

## **FONDAZIONE CENTESIMUS ANNUS PRO PONTIFICE**

### **2017 INTERNATIONAL CONFERENCE THE VATICAN, MAY 18 – 20, 2017**

#### **The Fight Against Human Smuggling and Economic Crime Presented By: Ernie Allen**

In his powerful presentation Raymond Baker notes that human trafficking is big business, a \$150 billion global industry. For more than thirty years I have focused on its most vulnerable and most hidden victims, the children.

This insidious practice thrives today because of its economics. It is easy, low risk and enormously profitable. I agree with Mr. Baker regarding the role of the shadow economy and the movement of funds from the developing world to the developed world. Yet, human trafficking and child exploitation do not just occur somewhere else on the other side of the world. They also occur right here in our enlightened, advanced Western world.

Mr. Baker's overview of the shadow economy is compelling. Yet, I submit there is one more factor to consider, one that has made the shadow economy even more central to this problem in the modern age. That factor is the internet. The internet has revolutionized the way we live, work and play. Yet, there is a dark side, with challenges unlike any we have ever seen before.

Two years ago a man in Sweden was convicted of the "long distance rape of children in the Philippines," which officials called "virtual trafficking." He hired men in the Philippines to obtain and rape children as young as 5, while he directed the assaults via webcam from the comfort of his home. Today, such "live streaming" of the sexual abuse of the world's poorest children, paid for and viewed by Western consumers, is big business.

There are no scientific incidence studies. Yet, the anecdotal data are overwhelming. In my nearly thirty years at the National Center for Missing & Exploited Children, in no single year did we handle as many as 1 million reports of child sexual exploitation. Yet, in 2016 the Center received 8 million. In 2002 we created a Child Victim Identification Program (CVIP) to identify and rescue children being sexually abused, whose photos were then disseminated via the internet. In 2003 we received 50,000 images from around the world. Last year, CVIP received 25 million. Child sexual exploitation has exploded with the advent of the internet.

How is this possible? Are that many people sexually attracted to children? Prior to the internet, someone with sexual interest in children felt isolated, aberrant, alone. Today, he is part of a global community. He can interact online with people of like interests worldwide. They share images, fantasies, techniques, even real children. And they do it all with virtual anonymity.

Last year authorities in Australia shut down a ring in which the child victim was adopted as a newborn, and then sexually abused and photographed from birth. The images were distributed via an encrypted network worldwide. The organizers then traveled with the child so members of this exclusive network could not only view the photos but also sexually abuse the little boy themselves. They were caught only because one of them made a mistake and their network was penetrated by law enforcement. At the time of the arrests, the child was 7 years old.

Canadian researcher Dr. Michael Seto estimates that at least 1% of males is affected by pedophilia (attraction to prepubescent children) and 3% by a combination of pedophilia and hebephilia (attraction to early teenage children). Today, there are 3.5 billion males on the planet: 1% is 35 million people; 3% is 105 million. This is not an insignificant problem, nor is it one that is limited to one country or one region or one institution. It is a global phenomenon.

Further, much of it is financial crime. A decade ago we received a lead that led us to the operators of a child pornography business. When their sites were shut down, they had 70,000 customers, paying \$29.95 per month and using their credit cards to access graphic images of small children being raped and sexually assaulted. One of their sites was called “Baby Rape.”

I called the Chairman of a major credit card company and asked, “how is this possible?” He said, “we don’t know what these transactions are for. If you can identify for us in a timely way where the account resides, who the merchant bank is, we can take action. This is an illegal use of the payments system.”

So, that is what we did. We brought together 34 major financial institutions in a Financial Coalition with a goal of eradicating commercial child pornography. One member, an Asian bank, hired a leading economic consultant to estimate the size of this illegal industry. The consultant said it was a \$20 – 30 billion industry. Concerned about the provability of the estimate, we simply called it a “multi-billion dollar industry.”

The companies donated live accounts. We provided the accounts to selected law enforcement which made purchases on illegal sites we identified. When the transaction went through, we would alert the payment company which would stop the payments and shut down the accounts.

We continued this process for seven years. In 2013 the US Treasury Department reported to me that in their estimation the problem of commercial child pornography had dropped to “effectively zero,” less than \$1 million per year. We had severely damaged the business model.

The companies wanted to hold a press conference and declare victory. But I was skeptical. I was convinced that we hadn’t ended it, we had just moved it. We concluded that this problem was migrating to a new kind of “shadow economy,” an unregulated, unbanked digital economy, fueled by internet anonymity and the use of virtual currencies. This new digital economy belongs to no nation and is overseen by no central bank.

This new digital economy is intertwined with the traditional economy, and includes cryptocurrencies, like Bitcoin, and many other vehicles for engaging in transactions and for sending or transferring money. Many of these have legitimate uses but are difficult to regulate. Russia's WebMoney has 31 million users. Africa's M-Pesa which allows users to send money via text message and store it via cellphones has 25 million users. There are many others.

To address this emerging phenomenon, I chaired a new task force which included law enforcement and financial leaders. It also included the Bitcoin Foundation, the Tor Project and others at the heart of this emerging challenge. We agreed on four fundamental premises:

1 – That this is a global phenomenon. Digital economy funds move network to network, not nation to nation. This is not a problem that any government can solve alone. It requires global cooperation and global leadership.

2 – That draconian regulation is not the answer and is, in fact, counter-productive. Many elements of the new digital economy are good. For example, according to the World Bank two billion people on the planet today do not have access to banks or credit cards. New technologies can help provide financial inclusion. We must be careful that we are not so aggressive in our approach that it simply pushes these enterprises into areas where there is little or no regulation, creating new safe havens.

3 – That there are existing laws and regulatory structures that should be utilized, focusing at the point at which digital currencies are exchanged for fiat currencies, like dollars, euros, pounds or yen. However, few countries have taken this step. And finally

4 – That the central challenge is internet anonymity. In the mid-1990s, the US government created Tor, a tool to enable anonymous internet use. It was designed to protect U.S. intelligence communications, and later to protect political dissidents and journalists from retaliation by repressive regimes.

The purpose was high-minded and noble. Yet, as with other innovations, there are unintended consequences. Political dissidents are not the only ones using these tools. Today, there is a "Dark Web," an anonymous, secret internet for drug dealers, weapons merchants, human traffickers, assassins, pedophiles, child exploiters and others.

A study by Portsmouth University in the UK found that while just 2% of Dark Web sites are pedophilia sites, they account for 80% of Dark Web traffic. And the Dark Web sites being used for commercial purposes are collecting payment primarily in virtual currencies.

Because advances in technology have outpaced changes in law, today law enforcement may be unable to trace even very large criminal transactions. I believe fervently in the right to individual privacy. However, I also believe there is a difference between privacy and anonymity, and that total internet anonymity is a prescription for disaster, ensuring unregulated safe havens for every form of criminality, including human trafficking and child exploitation.

Mr. Baker correctly notes that “the primary threat to peace and stability is coming from us, from our weakening of legal, ethical, moral practices.” I agree. I also submit that our challenge is to maximize individual privacy and human rights while balancing them against the rights of children to be free from abuse and exploitation.

*About the author: Ernie Allen serves as an advisor to governments, law enforcement, technology companies and others on the digital economy, public-private partnerships and child protection. Appointed by UK Prime Minister David Cameron, he chairs a global initiative to combat online child abuse and exploitation for the British Government. He is a founder and the former President and CEO of the National Center for Missing & Exploited Children, and the International Centre for Missing and Exploited Children.*