

**Statement of Sheriff Michael J. Brown
Bedford County, Virginia
19 September 2006
Washington, DC**

Prepared for the Senate Committee on Commerce, Science and Transportation

Senator McCain and distinguished members of this committee, thank you for inviting me to testify before you today.

My name is Mike Brown; I am the Sheriff of Bedford County, VA, home of the National D-Day Memorial. I am a retired federal agent with 42 years of law enforcement experience on a local, national and international level.

Since 1998, I have directed a Department of Justice, Office of Juvenile Justice and Delinquency Prevention, Internet Crimes Against Children Task Force...or, to shorten that a bit...an ICAC Task Force named Operation Blue Ridge Thunder. Our task force is responsible for Virginia and West Virginia, with the exception of five counties in Northern Virginia which are ably protected by the Virginia State Police ICAC Task Force.

I will not take up your time, nor my allotted time, by giving you a lot of statistics... your staffers are quite capable of researching this subject and providing you with reams and reams of stats, charts and graphs about children and the Internet, porn and the Internet, sexual solicitation over the Internet, unwanted exposure to sexual material, etc.

You asked that I address what, if any, appropriate controls might be placed on child pornography on the Internet, and how the government can help.

First, let me give you an idea of what goes on in this cesspool of child porn on the Internet...what we hear and a description of what we see.

On any given day an ICAC Task Force Investigator, assigned to any of the 46 task forces, will view the following:

The investigators are looking at a young female, as young as 3 to 4 years of age (the images can be either digital images or videos)... there is a look of stark fear on her face. She is being forced to perform any number of graphic sexual acts with an adult male or males...oral sex, vaginal sex, anal sex; many of the images have another adult male ejaculating on this young girl, most of the time on her face. Image after image...video after video...hundreds of thousands of them!

Parry Aftab, Cyber-Lawyer described the scene best, and I paraphrase:

“In most of the videos the cameraman has the young female facing the camera. All of her, and his, genitalia are graphically displayed in the video...close up, wide angle, overhead, side...a flash or special lighting is clearly being used and shone in her face to illuminate the graphic rape. The little girl was not only being painfully molested, she was forced to bear the additional humiliation of being filmed at the same time. Unable to stop the rape, she did the only thing she could do to protect herself: She shut her eyes.

Most parents understand this gesture. When our children are very young, they think that by closing their eyes they become invisible. They stand in front of us, thinking that if they can't see us, we can't see them. "Mommy, can you see me?" is the game of the day, and we all pretend that we can't. We call out to them, "Where are you? We can't see you!" pretending to look everywhere for them. The game ends with lots of giggling, tickling, laughter, and hugs. This little girl's attempt to be invisible would end very differently.”

Welcome to the world of child pornography on the Internet.

ICAC Task Force investigators, and other investigators working in local, state and federal cyber units, see these images every day...it use to be just (forgive me, how do I say “just”) one dimensional images, now it ‘s video “streams”, and if you look hard enough it can be live “stream” video. One of the most sought-after videos at this time is one of an adult male attempting to sexually penetrate what appears to be a 2 to 3 year old female. He removes her diaper at the start of the video. Investigator O’Neal mentions this in his recorded comments to this committee.

There is a 40 second video clip, according to Department R, Russian Police (Unit in charge of hi-tech crimes), where two sexual predators have sex with a young girl (10/12 years old?) after which they stab her, cut off her ears and smash her face to a bloody pulp. This clip, as reported by the Russian police, was first noticed by the US authorities. US police experts assert that the video footage represents real activity, not imitation.

Our investigators routinely pose as children, young teens, and like minded adults, in chat rooms on the Internet. Posing as a child they simply place their profile in the chat room, usually a 12, 13, 14 year old female...and then just sit back and wait. In a nana second they begin to be “hit” on by the sexual predator surfing the web for his next victim. Sometimes the predator takes his time and tries to schmooze his way in. More often that not, they simply open the conversation with, “What are you wearing, how big are your breasts (and I’m being polite), do you want to have sex, if I send you a video cam would you masturbate for me, would you like to see me masturbate, how far have you and your boyfriend gone...oral sex, anal sex, vaginal sex, are you a virgin, do you like to perform oral sex, how big is your boy friend’s penis, would you like to have sex with a real man with a big penis, would you like for someone to urinate/defecate on you”... and then offers or just sends porn pictures...sometimes adult, often child.

When posing as a like minded adult they are often engaged by parents or care-takers wanting them to share in the abuse, and or sexual exploitation of children in their care. These care takers and parents are often the persons responsible for the manufacturing and distribution of the horrific pictures and videos available on the web today.

Welcome to the world of child pornography on the Internet.

What can our government do?

Now to address what, if any, appropriate controls might be placed on child pornography on the Internet, and how the government can help.

The controls are already there in the form of our Federal law, codified at Chapter 110 of Title 18, 2251, United States Code, which prohibits all aspects of the child pornography trade, including its production, receipt, transportation, distribution, advertisement, possession, and enticing children to engage in unlawful sexual acts.

We can support these code sections with the following, just to mention a few:

- Federal courts that ensure the application of the appropriate punishment for convicted persons
- Ensure, through hefty fines, that communication services providers report the presence of child pornography on their systems, and do so in a timely manner
- Improve data retention requirements for all ISPs (6 months min., one year preferred)
- Encourage foreign governments to crack down on child porn in their country and to work with our law enforcement agencies, not only our federal agencies, but our national ICAC Task Forces.
- Pursue efforts to insure that taxpayer dollars are never used to fund Internet access without appropriate transactional logging to allow the location of individuals that use that access in the exploitation of children. How can we in good conscience demand that corporate Internet service providers log transactions if our own government, be it municipal, state, federal, or educational institutions fail to do the same.
- I would encourage continued support for the ICAC effort to coordinate child exploitation investigations through the ICAC Data Network. The computer systems used to facilitate our reactive and proactive investigations now represent over 6 million transactions involving criminal exploitation of children. The volume of information is overwhelming and we must fight to leverage technology as a force multiplier, giving us greater capabilities with our limited manpower.

In my forty-two years of law enforcement experience I don't think I've ever worked with a more dedicated and professional group of criminal

investigators...investigators like *Flint Waters (WY), Dave Peifer (PA), Ronnie Stevens (NY), Scott Christensen (NE), Mike Harmony (VA)...and, retired legend, Sergeant Nick Battaglia (CA). And, being from the federal system I know what a good administrator is, and the ICAC Task Forces have two of the best...OJJDP's Administrator Bob Flores, and Ron Laney, Director, Child Protection Division, OJJDP. I salute them all!

***This man could be making a million dollars in the private sector, but he chooses to stay in the public sector helping keep our children safe from the sexual predators that prowl the Internet.**

An invitation:

At this time I would like to extend a formal invitation to this committee, or someone on your staff, to drive down to Bedford, its only about 3.5 hours southwest of DC, and visit one of your ICAC task forces, Operation Blue Ridge Thunder, at their undercover location just outside of Lynchburg, Virginia. You will leave this location with a sense of urgency to do whatever is necessary to protect our most precious commodity...our children.

I invite you to look at the attached information for the ICAC Taskforces and view the brief remarks that follow. This is a clear representation of the work that the ICAC are doing and what they have and can do in the future.

	1998-2002	2003	2004	2005	2006	Totals
Travel/Enticement	1810	581	835	3429	4349	11004
CP Manufacture	322	116	3933	34062	1724	40157
CP Distribute	2836	768	9724	154545	4040	171913
CP Possession	5617	1726	6783	6306	5042	25474
Totals*	10028	3637	24138	****198883	16423	253109

Arrest		1418	1474	1575	1623	1744	7834
Victims ID**	NA			141	275	1135	1551
Technical Support***	NA		3563	4871	6143	6784	21361
Forensic Examinations***	NA		2594	2770	6131	8406	19901
LEO/Pros. Trained***	NA		5487	14561	12502	16413	48963
Case Referrals		1980	1205	4718	3869	3689	15461

* 2006 Stats thru July 2006

** Victim ID Collection Started 2004

*** Data not available

**** Task Forces started collecting P2P Transaction Data, stopped after only 2 months. **6 Million Transactions in 24 Months.**

The 2006 Stats are only through July of 2006. The ICAC program is on pace to hitting some milestones, to include breaking 2,000 arrests in one fiscal year, as well as breaking the 8,000 mark since the program's start.

Please note: Traveler/Enticement cases indicate a significant increase from FY05 to FY06. So far in 06 there are almost a 1,000 more cases of traveler/enticement over last year. That's about a 32% increase already this year, with several months' worth of data not in.

Additionally, in my opinion it is very noteworthy that the number of victims identified as a result of ICAC cases has increased... a total of over 1500 in just two years. To clarify; these are child victims who have been identified as a result of an ICAC investigation.

Lastly, the number of Forensic Exams the ICACs have already completed in FY06 is staggering... knowing how much data is due for the remainder of this fiscal year. If I were to guess, this number will break 10,000. I would also assume that this is due, in large part, to the increased number of computers being seized on any given case which, in turn, is increasing the number of exams needing to be completed.