TESTIMONY

of

ERNIE ALLEN

PRESIDENT AND CEO

THE INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN

for the

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

"Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies"

November 18, 2013

Mr. Chairman and distinguished members of the Committee, I welcome the opportunity to appear before you today to discuss the challenges and opportunities associated with the emerging digital economy. We are deeply grateful for the Committee's leadership on these issues and its long-standing commitment to the safety of our children.

The International Centre for Missing & Exploited Children ("ICMEC") is a not-for-profit corporation, supported entirely by private funds and resources. ICMEC leads a global movement to protect children from sexual exploitation and abduction. We have

- Trained law enforcement in 121 countries;
- Reviewed laws in 200 countries and worked with parliaments in 100 countries to enact new law on child pornography.
- Reviewed laws in 200 countries, developed model law on child sexual exploitation, and worked with parliaments and international bodies to change national legislation and international conventions.
- Created a research institute, the Koons Family Institute on International Law & Policy, to examine child abduction and sexual exploitation and launch policy initiatives with world leaders.
- Built a Global Missing Children's Network, now including 22 countries.
- Worked with Belgium, Romania, South Africa, Russia, Belarus and others to establish national centers on missing & exploited children.
- Created a regional center, the Southeastern European Center on Missing and Exploited Children, serving thirteen countries in the Balkan region.
- Entered into formal partnerships with Interpol, the Organization of American States, the Hague Conference on Private International Law, and others.
- Hosted international conferences, including a 2009 meeting of 400 Arab leaders in Cairo which produced "The Cairo Declaration," an agreement on child protection; a 2010 conference of judges from 15 countries at the US State Department to examine cross-border transportation of children, resulting in the "The Washington Declaration," now cited in case law worldwide; and a 2011 forum in Rome in partnership with the Vatican, the Mayo Clinic and Il Telefono Azzurro, which produced "The Declaration of Rome" on children's rights.
- Managed private sector financial industry and technology industry coalitions to address child sexual exploitation.
- Launched a Global Health Coalition of pharmaceutical companies and health care institutions to attack the problem of child sexual abuse and exploitation not just from a legal and law enforcement perspective but as a public health crisis.
- And there is much more.

I am honored to have the opportunity to address the risks and the promise of virtual currencies. We are enthusiastic about the potential of virtual currencies and the digital economy. We believe that the digital economy can achieve social good, particularly in bringing about real financial inclusion for the 2.5 billion adults on the planet today without access to banks, credit cards or the mainstream financial system. In addition, a digital economy is attractive to tech-centric young people, and has particular appeal in light of the global movement to mobile technologies and mobile payment systems.

Nonetheless, the International Centre for Missing & Exploited Children is involved in this issue because there are risks. For the past year I have consulted with law enforcement and financial experts worldwide. While much of the evidence is still anecdotal, there is consensus that commercial child pornography, sexual exploitation, sex trafficking and other criminal enterprises are increasingly moving to a new unregulated, unbanked digital economy. Through voluntary industry coalitions and following the money through the trails and tunnels of the payments system, these enterprises had declined dramatically. Yet, we have concluded that "we didn't end it, we just moved it."

There are three primary reasons for this migration: (1) anonymity; (2) the emergence of new, digital economy that belongs to no nation and is overseen by no central bank; and (3) most countries have not yet begun to apply existing laws and regulations to virtual currencies at the exchange level; i.e., the point at which virtual currencies are traded for dollars, euros, pounds, yen, etc. A US Treasury Department official told us, "the more virtual currencies function like real currencies, the greater the illicit finance threat." Yet, few countries are addressing this emerging threat.

There are positive signs. In March the Financial Crime Enforcement Network, or FinCEN, in the US issued guidance on the legal status of Bitcoin, the best-known digital currency, under the money laundering laws. Bitcoin exchanges, which exchange Bitcoins for conventional currencies, and most Bitcoin miners are required to register as Money Services Businesses and comply with anti-money laundering regulations. FinCEN indicated that a "money transmitter" is anyone that (1) "accepts and transmits a convertible virtual currency" or (2) "buys or sells convertible virtual currency for any reason." However, Bitcoin users who merely use the currency to purchase goods and services are not required to register. We believe that this is not only a positive step for the issues we are concerned about, it is also a positive step for Bitcoin.

In July the Financial Action Task Force (FATF), the 36-member, inter-governmental body based in Paris, issued similar guidance. The FATF focuses on combating money laundering and the financing of terrorism.

We define key elements of the digital economy as including digital currencies; anonymous online payment systems; anonymous Internet tools; and bulletproof hosting. A primary area of focus is digital currencies, particularly those with bidirectional flow; i.e., digital currencies which are bought and sold at prevailing exchange rates and used to purchase both real and virtual goods and services. The best-known example is Bitcoin.

As a result of our consultations with law enforcement leaders worldwide, ICMEC, in partnership with Thomson Reuters, the global media and information company, set out to find a balanced, reasonable response to the problems associated with the misuse of digital currencies for child sexual exploitation and other criminal activity. In June ICMEC and Thomson Reuters convened a conference on this issue and also met with global financial leaders at the World Bank. As a result we created a Digital Economy Task Force, which includes the Bitcoin Foundation, the Tor Project, the Gates Foundation, the Brookings Institution, the Cato Institute, Vital Voices, law enforcement leaders and others. Our goal is to offer recommendations and real solutions for the threats and risks without jeopardizing the promise and potential of the digital economy.

You asked that I address several questions:

(1) The extent to which virtual currencies are being used directly in child-exploitive or related online criminal activities, or in support of such activities;

(2) The unique challenges that virtual currencies bring for law enforcement investigations and prosecutions; and

(3) The work of our Digital Economy Task Force and other collaborative efforts;

(4) Future trends and potential policy considerations for Congress and other policymakers.

1 – The use of virtual currencies in child-exploitive or related online criminal activities, or in support of such activities.

Great progress has been made in addressing the use of the mainstream payments system for commercial child sexual exploitation. Nonetheless, we are concerned about the apparent migration of commercial child sexual exploitation, including sex abuse images, child exploitation and sex trafficking, along with other criminal enterprises to a new unregulated digital economy, made up of digital currencies; anonymous online payment systems; anonymous internet tools; and file hosting companies.

While much of our evidence regarding the use of digital currencies in child exploitation is anecdotal, a leading law enforcement expert advised us that child pornography producers are using Tor hidden services for the creation and dissemination of child pornography and Bitcoin for payment. However, he cautioned that the market to buy/sell child pornography on Tor hidden services using Bitcoins is small in comparison to the market for drugs and other illegal goods. He called the use of Tor and digital currencies for child pornography "significant" because those involved are the actual producers of the content. Thus, these crimes tend to involve new victims whom law enforcement has not seen before, and creates the presumption that the abuse is likely to be on-going.

There is a twofold challenge for law enforcement: the anonymity provided by Tor and the complexities of Bitcoin. The attractiveness of Tor and Bitcoin for child pornography is based upon a perception of anonymity. Those who use Tor and Bitcoin sacrifice speed for anonymity. Thus, if the perception of anonymity diminishes, we believe the criminal use will diminish with it.

In August 2013 the Irish founder/owner/operator of Freedom Hosting, which the FBI called "the largest facilitator of child pornography on the planet," was arrested. Freedom Hosting maintained servers for a number of Tor-based, so-called "deep web" child pornography sites and others. The best –known child pornography sites included Lolita City, the Love Zone and PedoEmpire, all of which accept Bitcoins for payment.

To shut down Freedom Hosting, law enforcement exploited a "java script exploit," a vulnerability in the site, enabling law enforcement to penetrate Tor and expose the IP addresses of the users of Freedom Hosting. Interestingly, in 2011 the hacktivist group, Anonymous, hacked into Tor to shut down Lolita City. However, Lolita City has reemerged with an estimated 15,000 members and 1.5 million child pornography images.

The digital economy of today is centered on peer-to-peer networks. There is clear evidence of the movement of child pornography and other types of exploitation from Internet Service Providers and central servers to peer-to-peer networks. Law enforcement is having some success in identifying individual users through the use of specialized peer-to-peer investigative tools to penetrate p2p-based operations. Yet, the emergence of a p2p-based digital economy is posing enormous challenges.

Much of the current discussion about digital currencies centers on Bitcoin, which can be bought and sold at prevailing exchange rates and then used to purchase both real and virtual goods and services. It is different from other digital currencies which may be purchased at a specific exchange rate, but may not be exchanged back. Examples are Facebook credits, Amazon coins, or frequent flyer points.

Recently, a judge in Texas ruled that Bitcoin is a currency. He compared it to a precious metal. Today, there are Bitcoin exchanges, like Mt. Gox in Japan, where one can exchange Bitcoins for conventional currencies. All Bitcoin transactions are visible and transparent. The challenge for law enforcement is in going from those transactions to an actual person.

It is not my position that Bitcoin or the emergence of a digital economy is negative. Nonetheless, there are challenges.

2 – The unique challenges that virtual currencies bring for law enforcement investigation and prosecution.

The primary challenge facing law enforcement worldwide today is the growing anonymity surrounding internet transactions and the emergence of a so-called "deep web." In its April 24, 2012 Intelligence Estimate focusing on Bitcoin, ("Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity"), the FBI reported, "Bitcoin…provides a venue for individuals to generate, transfer, launder and steal illicit funds with some anonymity. Bitcoin offers many of the same challenges associated with other virtual currencies, such as WebMoney, and adds unique complexities for investigators because of its decentralized nature."

The FBI report adds, "Since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records – problems that might attract malicious actors to Bitcoin. Bitcoin might also logically attract money launderers and other criminals who avoid traditional financial systems by using the internet to conduct global money transfers."

All of this is exacerbated by the emergence of Tor, The Onion Router, created by the US government to enable political dissidents to use the internet anonymously, avoiding retaliation from repressive regimes. It is a noble, high-minded, laudable purpose, and it protects not only political dissidents, but also journalists in countries where the practice of journalism is dangerous, victims of domestic violence or stalking, and others.

However, there are unintended consequences. Political dissidents, journalists and stalking victims are not the only ones using Tor. A March 6, 2013 headline in Business Insider read, "There's A Secret Internet For Drug Dealers, Assassins and Pedophiles." We are particularly concerned about the emergence of an unregulated "deep web" utilizing anonymizing hidden services and digital currencies for payment.

The so-called "deep web" made possible by anonymizing tools includes sites like Silk Road, but it also includes sites for the purchase of weapons; counterfeit currencies; assassins; stolen credit cards, fake IDs, and fake passports; and of particular concern to ICMEC, sites like Hard Candy, Jailbait, Lolita City, PedoEmpire, Love Zone and others for child abuse images. All of those sites accept digital currencies for payment.

It is important to note that while the so-called "deep web" is most often associated with Tor, Tor is not the only network being used or being developed to guarantee anonymity and untraceable access. In fact, there are indications that efforts are accelerating globally to create even more anonymous, impenetrable technologies.

In addition to Tor, there are the other "darknets," the Invisible Internet Project (I2P) and Freenet, and alternative top-level domains which are also called "rogue TLDs." I2P was designed as an anonymous peer-to-peer distributed communications layer that can run any traditional internet service. It was an evolution of the Freenet network. I2P's exclusive goal is to enable users to host services without being traceable or identifiable.

From consulting with law enforcement worldwide, it is clear there is progress. The recent arrest of the founder of Silk Road, "the Amazon for Drugs," was an important step. Yet, barely one month later the site is back up and is operating again.

There have been other arrests. In February Australian police arrested a cocaine dealer operating on Silk Road and being paid in Bitcoins. In May Israeli police broke up a drug distribution ring operating in Bitcoins. There have been others.

However, what I hear most from law enforcement worldwide is frustration. The primary investigative technique being utilized by police today for addressing anonymous, "deep web," criminal enterprises is infiltration. However, infiltration is expensive, time-consuming and often ineffective.

While there are some arrests, they primarily involve less sophisticated users who make mistakes and leave a trail. Even the Silk Road arrest appears to be largely the result of a series of mistakes by the offender. That doesn't minimize its importance or denigrate the incredible work of law enforcement to make it happen. Law enforcement must be vigilant and positioned to take advantage of the mistakes. It simply illustrates how daunting the challenge is.

In 2013 researchers at the University of Massachusetts reported that "while Tor presents a challenge to investigators, in practice offenders use Tor inconsistently. Over 90% of regular Tor users send traffic from a non-Tor IP at least once after first using Tor." Thus, most cases are currently being made due to mistakes by the offender. Our concern is that most often we are apprehending the less sophisticated offenders, not the serious, sophisticated organized criminals who represent the greatest threat and do not make these kinds of mistakes.

The Tor Project is committed to help train law enforcement in Tor technology, and should be praised for its willingness to help. It has also committed to help law enforcement develop ways to use Tor as part of its investigative arsenal. Nonetheless, it is vital that new investigative tools be developed.

We are also exploring some new techniques. For example, a recent analysis experimented with "clustering" Bitcoin transactions. While it is not possible to go from a transparent Bitcoin transaction to an actual human being, this analysis conducted by Forbes Magazine demonstrated that it is possible to identify patterns in Bitcoin transactions and to move from those patterns to the identification of specific offenders. The Forbes example unmasked the identities behind Bitcoin transactions on Silk Road.

Similarly, the recent investigation that shut down Freedom Hosting appeared to use variations of "hacking" techniques similar to those used by Anonymous in its efforts that shut down the child pornography site, Lolita City. These techniques offer potential for study, but must be examined carefully to ensure that legal and ethical standards are met.

Another concern is that in addition to the major "deep web" marketplaces like Silk Road, there are other sites that allow anonymous trading. According to an analysis by Digital Economy Task Force member, Trend Micro, there are underground message boards where people post and read generic classifieds regarding almost any good or service. There are also privately maintained sites that offer specific types of goods and services. Some are pages with prices and contact information for anonymous orders and others provide a full order and payment management system. Goods and services being offered include drugs, guns, hired assassins, child pornography, and much more.

TrendMicro concluded that the so-called "deep web" in general and Tor in particular offer a secure platform for cybercriminals to support a vast amount of illegal activities – from anonymous marketplaces to secure means of communications to an untraceable and difficult to shutdown infrastructure to deploy malware and botnets. It adds, "it becomes more important…to be able to track and monitor activities that take place in darknets, focusing today on Tor networks but extending in the future to other technologies."

3 – The work of the Digital Economy Task Force –

On June 13, 2013 ICMEC and Thomson Reuters hosted a conference with leaders of the Bitcoin movement, the Tor Project, government and law enforcement experts, private sector leaders, and others. Speakers included the US State Department's Ambassador who heads the Trafficking in Persons Office, an executive from the World Bank, the US Justice Department's Chief of the Child Exploitation & Obscenity Section, the US Department of Homeland Security's head of its Blue Campaign on human trafficking, an official from the State Department's International Narcotics & Law Enforcement (INL) bureau, a Deputy Assistant Attorney General, and the Director of the US Financial Crimes Enforcement Network (FinCEN). The conference also included private sector leaders from Thomson Reuters, General Electric Co., TrendMicro and others.

The representatives of Bitcoin, Tor and other entities explained their systems and indicated a desire to work with ICMEC, Thomson Reuters and others to ensure that their services are not used for child exploitation, human trafficking and other criminal purposes. They argued that the new digital economy represents an historic opportunity to advance financial inclusion and that the use of their systems for child sexual exploitation harms their larger purpose. They committed to work with us to seek solutions.

On June 14, 2013 ICMEC and Thomson Reuters participated in a meeting at the World Bank with officials of the International Monetary Fund, the European Central Bank, the US Federal Reserve, the US Department of Treasury's Office on Terrorist Financing and Financial Crimes, and others. I presented our concerns that digital currencies and the digital economy were becoming safe havens for child pornography, sexual exploitation and sex trafficking, in addition to other criminal enterprises.

The European Central Bank cited four primary conclusions:

(1) that virtual currencies do not yet pose a risk to price stability nor jeopardize financial stability;

(2) that since they are not yet regulated and not closely supervised or overseen by any public authority, they pose a risk for users;

(3) that they fall within the realm of central banks' authority as a result of characteristics shared with payment systems; and

(4) that they represent "a challenge for authorities, as they might be used by criminals, fraudsters, and money launderers."

The ECB committed to monitor developments, set payments security requirements, keep legal frameworks updated and "facilitate a social dialogue."

The US Federal Reserve raised several questions:

(a) Is Bitcoin a more efficient currency for illegal activities than physical currency?

(b) How anonymous is it?

(c) How vulnerable is Bitcoin to theft and counterfeiting? Like cash, there is no recourse for a victim of theft. Is it easier to steal virtual currency or physical currency?

(d) How vulnerable are Bitcoin exchanges to cyber attacks? This introduces volatility to the value of the currency.

(e) Will other virtual currencies emerge to challenge Bitcoin?

(f) Will Bitcoin or another virtual currency become "widespread enough to have implications for central bank currency and monetary policy?"; and

(g) “Will bank-like institutions emerge to take deposits and make loans of virtual currencies?”

The Federal Reserve also committed to monitor the situation.

Thus, as a result of the June conference and subsequent meetings and consultations, in August ICMEC and Thomson Reuters created a Digital Economy Task Force to seek reasonable, constructive solutions, including best practices models to address the challenge of anonymity.

ICMEC also committed to launch a global advocacy effort to urge individual nations and international bodies to begin applying anti-money laundering rules and regulations at the exchange level; to engage international law enforcement partners in an effort to increase awareness of the risks of the digital economy and develop specialized investigative techniques for addressing these kinds of crimes; and initiate discussions with policy makers regarding the use of “money transmitter” laws, which are in place in almost every country but are currently not being used to address this growing problem.

The Digital Economy Task Force created five working groups: Defining the Problem; Regulation; Law Enforcement; Human Rights/Financial Inclusion; and Interagency Cooperation and Coordination. Each group is compiling specific recommendations, which will be reviewed by the full task force. The Task Force is committed to issuing its final report and findings by February 2014.

(4) Future trends and potential policy considerations for Congress and other policymakers.

The digital economy is an evolving field. The pace of innovation will quicken. There will be new technologies and new currencies. The intensity of the effort to achieve total internet anonymity will also increase, posing increasing challenges for law enforcement.

What can Congress do?

You can ensure that we apply and utilize existing law and regulation, and that we focus our regulatory attention at the point at which virtual currencies are being exchanged for conventional currencies.

You can help ensure global cooperation and coordination. Digital economy funds flow globally, network to network, not nation to nation. This is not a problem that the US government can solve alone. An excellent model is the recent US-led investigation that shut down Liberty Reserve, the Costa Rican company indicted for unlicensed money transmissions; i.e., laundering $6 billion in illicit funds, some of which came from the sale of child pornography. Seventeen nations participated in that investigation.

We are gratified by the work of US and international law enforcement in the fight against Internet-based child sexual exploitation. Entities like the Virtual Global Task Force, which brings together national law enforcement agencies in 12 nations including international bodies Interpol and Europol, and the Global Alliance Against Child Sexual Abuse Online, launched recently by the US and Europe which now has nearly 50 member countries, are great models for international cooperation. We need a quick, nimble response system. These are global crimes and require a global solution.

You can ensure that the response of government to this fragile, emerging area is not so draconian that the effect is simply to push these new enterprises outside the United States to countries where there is little or no regulation.

Finally, you can help us address the core challenge, internet anonymity. For all of its importance, we simply cannot create an environment in which child exploiters, traffickers, and other organized criminals can operate on the internet with a complete veil of anonymity and no risk of being identified unless they make a mistake.

In our consultations with law enforcement worldwide, we have heard the argument that there is a difference between privacy and anonymity. Law enforcement leaders embrace the broadest possible privacy protections for individuals, but emphasize that absolute internet anonymity is a prescription for catastrophe.

Our challenge is to find the right balance. Free speech is not absolute. Nearly a century ago, the US Supreme Court articulated the "clear and present danger" test, emphasizing that limits on speech may be appropriate based upon the context in which that speech is exercised.

That determination is much more difficult today in the world of the internet, a medium that is global in scope. We recognize that protecting the rights of political dissidents, journalists and others is incredibly important. We also recognize that all countries are not equally committed to individual freedoms, and that there are countries which will use internet speech as a basis for retaliation.

Nonetheless, the crux of the challenge we face with regard to the use of the digital economy for the exploitation and victimization of children and other criminal purposes is internet anonymity. There have to be some limits, hopefully as minimal as possible. Law enforcement has to have some possibility of tracing evidence of unlawful behavior, with full and appropriate legal processes, to the person responsible for it.

In her "Remarks on Internet Freedom" at the Newseum in Washington, DC in January 2010, former Secretary of State Hillary Clinton said, "On the one hand, anonymity protects the exploitation of children. And on the other hand, anonymity protects the free expression of opposition to repressive governments." That is our challenge.

Secretary Clinton added, "…we must grapple with the issue of anonymous speech. Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities. But these challenges must not become an excuse for governments to systematically violate the rights and privacy of those who use the internet for peaceful political purposes."

She added, "None of this will be easy…But I think these overriding principles should be our guiding light. We should err on the side of openness and do everything possible to create that, recognizing, as with any rule or any statement of principle, there are going to be exceptions."

She was exactly right. We must develop and implement those limited exceptions.