



National District Attorneys Association
Staff Contact: Frank Russo
703-519-1655 or frusso@ndaajustice.org
www.ndaa.org

Senate Committee on the Judiciary Hearing

“Protecting Innocence in a Digital World”

July 9th, 2019

Testimony of Solicitor Duffie Stone

Solicitor of the Fourteenth Judicial Circuit, South Carolina
Incoming President, National District Attorneys Association

Chairman Graham, Ranking Member Feinstein, members of the committee, thank you for inviting me to speak with you today concerning the protection of our children in a digital world. I am Duffie Stone. I am the Solicitor or the elected prosecutor for the 14th Circuit in South Carolina. I am also the President–Elect of the National District Attorneys Association. Most importantly, I am a parent.

First, I think that we need to understand the reality of the world in which we live. As parents, we teach our children from an early age not to talk with strangers. We teach them not to open doors unless you know who is on the other side. We would be shocked to see our child standing in the dark shadows talking with an adult that we did not know. We would immediately call the police if we saw anyone crawling in the window of our child’s room, regardless of the time of day.

We take precautions against these threats. We equip our homes with security systems and even cameras that we turn on only after we have locked all of our doors and all of our windows. Our legislatures even pass laws that seek to limit sex offenders’ access to our children in parks and schools.

And yet, predators are communicating with our children every day. They are coming into our child’s bedrooms. They are coming into our house, past the locked doors, the cameras and the security systems. How are they getting in? The internet. Our children, sometimes unknowingly, invite them in with their cell phones and computers.

Statistics show that today almost every child in the United States has access to the cyber world, most through their cell phones. A Pew Institute study from 2018 stated that 95% of teens report having a smartphone that gives them access to the internet. 45% of teens say that they are online on a near constant basis. Further, while computer use by teens seem to vary by income, the same study indicates that smartphone access does not. Rich and poor alike have access and are therefore at risk.

The risk to the wellbeing of our young is substantial. According to the National Center for Missing & Exploited Children (NCMEC) over 18.4 million reports were made to their Cyber

Tipline in 2018. Further, a study conducted by NCMEC in 2017 found that of the total reported offenders, 98% were individuals seemingly unknown to the child, strangers. A June 27th, 2017 State Department Report Concerning Online Sexual Exploitation of Children states:

“New technologies are facilitating the online sexual exploitation of children, including the live streaming of sexual abuse of children using web cameras or cellphones, often for profit. Mobile devices also provide new and evolving means by which offenders sexually abuse children as apps are being used to target, recruit, and coerce children to engage in sexual activity. Experts believe tens of thousands of children globally are sexually exploited online, and the number appears to be growing. The victims may be boys or girls, ranging from very young children to adolescents, and hailing from all ethnic and socio-economic backgrounds.”

Prosecutors and law enforcement officials are fighting these predators throughout the country. South Carolina was one of the first states to start an Internet Crimes Against Children program. This program, started in 1999, is run by our Attorney General’s Office. They prosecute most of our state’s online predators. Last year the South Carolina Attorney General’s office indicted 250 online predators on 1379 charges. This was a 24% increase in arrests over the previous year. While these arrests were being made, five forensic analysts were reviewing new cases. Last year these analysts reviewed 85 cases and 2006 digital items that contained 1,086,910 files of child pornography. The most egregious of the files become the subject of warrants.

Prosecutors’ offices and law enforcement agencies are using sophisticated tools in this fight. In January 2018 Manhattan District Attorney Cyrus Vance, testified before the House Financial Services Committee Subcommittee on Oversight and Investigations concerning online human trafficking. Mr. Vance noted that his was one of the first prosecutor’s offices in the country to use a ground-breaking search tool called Memex. This is an advanced search engine tool that crawls the dark web locating and tracking human traffickers. It was created by the U.S. Department of Defense’s Defense Advanced Research Projects Agency (DARPA), and it organizes intelligence from online prostitution advertisements to aid human trafficking investigations and prosecutions.

Mr. Vance went on to explain that this program was used in 271 human trafficking investigations and in six new sex trafficking indictments that were brought in 2017.

Small and medium sized District Attorneys' offices are also employing intelligence to aid in the discovery of crimes being perpetuated against our youth and gathering cyber data to improve the prosecution of these crimes. My office employs roughly 30 prosecutors and 30 support staff. Nationally speaking we are an average sized prosecution office. We spend over 14% of our personnel budget every year on intelligence and investigation. We have on staff computer and cell phone extraction experts. That is how important we think the cyber world is in keeping our community safe.

Even with these new approaches law enforcement and prosecutors still face significant challenges. I began my career as a prosecutor in January 1989. The next year I started prosecuting exclusively narcotic cases. When a narcotic officer executed a search warrant on a drug dealer's home, they would find drugs to sell, cash from the sales, scales to weigh the product and usually guns to protect it. This was good evidence against that dealer. However, some of the best evidence that could potentially take down the entire criminal enterprise was the dealer's notebook. This notebook commonly showed the names of the bigger traffickers, logistics, accountings of the profits and outstanding debt. It also showed a list of coconspirators who helped make the business work. Today's child sex trafficking industry needs the same infrastructure as the drug traffickers. They need suppliers, warehouses, transportation and customers. Traffickers keep track of all of that, not in notebooks, but on their cell phones.

As a prosecutor, my job is to protect the constitutional rights of all of our citizens, including people charged with crimes. I will never advocate for the trampling of those rights. Our Constitution provides a privacy right in people's homes and, of course, in their cell phones and computers. This right, however, gives way to a lawful search warrant backed by probable cause and authorized by a neutral and detached judge. Everyday law enforcement officers execute court orders that allow them to search through the most intimate areas of criminal suspects' homes and effects.

Court orders allowing law enforcement to search cell phones and computers should also be enforced. Yet cell phone and computer companies can deny law enforcement access regardless of what a judge has ruled. If we want our law enforcement to investigate child exploitation, we must allow them to effectively execute search warrants on criminals' smartphones as well as their houses by mandating cell phone companies comply with court orders and not evade them by refusing to provide give law enforcement security codes.

My circuit is comprised of five counties in what is called the low country of South Carolina. It spans over 3700 square miles. We have a population of over a quarter of a million people. One of my counties, Beaufort County, is the second wealthiest county in the state. It houses Hilton Head Island, the Heritage Golf Tournament and seemingly endless tourism. Allendale County is also in my jurisdiction. Unless you are from South Carolina you probably have never heard of it. It is the second poorest county in the state registering at the last census a 30% poverty rate. The average poverty rate in South Carolina is 16.6 percent. Three of my counties suffer poverty rates higher than that. We have heavy and conversely sparse, areas of population. We have a wide variety of racial and ethnic people. The white population of our circuit is between 67.4% to 22.5 %. The black population is from 73.5 % to 18.1%. The Hispanic population makes up between 13.2% and 3.1% of the population. All depending on the particular county. The demographics of my circuit are particularly relevant to this discussion because I find the same cyber issues in all of my counties and I believe that there are the same issues that can be found throughout the country. The Fourteenth Circuit is a microcosm of South Carolina and, in many ways, the United States.

While the dark web gets most of the attention for criminal activity, the more mainstream part is just as dangerous. Investigators in my office routinely see professionally made music videos produced by and for gangs. A few years ago, I watched one of these music videos. In it the participants are brazenly declaring themselves a gang, flashing gang signs, glorifying drugs, guns and violence. These videos show clips of officers walking the beat while the gang belittles them. Gangs are using similar videos to recruit new members, many of which are teenagers searching for a sense of belonging. I did not watch this on the dark web. I watched it on YouTube.

Our analysts compared this music video with a video from a local convenience store that depicted a shootout and were able to match a number of members of the gang with the shooters. My office then worked with the Justice Department on a RICO Act investigation and prosecution that convicted, and sent to federal prison, 15 of these gang members.

In May of this year I also prosecuted a teenager for shooting and killing another teenager in broad daylight in the most crowded area of Hilton Head. The shooter threatened the victim using Snapchat. The shooter obtained the .40 caliber handgun he used to kill after posting a request on his Facebook account. Some of the shooter's friends took him seriously. Those that did not ridiculed and challenged him on their social media accounts.

Analysts in my office also monitor the cyber activity of some that we have put in prison. One offender in particular is serving a 39-year sentence for murder and 20 years for attempted armed robbery. While he was in jail awaiting trial, he orchestrated the murder of one of the eyewitnesses by using a cell phone provided by a detention facility officer. We were still able to successfully prosecute him, but this witness was the sole witness to another murder committed by someone else that we had to dismiss. This offender continues to run a prostitution ring from his prison cell using smartphones. He routinely posts pictures on his social media pages of the cash that he has made and the phones that he uses to make it.

One of the purposes of prison and jail is to keep our community safe by isolating our worst criminals. If prisoners can get a cell phone and obtain a signal then they have access to everyone in our community, including our children. Physically placing dangerous predators in prison is not enough. We must isolate them by blocking their access to the internet by jamming their cell service. I want to thank Chairman Graham and Senator Kennedy for cosponsoring legislation allowing our prisons to fix this very dangerous problem.

Over the past ten years the biggest change in criminal justice I have seen has been the use of technology by criminals. They commit crimes, brag about them and lure others to join them. They threaten, bully and exploit people. All by the use of social media. Our children are perhaps the most susceptible to these acts. We no longer live in an exclusively bricks and mortar world.

We live in a world in which criminals can interact with our children without ever physically stepping inside our home. We must think about this threat differently than we have in the past. The safety of our children depends on it and we all have a role to play.

Mr. Chairman, Ranking Member Feinstein, members of the committee, thank you again for allowing me to speak to you and I will be glad to answer any questions that you may have.