

**Testimony before the United States House Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security**

**Hearing on “H.R. 1981 - Protecting Children From Internet
Pornographers Act of 2011”**

**Michael J. Brown
Sheriff, Bedford County, VA
Executive Committee Member and Board of Directors
Member, National Sheriffs' Association**

July 12, 2011

Good Morning Chairman Sensenbrenner, Ranking Member Scott, and Members of the Committee. My name is Michael Brown and I currently serve as the Sheriff of Bedford County, VA. I also serve on the Executive Committee and Board of Directors for the National Sheriffs' Association (NSA). The National Sheriffs' Association represents the 3,083 elected sheriffs across the country and more than 20,000 law enforcement professionals, making us one of the largest law enforcement associations in the nation. I am pleased to have this opportunity to appear before you today to discuss **H.R. 1981 – Protecting Children From Internet Pornographers Act of 2011**.

The expansion and development of technology has enabled child pornography to become a worldwide epidemic. Child predators have become adept in exploiting their perversion and hiding behind the anonymity of the Internet, making it difficult for law enforcement to identify these predators. As such, unmasking child pornographers on the Internet is a painstaking and complex process for law enforcement officers and typically requires assistance from Internet Service Providers (ISP) to accurately identify the perpetrator.

However, some ISPs only retain their clients' records for a short period of time. It could be hours. It could be days. It could be weeks. It could be months. And it varies from ISP to ISP. As such, the limited data retention time and lack of uniformity among retention from company to company significantly hinders law enforcement's ability to identify predators when they come across child pornography.

Mr. Chairman, protecting our nation's children against internet predators has been a personal crusade of mine. Since 1998, the Bedford County Sheriff's Office has administered the Southern Virginia Internet Crimes Against Children Task Force

(SOVAICAC) in an effort to crack down on child pornography distributed over the Internet and other computer-related crimes. The SOVAICAC Task Force includes a supervisor, four full time investigators, two forensic analysts, an intelligence analyst, and 64 affiliate law enforcement agencies who blend their talents and resources to fight child exploitation on the Internet.

To help law enforcement combat internet child pornography, Congressman Lamar Smith (R-TX) and Congresswoman Debbie Wasserman Schultz (D-FL) introduced the **H.R. 1981 – the Protecting Children From Internet Pornographers Act of 2011**.

Through H.R. 1981, ISPs will be required to retain the IP addresses and all associated customer information, i.e., billing, lease initiated and expiration information (date IP address assigned and expired) assigned to customers for 18 months. The 18-month provision is critical as it will ensure that when law enforcement contacts an ISP looking for a child predator, the identifying information will still exist.

I would like to give you a real life example of why we need this time limit in regards to ISP data retention. A cybertip from the National Center for Missing and Exploited Children (NCMEC) came into the Southern Virginia ICAC office in February of this year (2011). This case involved someone posting that they were exposing themselves to their 2 ½ year-old child. The only piece of evidence was the IP address that was accessing a YAHOO chat room through a NTelos wireless connection. While going through the legal process to access the information, we discovered that the ISP only kept the MAC (Media Access Control) address and IP history for a period of 30

days. Sadly, the 30-day limit had passed since the evidence was posted. The case had to be closed due to the lack of further investigative material.

This case, and hundreds like it from the files of the ICAC Task Forces, clearly demonstrates the need to ensure that ISPs retain customer information for law enforcement.

Child predators have become technologically savvy and are able to skillfully conceal their identities. As such, it can take law enforcement time to comb through the multitude of online information to successfully identify and locate the child pornographer. Therefore, it is imperative that data be retained by ISPs for a significant and standard period of time so that when law enforcement goes to lawfully request the online information and records, the information still exists.

Additionally, H.R. 1981 provides legal protections for ISPs to further facilitate cooperation with law enforcement and help ease concerns that the ISPs could be held civilly liable for sharing customer information with law enforcement during valid investigations.

H.R. 1981 also creates a new federal offense for individuals who profit from child pornography; significantly enhances penalties for possession of child pornography; provides administrative subpoena authority to the U.S. Marshals to access critical travel information and records on fugitive sex offenders; and strengthens the protections for child witnesses and victims. Those who prey upon children are among the vilest offenders in society and the aforementioned provisions will ensure that the predators are appropriately and strongly punished.

As sheriffs, it is our responsibility to protect society's most vulnerable – our nation's children – from the evils of the world. Child pornography is one such evil. The provisions within H.R.1981 provide law enforcement officers the capabilities necessary to combat child predators and child pornography. The National Sheriffs' Association strongly supports H.R. 1981 and looks forward to working with Congress on passage of this legislation.

I want to thank you for the opportunity to come before you today to discuss **H.R. 1981 – the Protecting Children From Internet Pornographers Act of 2011.**