related to electronic surveillance.

State, local, tribal and federal law enforcement are doing all that we can to protect our communities from increasing crime rates and the specter of terrorism—both in our streets and in the many communications devices available today, but we cannot do it alone. We need the full support and assistance of the federal government and clear guidance and regulations on our use of lawful interception of voice and data communications to aid us in successfully investigating and prosecuting the most dangerous of criminals.

Thank you.