International Centre
FOR MISSING & EXPLOITED CHILDREN

THOMSON REUTERS

The Digital Economy: Potential, Perils, and Promises

A REPORT OF THE DIGITAL ECONOMY TASK FORCE

MARCH 2014

CO-CHAIRS
ERNIE ALLEN
International Centre for Missing & Exploited Children

STEVE RUBLEY
Thomson Reuters

VICE-CHAIR
JOHN VILLASENOR
The Brookings Institution/UCLA

TABLE OF CONTENTS

The Digital Economy: Potential, Perils, and Promises

A REPORT OF THE DIGITAL ECONOMY TASK FORCE

International Centre
FOR MISSING & EXPLOITED CHILDREN

THOMSON REUTERS

International Centre for Missing and Exploited Children
1700 Diagonal Road, Suite 625
Alexandria, Virginia 22314
+1 703.837.6313

Thomson Reuters
3 Times Square
New York, New York 10036
+1 646.223.4000

TASK FORCE ON THE DIGITAL ECONOMY

CO-CHAIRS

Ernie Allen
President and Chief Executive Officer,
International Centre for Missing & Exploited Children

Steve Rubley
Managing Director, Government Segment,
Thomson Reuters

VICE-CHAIR

John Villasenor
Nonresident Senior Fellow, The Brookings Institution
Professor of Electrical Engineering and Public Policy, UCLA

POLICY ADVISORY GROUP

Luis CdeBaca
Ambassador-at-Large, Office to Monitor and Combat Trafficking in Persons,
U.S. Department of State

The Honorable Paula J. Dobriansky
Senior Fellow, Harvard University Belfer Center for Science and International Affairs and former Under Secretary of State for Democracy and Global Affairs

Frances Fragos Townsend
Executive Vice President at MacAndrews and Forbes Holdings, LLC. and former Homeland and Counterterrorism Security Advisor, The White House

Juan Zarate
Senior Adviser,
Transnational Threats Project and Homeland Security and Counterterrorism Program

TASK FORCE MEMBERS

César Alonso-Iriarte
DG Home Affairs,
European Commission

Jerry Brito
Senior Research Fellow and Director of Technology Policy Program,
Mercatus Center at George Mason University

Don Codling
President,
CGI-LLC

Marina Colby
Senior Counter-Trafficking in Persons Fellow, Center for Excellence on Democracy, Human Rights and Governance,
United States Agency for International Development

Julie Cordua
Executive Director,
Thorn: Digital Defenders of Children

Cindy Dyer
Vice President, Human Rights,
Vital Voices

Kate Friedrich
Vice President, Government Affairs,
Thomson Reuters

Tom Kellermann, CISM
Managing Director for Cyber Protection,
Alvarez & Marsal

Scott McCleskey
Senior Advisor,
The Ethisphere Institute

Sheila Miller
Program Officer, Financial Services for the Poor
Global Policy & Advocacy,
Bill & Melinda Gates Foundation

Kelley Misata
Director of Outreach, Marketing & Communications,
The Tor Project, Inc.

Cody Monk
Special Agent,
Federal Bureau of Investigation

Patrick Murck
General Counsel,
Bitcoin Foundation

Neil J. O'Callaghan
Section Chief,
Homeland Security Investigations
Cyber Crimes Center, Child Exploitation
Investigations Unit

Xiomara Ramos-Bonakdar
AML Compliance Officer,
Citigroup

Ron Rowe
Assistant to the Special Agent in Charge,
United States Secret Service, Criminal
Investigative Division – Cyber Intelligence Section

Maria C. Stephens

Jason Thomas
Chief, Innovation and Strategy,
Thomson Reuters Special Services, LLC

Mark Witzal
Deputy Assistant Director for the Financial Narcotics
and Special Operations Division,
Homeland Security Investigations

Veronica Zeitlin
Human Trafficking and Gender Advisor,
United States Agency for International Development

ACKNOWLEDGEMENTS

Nancy Dube
Executive Vice President &
Chief Operating Officer,
International Centre for Missing & Exploited
Children

Judith Grabski
Project Manager, Digital Economy Task Force,
International Centre for Missing & Exploited
Children

Eliza Harrell
Marketing Manager,
International Centre for Missing & Exploited
Children

Sandra Marchenko
Director, Koons Family Institute on International
Law & Policy,
International Centre for Missing & Exploited
Children

Ellie Moseley
Senior Consultant, Strategy, Policy & Regulation
Deloitte

Katherine Sagona-Stophel
Government Analyst, Research,
Thomson Reuters Special Services, LLC

PREFACE

In 2013, the International Centre for Missing & Exploited Children (ICMEC) and Thomson Reuters joined forces to lead an effort focused on exploring the benefits and risks of the emerging digital economy.

In June 2013, we co-hosted a one-day conference to discuss these key issues, which for the first time convened thought leaders from academia, government, the financial and web services industries, as well as the nonprofit sector.

Our shared belief in the power of innovation brought these stakeholders together to address the economic opportunities that arise from the digital economy while confronting illicit activities from money laundering, to the illegal drug and weapons trade, to human sex trafficking, and more. This was the birth of the Digital Economy Task Force (DETF) and the ongoing discussion of several pressing topics.

The technological frontier of the digital economy presents countless opportunities and challenges for the public and private sectors, including for example, the potential to provide financial tools for more of the world's poor who are currently "unbanked." It is also evident that new forms of payment and trade continue to emerge – including digital currencies, prepaid cards, and alternative payment systems, among others – where anonymity reigns and their growth has been left largely unchecked.

While the growth of the digital economy can lead to many benefits, it also opens the door to those who seek new and profitable avenues to perpetrate illicit activities. The child pornography and sexual exploitation industries, in particular, are moving outside of traditional economic mechanisms and into the shadows of the digital world. It's on this central issue that the DETF has decided to focus their effort.

Among the conclusions of the conference: cross-sector communication and collaboration is vital to address a worldwide response to the growing digital economy. The DETF approached key stakeholders, ranging from web industry leaders to law enforcement officials and advocacy organizations, to assess the risks and advantages of the digital economy with the goal of offering informative and timely recommendations for those who seek to understand its impact on our world.

At the first meeting of the DETF, members agreed that use of digital economy tools and technologies for the victimization of children is morally abhorrent and of urgent importance. From this point, we set out to frame the policy discussion in a manner that enables the digital economy to grow while creating an inhospitable environment for those who seek to abuse it. We realize that piecemeal regulation can't tackle a global issue, but we believe these initial recommendations can lead to a broader exploration of these issues beyond this report.

Our hope is that the recommendations contained in this report can lead to a worldwide policy debate of the digital economy. We need to inform decision makers and digital pioneers in order to develop new methods and mechanisms for addressing these groundbreaking technologies. And we must create a coordinated and thoughtful approach in light of this global, technological revolution. Together we can ensure that the potential of the digital economy is not exploited by those who seek to use it for harm.

Our global community deserves no less.

Ernie Allen
President & CEO
International Centre for Missing
& Exploited Children

Steve Rubley
President & CEO
Thomson Reuters Special Services LLC

The International Centre for Missing & Exploited Children (ICMEC), together with Thomson Reuters, have assembled a task force of leading experts from academia, think tanks and the private sector, as well as government representatives, to discuss the impact of the digital economy on illicit activity, particularly the sexual exploitation of children. The views expressed in this Report do not necessarily reflect a consensus among the task force members, nor do they necessarily reflect the views of the public and private organizations for whom the various task force members work.

INTRODUCTION

While improving the quality of life for people around the world, advances in digital technology and the growth of the digital economy have also led to a rise in illicit activities including drug trafficking, money laundering, human trafficking, and sexual exploitation of children.

Technologies that facilitate online anonymity, such as bulletproof hosting, anonymizing networks, and anonymous payments systems, offer a particular challenge: balancing their use for positive social impact against their potential misuse by those who perpetrate illicit activities.

Confronting exploitation and other misuses of digital technology can be effective if it is precisely targeted and methodically carried out. At the same time, these behaviors should be addressed in a broader context that includes consideration of both the unlawful uses, as well as the many benefits of digital technology tools. Combating unlawful uses of online technology must also be balanced to protect the rights and privacy of law-abiding people, and to retain access to the many economic and social benefits afforded by their use.

What is Anonymity?

In today's digital age, many online technologies and tools exist to conceal one's identity, each used for different reasons ranging from protection to evasion. It is crucial to begin by distinguishing between identification, privacy, and anonymity in order to frame a discussion of such technologies and address their potential misuse by those who conduct unlawful activities.

Identification occurs when identifiers are collected that provide sufficient assurance of who a person or thing is. The identifiers that are "sufficient" for any given interaction, transaction, or relationship can vary widely depending on context. Many formal and interpersonal interactions are fully "identified;" meaning that the parties know who each other are. Because these interactions are more memorable and important, many people believe that full identification is the norm, but it may not be as strong as they believe. Human interactions with others are often weakly identified, such as recognition of a store clerk only by facial characteristics or gait. These are identifiers that cannot be reliably reproduced should it be necessary to locate that same person in a different setting. Many real-world transactions involve the sharing of few, if any, useful identifiers, thus they are effectively anonymous.

Withholding identifiers – that is, maintaining anonymity – is a common and important social practice. People use it to delimit social relationships, such as when a person declines to give a real name or phone number to a stranger who approaches them in public, or when a person provides a fake email address to a website to avoid receiving unwanted e-mails. Along with social and commercial freedom, anonymity is also well recognized as a tool of political freedom. In the United States, the Supreme Court recognized the relationship between anonymity and freedom of speech

and association in *NAACP v. Alabama*.[1] It held that the government could not acquire the membership list of a civil rights advocacy organization as it was likely to have a "…deterrent effect on the free enjoyment of the right to associate…" and it may cause members "…to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."[2] In 1995, in *McIntyre v. Ohio Elections Commission*, the Court again expressed support for the role of anonymity in freedom of speech, writing "[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority."[3]

Anonymity Online

Many of the same concepts regarding identification and anonymity apply to the online world as well, albeit magnified. It can be easier to track and monitor online activity because records are digital, and can thus be stored, recalled, and processed indefinitely. For good or bad, people can act anonymously, withholding their identifiers that could give others access to them, such as their real name, addresses, fixed email addresses, and fixed Internet Protocol (IP) addresses.

There also are a variety of techniques and services designed to preserve online anonymity for people who want it. These are useful for a wide variety of legitimate purposes from general privacy protection, to securing government communications, to protecting journalists and dissidents from oppressive governments. The Onion Router (Tor), based on onion routing technology[4], helps Internet users retain anonymity. It "was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications."[5] It helps mask the source and destination of Internet data by directing data packets through a series of "relays" in which "no individual relay ever knows the complete path that a data packet has taken."[6] While Tor technology does what it was designed to do, it also can be a tool to mask criminal activity, including crimes against children.

In August 2013, the Federal Bureau of Investigation (FBI) orchestrated the arrest of the alleged owner and operator of Freedom Hosting,[7] a service that provided web server space for Tor and other hidden services – essentially websites that use anonymizing technology to hide their IP addresses and thus the identity of their operators.[8] Among Freedom Hosting's customers were child pornography websites such as Lolita City, the Love Zone, and PedoEmpire.[9]

A few months earlier, in May 2013, the FBI also shut down Liberty Reserve, a digital currency and payments network that the government alleges was "designed to help criminals conduct illegal transactions and launder the proceeds of their crimes . . . by making financial activity on Liberty Reserve anonymous and untraceable."[10] According to the U.S. Government's allegations, Liberty Reserve "ha[d] become a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking."[11]

Simply identifying instances and possibilities of anonymity-facilitating technologies enabling crimes against children is insufficient. It is important to acknowledge that some of the same technologies that can be used to mask commercial sexual exploitation of children (e.g. encryption) have beneficial uses as well, and it would be unwise to overreact to the potential dangers of any technology before its possible benefits are widely recognized. Along with identifying modes of abuse, effort should be made to determine the prevalence of any type of exploitation facilitated by given technologies so that the greatest effort can be directed to the most serious facilitator of abuse. Then, responses must be balanced in light of the benefits technologies produce and the rights lawful technology users enjoy.

1 *NAACP v. Alabama,* 357 U.S. 449 (1958).
2 *Id.*
3 *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995).
4 B.V.V. Sri Raj Dutt et al., *Implementation of Onion Routing CS425: Computer Networks - Course Project Report*, Department of Computer Science and Engineering, http://www.cse.iitk.ac.in/users/mprateek/project/onion_routing/report/report.pdf (last visited Feb. 21, 2014).
5 *About Tor*, TorProject.org, https://www.torproject.org/about/overview.html.en.
6 *Id.*
7 Press Release. U.S. Dep't of Justice, Manhattan U.S. Attorney Announces Charges Against Three Individuals In Virginia, Ireland, And Australia For Their Roles In Running The "Silk Road" Website (Dec. 20, 2013), http://www.justice.gov/usao/nys/pressreleases/December13/JonesetalArrestsSilkRoad2PR.php.
8 Patrick Howell O'Neill, *An in-depth guide to Freedom Hosting, the engine of the Dark Net*, The Daily Dot (Aug. 4, 2013) http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/.
9 *Id.*
10 U.S. Dep't of Justice, Sealed Indictment at ¶ 8, United States v. Liberty Reserve S.A., 13 Cr. 368 (S.D.N.Y. 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf.
11 *Id.* at ¶ 9.

Privacy, Anonymity, and Striking the Right Balance

Any policy that addresses developing technology must confront the challenge of balancing its possible benefits with its potentially negative consequences. In the wake of recent revelations regarding broad-based monitoring of the Internet, this balance is increasingly difficult. There will likely be new restrictions on law enforcement that will push cybercriminals, including those who prey upon children, into the even-deeper web, including alternative darknets and private networks making law enforcement's job even more challenging.

Law enforcement leaders worldwide argue that policymakers must examine and discuss the difference between privacy and anonymity. In many countries, law enforcement leaders believe that citizens have a right to privacy, but they also believe that there are exceptions based upon a lawful reason to penetrate that right. Privacy is clearly a close cousin to anonymity. Yet one can be a robust believer in the importance of privacy rights while also understanding that anonymity is a double-edged sword. Anonymity can be misused to sell drugs online, plot a terrorist attack, launder money, or to produce and trade in child exploitation images.

In her "Remarks on Internet Freedom" at the Newseum in Washington, D.C. in January 2010, former U.S. 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."[12]

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."[13]

She continued,

> "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."[14]

This sentiment, to err on the side of openness while allowing limited exceptions, offers a valid guiding principle for any effort to combat child sexual exploitation online.

Digital Technologies and the Sexual Exploitation of Children

As demonstrated through some of the examples above, child sexual exploitation represents one of the ways in which these anonymity-facilitating technologies are grossly misused. The sexual exploitation of children is deeply repugnant in any context, and no less so when it is accomplished with the aid of digital technologies. In order to confront online sexual exploitation of children we believe there must be clear definitions to frame the issues.

At least one scholarly resource offers a set of highly relevant definitions. A study by Richard J. Estes and Neil Alan Weiner entitled, "The Commercial Sexual Exploitation of Children In the U. S., Canada and Mexico" defined the broad category of sexual exploitation of children as:

> "A practice by which a person, usually an adult, achieves sexual gratification, financial gain or advancement through the abuse or exploitation of a child's sexuality by abrogating that child's human right to dignity, equality, autonomy, and physical and mental well-being, i.e., trafficking, prostitution, prostitution tourism, mail-order-bride trade, pornography, stripping, battering, incest, rape and sexual harassment." [15]

12 Hillary Rodham Clinton, Sec'y of State, Remarks at the Newseum in Washington, DC: Remarks on Internet Freedom, (Jan. 21, 2010), *available at* http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html#axzz2sNutq0iw.

13 *Id.*

14 *Id.*

15 Richard J. Estes & Neil Alan Weiner, *The Commercial Sexual Exploitation of Children In the U. S., Canada and Mexico,* University of Pennsylvania School of Social Work 9 (Sept. 18, 2001) (revised Feb. 20, 2002), *available at* http://www.sp2.upenn.edu/restes/CSEC_Files/Complete_CSEC_020220.pdf; *see also* Donna M. Hughes, *Pimps and Predators on the Internet: Globalizing the Sexual Exploitation of Women and Children* (1999), *available at* http://www.uri.edu/artsci/wms/hughes/pprep.pdf.

Exploitation, they noted, "reflects a continuum of abuse ranging from child sexual abuse to child sexual exploitation to the commercial sexual exploitation of children."[16]

Drs. Estes and Weiner further defined commercial sexual exploitation of children as:

> "The sexual exploitation of children (SEC) entirely, or at least primarily, for financial or other economic reasons. The economic exchanges involved may be either monetary or non-monetary (i.e., for food, shelter, drugs) but, in every case, involves maximum benefits to the exploiter and an abrogation of the basic rights, dignity, autonomy, physical and mental well-being of the children involved."[17]

Unfortunately, criminals have demonstrated their ability to utilize and adapt emerging technologies to exploit children. One of the most notorious examples is Dreamboard, which Secretary of the U.S. Department of Homeland Security Janet Napolitano and U.S. Attorney General Eric Holder described as "a private, members-only, online bulletin board that was created and operated to promote pedophilia and encourage the sexual abuse of very young children, in an environment designed to avoid law enforcement detection."[18] Dreamboard was a barter-based site with new images serving as "payment" in exchange for access.[19] Aspiring members were required to post child pornography on the site in order to join, and to continue to post images to avoid having their access suspended.[20] Membership was hierarchical, with greater privileges provided to members who posted previously-unavailable content, including newly produced child pornography images.[21]

16 *See* Estes, *supra* note 15, at 10.
17 *Id.* (sometimes referred to using the acronym CSEC).
18 Press Release, U.S. Dep't of Homeland Security, *Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children* (Aug. 3, 2011), https://www.dhs.gov/news/2011/08/03/secretary-napolitano-and-attorney-general-holder-announce-largest-us-prosecution.
19 *Id.*
20 *Id.*
21 *Id.*

Incidence and Prevalence of Exploitation

The authors of the Estes-Weiner study gathered data from many sources about sexual exploitation of children, including U.S. Postal Inspection Service data on child pornography, information about child victimization in sexual crimes from the Crimes Against Children Unit of the FBI, data concerning the number of runaway and homeless youth from a variety of sources, and U.S. State Department research on domestic and international trafficking in children for sexual purposes.[22] "[E]ach organization possessed a piece of the puzzle that was needed to see the total picture," the authors reported, "but most of the pieces either were missing or buried deep in irretrievable case and administrative data sets."[23] Ultimately, they concluded, "Reliable estimates of the number of commercially sexually exploited children in the United States do *not* exist."[24]

Rigorous, continuously updated research into the incidence and prevalence of child sexual exploitation is essential if the concerns that these crimes raise are to be converted to productive action to protect children. The Estes-Weiner study, which was conducted in 2001 and limited to North America, has not to our knowledge been expanded upon or repeated. There are few reliable estimates of the number of sexually exploited children in the United States or anywhere in the world.

Estimates are hard to establish because acts, commercially or otherwise, are usually committed in private and often go unreported. In general, there are no national or local registries of cases of sexual exploitation of children, and in many instances the nature, extent, and severity of these crimes are ignored. The methodical efforts that have been used to study other areas, such as human slavery, could be used to grasp the scope of the sexual exploitation of children.[25]

Learning more about these crimes, including the conditions that foster them and the modes by which they are perpetrated, would permit responses to be appropriately adjusted for maximal effect. For example, how close is the correlation between poverty and the commercial sexual exploitation of children? How much more of this exploitation occurs in border communities or areas with high numbers of transient workers and travelers? What cultural factors, such as age-of-consent laws, gender equality norms, and other customs, correlate with incidence and/or reporting rates? What legal,

22 *See* Estes, *supra*, note 15.
23 *Id.* at 127.
24 *Id.* at 142 (emphasis in original).
25 *See, e.g.,* Walk Free Foundation, The Global Slavery Index 2013, App. 1 (2013), *available at* http://www.ungift.org/doc/knowledgehub/resource-centre/2013/GlobalSlaveryIndex_2013_Download_WEB1.pdf.

political, and societal factors make law enforcement in this domain robust or anemic? These crimes should be rigorously studied, and estimates of incidence and prevalence produced, so that efforts to combat them can be directed toward areas with the greatest need.

Modes of Abuse

The benefits of digital technologies and the digital economy they enable are manifold; they can improve news gathering and dissemination efforts, education, speech and political participation, as well as provide economic opportunities that positively impact community and individual development. However, they have also led to new forms of exploitation. For example, recent years have seen the growth of live-streamed, on-demand paid sex shows involving children, typically filmed using a webcam overseas. In 2011, a Pennsylvania man was charged with possession of child pornography after investigators from U.S. Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI) found evidence that he was "exploiting minors by viewing cyber sex shows that were broadcast via a webcam…" located in the Philippines.[26]

Children exploited in this manner are often located in impoverished communities outside of the United States, and forced into online pornography by criminal syndicates, locally powerful neighborhood residents, or even their own parents.[27] Payment is provided using a variety of mechanisms, including traditional money remitting services. It could be argued that in time, emerging digital payment systems, with their potential for anonymity, could become an attractive payment option in these situations, further complicating efforts to investigate and apprehend those responsible for exploiting young victims.

"Sextortion" cases are also on the rise, involving exploitation in which an attacker will threaten to make public compromising images of the victim unless they are supplied with more images, videos, or occasionally even payment.[28] In September 2013, a California man was arrested after he allegedly obtained nude and semi-nude images of victims (at least one of whom was under 18 years-old) by hacking into their computers and remotely turning on their built-in cameras.[29] He would then demand that the victim send him additional nude photos.[30]

Unfortunately, many criminals who engage in technologically facilitated exploitation of children are not caught. Dreamboard had approximately 600 members, only a subset of whom were arrested in Operation Delego.[31] Many Dreamboard users managed to escape prosecution by using anonymizing software and encryption to mask their identities.[32] Often, criminals are caught only when they make mistakes. Some users of Dreamboard, for example, would often attempt to anonymize their activity by using proxy servers to mask the real location of the computers they were using to access the Internet. But not all Dreamboard members used anonymizing tools every time they accessed the site. These lapses likely proved critical in enabling law enforcement to identify them.

In short, while anecdotal examples of online abuse, and subsequent arrest of perpetrators exist, the scope of the problem remains uncertain. Determining the magnitude and methods of child sexual exploitation perpetrated or facilitated by anonymity-facilitating technologies is essential to eradicating this type of victimization.

Recommendation:

Conduct rigorous, validated studies of the sexual exploitation of children, its incidence, and its prevalence, so that resources can be directed towards reducing the victimization of children as effectively as possible, with measurable results.

26 Press Release, U.S. Dep't of Homeland Security, Pennsylvania man indicted on child pornography charges (Sept. 12, 2011), http://www.ice.gov/news/releases/1109/110912pittsburgh.htm.

27 Child Exploitation and Online Protection Centre, *Threat Assessment of Child Sexual Abuse and Exploitation* 8 (June 2013), http://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf.

28 Erin McClam, *Experts increasingly worried about 'sextortion' of minors online,* NBC News (Jul. 21, 2013), http://www.cnbc.com/id/100889001.

29 Christopher Weber, *Miss Teen USA Extortion Plot Foiled, Suspect Arrested*, HUFFINGTON POST (Sept. 26, 2013), http://www.huffingtonpost.com/2013/09/26/miss-teen-usa-exortortion_n_3997828.html.

30 *Id.*

31 *"Living horror": Dozens charged in international child porn ring*, NBCNEWS.COM (Aug. 3, 2011), http://www.nbcnews.com/id/44002915/ns/us_news-crime_and_courts/t/living-horror-dozens-charged-international-child-porn-ring.

32 *Id.*

PREVENTING SEXUAL EXPLOITATION OF CHILDREN: A MULTI-FACETED APPROACH

In terms of the methods used, technology-facilitated commercial sexual exploitation of children has some commonalities with other criminal uses of the digital economy, including money laundering and terrorism financing. As a result, some aspects of the problem can and should be addressed in a broader context.

The remainder of this report will provide an overview and recommendations around three topic areas: law enforcement, regulation, and interagency coordination. Law enforcement has the extremely challenging job of identifying and locating perpetrators of crimes against children in an era when the perpetrators are armed with an increasingly sophisticated set of digital tools designed specifically to make them hard to locate and identify. To adapt, law enforcement agencies will need to alter their investigative methods, introduce new training programs, and conduct research to better understand the nature of criminal activities involving the "deep web."

In addition, regulatory agencies face a difficult task in adapting to the rise of the digital economy (including the growth of non-fiat currencies and the associated infrastructures designed to facilitate anonymous or pseudonymous storage and movement of money), and its relation to multiple forms of unlawful behavior, including commercial child sexual exploitation. The role of regulation, however, is not only to impede unlawful behavior, but also to provide consumer protection for lawful behavior and to foster economic growth. Thus, the portion of this report addressing regulation reflects a view that decisions about whether, when and how to regulate must be made with these multiple goals in mind.

Regulators in the United States offer a unique perspective regarding existing government frameworks around the digital economy. Inter-agency relationships have already been developed to confront money laundering and for the elimination of financing for terrorism, these are the most robust in place to date. However, interagency cooperation and regulation are challenged by ever changing technologies. Increased collaboration among multiple agencies is clearly needed. The effort to legislate the digital economy in the United States can lead to a more systematic global framework that maximizes the benefits of the digital economy while halting its use by criminals, particularly those who engage in the commercial sexual exploitation of children.

As a general principle, efforts to address unlawful uses of digital technologies need to be framed with a strong understanding of the precise problems being addressed. In particular, moving towards success in the fight against technology-facilitated commercial sexual exploitation of children will require demonstrating that the scale of the problem has been tangibly reduced. That is an enormous challenge, but one that the recommendations provided in this report can help make achievable.

LAW ENFORCEMENT

Collaboration and partnership between law enforcement and financial services providers have inspired progress in mitigating the use of credit cards and other mainstream payment systems for commercial child sexual exploitation.[33] As illustrated earlier, there is an apparent migration of commercial child sexual exploitation, along with other criminal enterprises, from the traditional payments system to a new, largely unregulated digital economy made up of file hosting services, anonymizing Internet tools, and pseudonymous online payment systems.

While much of the evidence to date remains anecdotal, a high-ranking official from a U.S. federal law enforcement agency stated that child pornography producers are using anonymizing Internet tools for the creation and dissemination of child pornography and digital currencies as a medium of exchange for payment. However, the official cautioned that the market to buy and/or sell child pornography on anonymous hidden services using digital currencies is small in comparison to the market for drugs and other illegal goods. But regardless of their comparative size, arguably child sexual exploitation using these same tools is far more egregious because of the lasting impact of this victimization on the child.

Challenges for Law Enforcement

The digital economy poses unique challenges for law enforcement. These vary based upon the particular digital economy components used, which range from centralized digital currencies and money transfer systems, like Webmoney, Perfect Money and Liberty Reserve, to decentralized currencies like Bitcoin, to hybrid products combining characteristics of each of these systems. The commonality across all of these is the growing anonymity surrounding Internet transactions and the emergence of a so-called "deep web."

There has been particular attention directed to the emergence of Bitcoin, which is both a protocol for private, decentralized transactions and an associated digital currency.[34] In its April 24, 2012 *Intelligence Assessment* focusing on Bitcoin, the FBI reported the following:

> "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,

33 Int'l Ctr. for Missing & Exploited Children, *Financial Coalition Against Child Pornography Backgrounder*, http://www.icmec.org/en_X1/pdf/FCACPBackgrounder1-13.pdf (last visited Feb. 11, 2014).

34 *See Bitcoin: Protect Your Privacy*, Bitcoin.Org, https://bitcoin.org/en/protect-your-privacy (last visited Feb. 13, 2014). (To the extent that bitcoin public keys are not publicly associated with a particular person, transactions can be private. However, that privacy can be lost if a link is established between a public key and its owner.)

> and adds unique complexities for investigators because of its decentralized nature."[35]

The FBI report added,

> "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."[36]

The emergence of Internet anonymizing tools can offer additional venues for these "malicious actors," though they may have originally been created for social good. They can protect political dissidents, victims of domestic violence or stalking, and journalists in countries where free speech is limited. However, as with any technology there are unintended consequences.

A March 6, 2013 headline in Business Insider read, "*There's A Secret Internet For Drug Dealers, Assassins and Pedophiles*." [37] The article that followed outlined the emergence of an unregulated "deep web" utilizing anonymizing hidden services and digital currencies for payment.[38]

The "deep web" made possible by anonymizing tools includes sites like Silk Road, once alleged to be the so-called "eBay for drugs,"[39] but it also includes sites that appear to offer the purchase of weapons, counterfeit currencies, murder-for-hire contracts, stolen credit cards, fake IDs, and falsified passports. The "deep web" is also a sanctuary for operators of child pornography sites like Hard Candy, Jailbait, Lolita City, PedoEmpire, Love Zone, and others for child abuse images.[40]

While the "deep web" is most often associated with Tor in the media, there are other anonymizing networks in development or that are already being utilized to provide anonymity and untraceable access. Other anonymizing networks include the Invisible Internet Project (I2P), Freenet, and alternative top-level domains. I2P was designed as an anonymous peer-to-peer distributed communications layer that can run any traditional Internet service.[41] It was an evolution of the Freenet network.[42] I2P's exclusive goal is to enable users to host services without being traceable or identifiable.[43] In addition, there are continuing efforts to create more anonymous and impenetrable technologies.[44] These efforts are on a global scale and will expand the availability of choices for illicit actors seeking to thwart law enforcement investigative tools and techniques.

Law Enforcement Lacks Specialized Investigative Tools

Faced with this complex and rapidly evolving landscape, law enforcement worldwide frequently express frustration. The primary investigative technique being used by police today for addressing anonymous "deep web" criminal enterprises is often infiltration. However, infiltration can be expensive, time-consuming and often ineffective, so alternative tools are needed.

In 2013, University of Massachusetts researchers reported that "…while Tor presents a challenge to investigators, in practice, offenders use Tor inconsistently…" and "[o]ver 90% of regular Tor users send traffic from a non-Tor IP at least once after first using Tor."[45] Thus, most prosecutions result from mistakes by the offender. Unfortunately in some cases, law enforcement is only locating and apprehending the less-sophisticated offenders, not the high-level, technically skilled criminals operating these enterprises who are far less likely to make mistakes made that would expose their identity.

35 FBI Directorate of Intelligence, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*, Federal Bureau of Investigation Intelligence Assessment (Apr. 24, 2012), http://www.frank-cs.org/cms/pdfs/DOJ/DOJ_FBI_Bitcoin_24.4.12.pdf.

36 *Id.*

37 Dylan Love, *There's A Secret Internet For Drug Dealers, Assassins, And Pedophiles*, BusinessInsider.com (Mar. 6, 2013, 7:00 AM), http://www.businessinsider.com/tor-silk-road-deep-web-2013-3.

38 *Id.*

39 Meghan Ralston, *The End of the Silk Road: Will Shutting Down the 'eBay for Drugs' Cause More Harm Than Good?*, Huffington Post (Oct. 3, 2013, 3:03 PM), http://www.huffingtonpost.com/meghan-ralston/silk-road-shut-down_b_4038280.html; *see also* Monica J. Barratt, *Silk Road – eBay for Drugs*,107 Addiction 683 (2012).

40 *See* O'Neill, *supra* note 8.

41 Vincenzo Ciancaglini, et al., *Deepweb and Cybercrime: It's Not All About TOR* 6, Trend Micro, *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf; *see also* Lucian Constantin, *Financial malware program appears to communicate with attackers over the darknet*, pcworld.com (Nov. 21, 2013, 10:10 AM), http://www.pcworld.com/article/2066040/cybercrime-forum-advertises-financial-malware-that-uses-stealthy-i2p-communications.html.

42 *See* Ciancaglini, *supra* note 41.

43 *Id.*

44 Andrew Seymour, *Anonymous 'deep web' is new frontier of child exploitation, conference told,* OttawaCitizen.Com (Nov. 16, 2013), http://www.ottawacitizen.com/business/Anonymous+deep+frontier+child+exploitation+conference+told/9175718/story.html.

45 Ryan Hurley et al., *Measurement and Analysis of Child Pornography Trafficking on P2P Networks* 1 (2012), *available at* https://web.cs.umass.edu/publication/docs/2012/UM-CS-2012-016.pdf.

Despite these challenges, law enforcement has had some notable successes in apprehending operators of online illicit marketplaces who have used anonymizing tools to conceal their true identities. In August 2013, Eric Eoin Marques, the alleged founder of Freedom Hosting, an Ireland-based hosting service operating from servers in France, was arrested.[46] The FBI called Freedom Hosting, "the largest facilitator of child pornography on the planet."[47] Among other things, Freedom Hosting allegedly maintained servers for "deep web" child pornography sites including Lolita City, the Love Zone, and PedoEmpire. According to sources familiar with the case, investigators used innovative cyber techniques to enter Freedom Hosting and expose the Internet Protocol address of its users, thus allowing law enforcement to apprehend a large number of users.[48]

Published reports indicate that ideologically motivated cyber hackers, also known as hacktivists, have also been able to confront illicit "deep web" networks. In 2011, the hacktivist group Anonymous shut down Lolita City.[49] However, it has been estimated that Lolita City is back online with 15,000 members and 1.3 million child pornography images available.[50]

In another recent case, Ross William Ulbricht, the founder and alleged mastermind of Silk Road, who was commonly referred to as the "Dread Pirate Roberts" in online circles, was arrested in October 2013.[51] Law enforcement investigations by foreign authorities had developed information that Silk Road allegedly was the online market place for all things illicit.[52] In February 2013, Australian police arrested a cocaine dealer operating on Silk Road who was being paid in Bitcoin.[53] In May 2013, Israeli police broke up a drug distribution ring believed to be operating in Bitcoins.[54]

The Silk Road arrest was an important step. Yet, replacement sites were up and running soon after the arrest.[55] This illustrates how daunting the challenge is for law enforcement to disrupt these networks.

To help address this challenge, law enforcement can increase its knowledge about Tor and other anonymizing tools and about new payment systems that can be used to obscure the identity of both the transactor and transaction. This training is vital to the future development of investigative tools. Coordination and collaboration between law enforcement and experts from private sector and academia can further their investigative capabilities.

For example, an interesting experiment was described in September 2013 by *Forbes* magazine.[56] With the aid of Sarah Meiklejohn, a researcher at the University of California, San Diego, who studies Bitcoin transactions, *Forbes* staff explored the technique of "clustering" Bitcoin transactions in order to identify patterns of behavior.[57] Ms. Meiklejohn's work has demonstrated that even though the Bitcoin protocals do not enable law enforcement directly connect a transaction to an actual human being, there may be ways to identify users through examining the patterns of their transactions. As *Forbes* writer Andy Greenberg explained, Ms. Meiklejohn was asked to attempt to trace *Forbes*' transactions and "[w]ith just that list of my public addresses, she was able to identify every transaction we had made, including deposits to the Silk Road [and] to competitor sites Atlantis and Black Market Reloaded…."[58]

46 Paul Peachy, *Eric Eoin Marques: 28-year-old architect's son from Dublin accused of being world's biggest dealer in child abuse images,* Independent.co.uk (Aug. 23, 2013), http://www.independent.co.uk/news/world/europe/eric-eoin-marques-28yearold-architects-son-from-dublin-accused-of-being-worlds-biggest-dealer-in-child-abuse-images-8782756.html.

47 *See* O'Neill, *supra* note 8.

48 *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,* Wired.Com (Sept. 13, 2013), http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/.

49 Christopher Williams, *Anonymous hacktivists target child abuse websites*, The Telegraph (Oct. 24, 2011), http://www.telegraph.co.uk/technology/news/8846577/Anonymous-hacktivists-target-child-abuse-websites.html.

50 Patrick Howell O'Neill, *The year the Deep Web went mainstream*, The daily dot (Jan. 1, 2014), http://www.dailydot.com/crime/deep-web-2013-dread-pirate-roberts-backopy-sheep-marketplace/.

51 Alex Konrad, *Feds Say They've Arrested "Dread Pirate Roberts," Shut Down His Black Market "The Silk Road"*, Forbes.com (Oct. 2, 2013), http://www.forbes.com/sites/alexkonrad/2013/10/02/feds-shut-down-silk-road-owner-known-as-dread-pirate-roberts-arrested/.

52 *Id.*

53 Olivia Solon, *Police crack down on Silk Road following first drug dealer conviction*, Wired.Co.Uk (Feb. 1, 2013), http://www.wired.co.uk/news/archive/2013-02/01/silk-road-crackdown.

54 Ben Hartman, *30 arrested in raid on online drug distribution ring*, The Jerusalem Post (May 8, 2013), http://www.jpost.com/National-News/30-arrested-in-raid-on-online-drug-distribution-ring-312441.

55 John Biggs, *Silk Road Rises Again*, Techcrunch.com (Nov. 6, 2013), http://techcrunch.com/2013/11/06/silk-road-2-0-rises-again/.

56 Andy Greenberg, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, forbes.com (Sept. 5, 2013), http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/.

57 *Id.*

58 *Id.*

While recent successes in investigating criminal behavior "deep web" networks may be a positive sign, the ever-shifting technological landscape and sophistication of criminal enterprises only serves to complicate matters.

For instance, the rise of sites that allow anonymous trading of items is a new concern. According to Trend Micro, underground message boards have emerged where users post generic classified advertisements regarding illicit goods or services.[59] There are also privately maintained sites that offer specific types of goods and services.[60] Some are pages which offer prices and contact information for anonymous and others provide a full order and payment management system.

Trend Micro concluded that the so-called "deep web" provides

> "a secure platform for cybercriminals to support a vast number of illegal activities – from anonymous marketplaces to secure means of communications to an untraceable and difficult to shutdown infrastructure to deploy malware and botnets."[61]

It adds that it is more important "…to be able to track and monitor the activities that take place in darknets, focusing today on TOR networks but possibly extending in the future to other technologies…."[62]

Trend Micro also reported that goods and services are being sold in Russian language underground forums that do not use Tor.[63] It is likely that users of these forums have confidence in these sites based on the exclusive use of Russian language combined with requirements that membership is limited to trusted individuals with bona fides and an established reputation within the Russian hacker community. An analysis of these transactions found that underground forums offer a larger range of digital goods and transactions (credit card numbers, PayPal accounts, malware, etc.).[64] There are also many "potential users since access does not require the use of additional darknet software…."[65] In addition, "[t]he increased anonymity afforded by the TOR network, while useful for sellers to avoid getting caught, is somewhat detrimental because it prevents an actor of a commercial transaction to build and maintain a reputation over time."[66]

Nonetheless, Trend Micro observed that the peer-to-peer-based "deep web" "offers 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."[67] Trend Micro added, "it becomes more and more important…to be able to track and monitor activities that take place in darknets, focusing today on Tor networks but possibly extending in the future to other technologies (i.e., I2P, above all)."[68]

Enforcement under Existing Regulatory Frameworks

It is important to note, that there are some existing statutes and legal authority in the U.S. and other countries that can and should be used to address abuses associated with the digital economy.

As discussed in more detail in the "Regulation" section of this report, in March 2013, Financial Crimes Enformcement Network (FinCEN) issued guidance applying anti-money laundering, combating the financing of terrorism (AML/CFT) rules to digital economy exchanges.[69] In addition, similar guidance has been issued by the Financial Action Task Force (FATF), based in Paris.[70] A key point at which intervention is required is at the exchange level where users trade their non-fiat currencies for dollars, euros, pounds, yen or other fiat currencies. The U.S. Treasury Department has stated that the exchange of what it calls "virtual currencies" for fiat currencies opens the door to regulation through current laws for "money service businesses" (MSBs).[71]

59 *See* Ciancaglini, *supra* note 41, at 14; *see also,* Max Goncharov, *Russian Underground 101*, Trend Micro, *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.
60 *See* Ciancaglini, *supra* note 41.
61 *Id.* at 18.
62 *Id.*
63 *Id.*at 17.
64 *Id.*
65 *Id.*
66 *See* Ciancaglini, *supra* note 41.
67 *Id.*
68 *Id.*
69 Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 2013), http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html; *see also* Timothy B. Lee, *New Money Laundering Guidelines Are A Positive Sign for Bitcoin*, Forbes.com (Mar. 19, 2013), http://www.forbes.com/sites/timothylee/2013/03/19/new-money-laundering-guidelines-are-a-positive-sign-for-bitcoin/.
70 Financial Action Task Force, Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services (June 2013), http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.
71 Thomas Brown & Angela Markle, *FinCen Virtual Currencies Guidance Already Shaking Up Online Currency Exchanges*, Paul Hastings (Jun. 13, 2013), http://www.paulhastings.com/publications-items/oldblog/oldpost/caveat-vendor/2013/06/13/fincen-virtual-currencies.

Another challenge in the United States is that current U.S. regulation of money transmitters is also addressed at the state level and is not uniform in terms of both its development and implementation. For example, some states such as New York and California have robust money transmitter regulation and oversight capacity relative to other states.[72] A consistent and comprehensive regulatory and enforcement frameworks both within the United States and globally is recommended. To help achieve that goal, it is important to increase the commitment to training and education on the digital economy for law enforcement and for regulatory authorities worldwide.

Additional regulatory tools will be explored further later in this report, but one particularly useful example of their enforcement can be found in the money laundering investigation and May 2013 indictment of Costa Rica-based Liberty Reserve which allegedly laundered $6 billion in illicit funds was based on a money laundering investigation. [73] This investigation necessitated the cooperation and involvement of law enforcement from 17 countries.[74] Future investigations may require the participation of far more countries.

Today, new entities and alliances are being formed to address these issues in a more collaborative way. For example, the Virtual Global Task Force (VGT) is an alliance of law enforcement agencies that have come together to attack online child sexual abuse as a global crime.[75] Members include national law enforcement in Australia, Canada, Indonesia, Italy, Korea, The Netherlands, New Zealand, the United Arab Emirates, the United Kingdom, the United States, with additional cooperation from Europol and INTERPOL.

In addition, the United States and the European Union recently launched the Global Alliance Against Child Sexual Abuse Online, which now includes more than 50 member countries.[76] The Global Alliance seeks to enhance efforts to identify victims, investigate cases and prosecute offenders; increase awareness; and reduce the availability of child sexual abuse images online. Cooperative efforts such as these and others worldwide should be promoted and expanded in order to effectively address the global nature of these crimes.

72 *See, e.g., Money Transmitter Division*, CA.GOV (2014), http://www.dbo.ca.gov/Licensees/money_transmitters/.
73 *See* Sealed Indictment, *supra* note 10.
74 *Id.*
75 *Who We Are*, VIRTUAL GLOBAL TASKFORCE (2011), http://www.virtualglobaltaskforce.com/.
76 *A Global Alliance against Child Sexual Abuse Online*, EUROPEAN COMMISSION (last updated Nov. 12, 2013), http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm.

Recommendations:

1. Research should be conducted on the following:
   a. Determine if there are methods accessible to law enforcement, including "clustering," that could be used based on probable cause and appropriate legal process to overcome criminal misuse of anonymizing tools.
   b. Identify lessons learned from recent network exploitations of anonymizing tools to develop more effective and lawful investigative tools and models.
   c. Assess current money transmitter laws and how they apply to child sexual exploitation investigations.
2. Develop enhanced law enforcement investigative protocols, techniques and methods, based upon these research results with a focus on cross-sector partnerships and collaboration. Draft model law and procedures regarding uniform cyber investigative techniques for law enforcement as an implementation guide for parliaments and legislative bodies worldwide.
3. Promote and facilitate international law enforcement coordination, information sharing, and cooperation to address problems associated with the digital economy, and ensure that entities like the Virtual Global Task Force and the Global Alliance Against Child Sexual Abuse Online are utilized to ensure broader global law enforcement cooperation in investigating these crimes.
4. Policymakers should become familiar with AML/CFT rules and principles and encourage their application to digital economy money services businesses globally.
5. Reasonable regulatory definitions and limits should be developed to ensure that Internet anonymity does not become a safe harbor for criminal activity, including greater awareness amongst the global law enforcement community to proactively respond to the rise of anonymizing tools in child sexual exploitation.

REGULATION

There has been considerable debate on the merits of regulatory oversight tied to the digital economy. This discussion has taken place among policymakers, academics, and the media. It has been driven in part by the use of non-fiat digital currencies (most notably, Bitcoin) and the exploitation of their infrastructures in furtherance of criminal activity, as well as by the very large swings in the value of some digital currencies. While some of these factors imply, at least on the surface, that a degree of regulation is appropriate, the unique characteristics of digital currencies (and new payment systems more generally) may make some traditional approaches to regulation unnecessary, difficult to apply, or ineffective in their application. Moreover, many critical components of a digital currency system, such as servers, exchangers, and administrators, are more likely to be spread across numerous jurisdictions, including some with less oversight of financial crime and consumer protection.

In considering whether and how to regulate aspects of the digital economy, it is recognized that historically there are multiple philosophies regarding the role of regulation overall. It is not the intention of this report to resolve – or even engage in a debate regarding – these competing viewpoints. However, it is generally agreed that an objective analysis should be performed to determine whether regulation is appropriate, and, if so, what regulatory alternative is best. A risk-based approach is important in this regard, so that specific risks are identified and solutions proposed, weighing their costs against the benefits to be derived from them.

Presidents of both parties since Richard Nixon have sought to ensure that the benefits of regulation outweigh its costs, and that government engages in regulation only when systemic failures, such as market failures, are present.[77] This approach is embodied in President Clinton's Executive Order 12866,[78] and implemented via the Office of Management and Budget Circular A-4.[79] First, an analysis should be performed to determine whether there exists a market failure or other systemic problem that may warrant regulation.[80] Second, alternative approaches to address these problems should be identified.[81] Third, the approaches should be assessed on the basis of a cost-benefit analysis, with the alternative showing the best net benefits selected the presumed regulatory choice.[82] This analysis should reflect the most detailed economic, scientific, and technical analysis possible, as well as a thorough evaluation of the impact on all parties involved.

77 Susan E. Dudley & Jerry Brito, Regulation: A Primer, (2nd ed. 2012), *available at* http://mercatus.org/sites/default/files/RegulatoryPrimer_DudleyBrito_0.pdf.

78 Regulatory Planning and Review, 58 Fed. Reg. 190 (Oct. 4, 1993), *available at* http://www.archives.gov/federal-register/executive-orders/pdf/12866.pdf.

79 Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular No. A-4, Regulatory Analysis (Sept. 17, 2003), http://www.whitehouse.gov/omb/circulars_a004_a-4.

80 *See* Dudley, *supra* note 77.

81 *Id.*

82 *Id.*

Each stage of this analysis requires considerable research, whether along the path recommended above or some variation of it. There remain divergent views within this task force as to whether evidence of systemic failures is needed before regulation should be considered, or whether ex-ante regulation is appropriate to address specific vulnerabilities before they result in harm. There is general consensus within the group however, that any regulation should be well justified, effective and, to the extent possible, seek to identify and address unintended consequences.

With respect to child exploitation, for example, the extent to which digital currencies like Bitcoin might be misused to further exploitation of children remains undetermined. Even if such uses of bitcoin networks are demonstrated, it is still debated whether a regulatory framework is even necessary, and if so, whether current regulatory frameworks suffice.

Regulation and The Digital Currency Ecosystem

Businesses engaged in currency exchange or currency dealing are generally considered to be MSBs, raising the question as to whether the definition should be extended to include exchange between digital currencies and government-issued ones. The determination has profound implications for affected businesses since MSBs must comply with the provisions of the Bank Secrecy Act (BSA) to combat money laundering, terrorist financing and other forms of financial crime.

Recognizing that financial protections must keep pace with the emergence of new payment systems, in July 2011, FinCEN amended the Money Services Businesses (MSBs) rule[83] to provide the flexibility needed to accommodate payments innovations under the existing BSA regulatory framework. The amended MSB rule added the phrase, "other value that substitutes for currency" to the definition of "money transmission services," enabling the United States to regulate convertible "virtual" currency (the term used by FinCEN for non-fiat digital currencies) exchangers and administrators as money transmitters, subject to AML/CFT registration, recordkeeping, and reporting requirements.[84] In March 2013, FinCEN issued guidance clarifying the application of MSB regulations to virtual currencies.[85] The guidance explains "[a] person must exchange the currency of two or more countries to be considered a dealer in foreign exchange. Virtual currency does not meet the criteria to be considered "currency" under the BSA, because it is not legal tender."[86] The guidance also distinguished virtual currency participants from "Prepaid Access" participants, which many businesses and legal authorities believed to be the controlling framework for virtual currency exchangers.

The guidance distinguishes between three types of participants in "virtual" currency transactions: users, exchangers, and administrators The guidance explains that under the revised MSB rule, exchangers and administrators of convertible virtual currency are regulated as money transmitters. The regulation covers both centralized and decentralized convertible virtual currencies. By contrast, the guidance explains that a "user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not an MSB under FinCEN's regulations.[87] Such activity, in and of itself, does not fit within the definition of 'money transmission services' and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs."[88]

All MSBs have certain know-your-customer and transaction monitoring obligations, which can vary based on the classification of the MSB. MSBs that are classified as money transmitters must identify every customer that uses their service and keep records of all transactions. Additionally, "[g]enerally, a money services business must file a Suspicious Activity Report (SAR) for each transaction involving $2,000 or more where the money service business knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part): (1) involves funds derived from illegal activity; (2) is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any federal law or regulation (including any transaction reporting requirements); or (3) serves no business or apparent lawful purpose, and the reporting business knows of no reasonable explanation for the transaction after examining all available facts."[89]

83 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2014) (the Money Services Businesses [MSB] rule) (emphasis added).

84 U.S. Dep't of Treasury Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FINCEN.GOV (Jan. 30, 2014), http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf.

85 *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, *supra* note 69 (as of December 2013, approximately 40 virtual currency exchangers obligated to register with FinCEN have done so).

86 *Id.*

87 See FINANCIAL CRIMES ENFORCEMENT NETWORK, *supra* note 69.

88 *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, *supra* note 69 (internal citations omitted). (Users do not fit the money transmitter definition because they are not engaged in the business of providing money transmission services or transferring funds, as required by the general definition of an MSB.); *see also* 31 C.F.R. § 1010.100(ff) (2014).

89 Ryan J. Straus, *The FinCEN Virtual Currency Guidance: Neutering Bitcoin?*, E-Finance & Payments Law & Policy (April 2013), *available at* http://www.riddellwilliams.com/uploads/pdf/articles/article20130415-fincen-efplp.pdf; see also 31 C.F.R. § 103.20(a)(2) (2014).

By issuing guidance on how it believes existing regulations apply FinCEN has provided much needed clarity for this emerging industry. However, at the state level, regulators have not yet provided clarity and guidance about how their rules apply. Given the geographically dispersed nature of most digital currency transactions, the potential for mutually incompatible state-level guidance is a cause of concern for users of digital currencies, companies engaged in digital currency transactions, and regulators.

Invariably, the application of rules written for more conventional products and services, will often require amendment and interpretation when applied to transactions which are inherently global in scope and often decentralized in nature. Creating uniform and clear rules for digital currency exchanges is vital to managing risks posed by the digital economy and harnessing the many beneficial uses and outcomes.

Beyond these specific issues, there remain more fundamental questions as policymakers consider whether and how to regulate various aspects of the digital economy. The first broad question to be addressed is whether regulation is desired at all and, if so, to what extent. This will likely vary from issue to issue, but choices include simple disclosure of risks to consumers and potential consumers; the extension of existing regulatory regimes to cover the digital economy; and the creation of new rules and regulations specifically tailored to digital transactions.

To the extent that regulation may be necessary, the question will then become whether regulation should be constructed from the ground up or by extending existing rules to the digital economy or some combination thereof. As noted above, the application of rules written for more conventional products and services will often require amendment and interpretation, but this is part of the core work of regulatory agencies. This approach should not be avoided simply on the basis of the burden of interpretation.

Second, it should be considered whether some level of self-regulation would be appropriate for the digital economy. A detailed discussion of self-regulatory approaches is beyond the scope of this report, but there are several advantages to this method (which is used in a number of industries including securities, commodities, the law, and medicine). One is that self-regulatory organizations have at their disposal the expertise of their membership, making them less prone to regulatory lag or to a poor understanding of the regulated industry. They can be partially or completely self-funded through fees and disciplinary fines, among other sources, so that the broad taxpayer base is not responsible for funding the oversight of an industry used by only a few. Self-regulation frameworks may include the development and enforcement of rules as well as a code of conduct, and standard setting (for instance, minimum security standards). If membership is required in order to participate in an industry, self-regulatory organizations also can act as the watchdog to bar from the industry those who engage in egregious violations.

Finally, the level of jurisdiction of a regulatory regime needs to be considered. As it stands, many of the issues discussed in this report are treated at the state or federal level or both. This arrangement is best left in place absent an overriding argument in favor of placing all regulation at one level or another. But the larger issue is to what extent regulation of the digital economy can be effective at all, given that the digital economy is inherently international and highly mobile as firms can easily close their doors and re-open in another unregulated country. In the end, solutions must involve international coordination both in terms of developing comparable regulation and enforcement, though this may take years to achieve. For this reason alone, it may be more prudent to address these issues first within the United States and establish best practices that can be adopted by other countries and lead to a global response framework.

Recommendations:

1. Regulation in this sphere should be done through a risk-based approach, identifying and addressing the unique and similar potential risks – including commercial sexual exploitation of children, money laundering, terrorist financing, fraud, consumer protection and other areas of illicit finance and these must be weighed against the potential benefits of the digital economy. As with other regulations, a cost-benefit analysis should be conducted.

2. A specialized group should be formed with a mandate to research the following topics, among others:
   a. The process flows and critical control points in digital transactions. With regard to digital currency transactions, this should distinguish between centralized and decentralized currencies.

   b. Whether and where there is a need for regulation among aspects of the digital economy.

   c. Where regulation is deemed appropriate and whether existing rules and regulations may be applied effectively.

   d. If and where a need for regulation is found but there are no existing regulations, other regulatory remedies should be considered (subject to cost benefit analysis).

   e. The appropriate division of authority between state and federal regulatory agencies.

   This group should include representatives from across the digital economy and other affected industries; regulatory authorities at the state and federal level; academic experts; and consumer advocates.

3. Further clarification is needed with respect to FinCEN's guidance on the application of Bank Secrecy Act provisions toward digital currencies as well as explicit guidance from the Internal Revenue Service (IRS) on tax compliance, in accordance with the U.S. Government Accountability Office (GAO) report on virtual currencies. Current regulatory guidance has left open many questions.

INTERAGENCY COORDINATION IN THE UNITED STATES

To combat the exploitation of children, the U.S. Government utilizes numerous task forces, international initiatives, and reporting mechanisms. And, while the digital economy realm is an emerging, important part of the effort, its implications move beyond the space and include everything from trafficking (human, drugs, and arms) to the extension of financial inclusion initiatives to the unbanked globally. As a result, how to define the digital economy creates challenges in assigning and assuming ownership of associated responsibilities. The outcome is a diffusion of responsibilities across a multitude of agencies, all of which are working diligently to address specific sub-challenges associated with the digital economy, however, none of which capture the entirety of the overall situation. While this section is not meant to be exhaustive in examining all of the obstacles presented by the digital economy, it will look at the functions of key U.S. government departments/agencies, including education, training and reporting programs that play a role in the digital economy, address existing gaps in the interagency process, and make recommendations on next steps.

Brief Overview of the Current U.S. Interagency Process and the Digital Economy

Law Enforcement – Departments of Justice and Homeland Security

The "faces" of the digital economy are many, with divergent issues including innovation, transparency, Internet governance, and human rights. In the United States, responsibility for implementing policies often overlaps between agencies. Where there is illegal activity, for example, involving the digital economy, it falls under the jurisdictions of several departments and agencies. The U.S. Department of Justice (DOJ), through the 93 U.S. Attorneys Offices, prosecutes crimes that result from federal criminal investigations by the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), The Bureau of Alcohol, Tobacco, and Firearms (ATF), the U.S. Secret Service (USSS), and U.S. Immigrations and Customs Enforcement Homeland Security Investigations (ICE HSI). The latter two are federal law enforcement agencies under the U.S. Department of Homeland Security (DHS). Both the Departments of Justice and Homeland Security have strong structures in place to enforce existing federal laws that prohibit many of the illicit activities that can be enabled by the digital economy. These activities include money laundering, identity theft, child sexual exploitation, bank fraud, and wire fraud. The law enforcement components of both departments are actively engaged in sharing information with state, local, territorial, and tribal law enforcement partners, and when appropriate, intelligence community partners.[90] While too plentiful to list, there are numerous existing interagency working groups and task forces that coordinate policy, share law enforcement intelligence (domestically and internationally) and are working to combat crimes associated with the digital economy, including child exploitation.

90 *Partnerships and Outreach*, The Federal Bureau of Investigation, http://www.fbi.gov/about-us/partnerships_and_outreach/.

U.S. Department of State

As the international face of the U.S. Government, the U.S. Department of State is charged with implementing the President's foreign policy agenda. The State Department works closely with the U.S. Agency for International Development (USAID) to carry out U.S. global foreign assistance programs; collaborates with the Department of Defense (DOD) in coordinating key security assistance programs such as military and police training, counter-drug assistance, and counterterrorism activities; and serves as a pivotal partner along with the National Security Council (NSC) and Department of Treasury to international financial organizations while also playing a key role in delivering on U.S. commitments to foreign countries. For example, the State Department (along with USAID) is responsible for implementing U.S. commitments on global financial inclusion which seeks to help the approximate 2.5 billion unbanked people in the world gain access to financial products. This includes using a variety of payment methods and systems to deliver financial services globally.

Additionally, the State Department leads the U.S. Government's efforts to combat trafficking-in-persons (TIP). Chaired by the Secretary of State, the President's Interagency Task Force to Monitor and Combat Trafficking in Persons (PITF) brings together federal departments and agencies to ensure a holistic approach that addresses all aspects of human trafficking (including child sex trafficking and forced labor)[91]. As part of the PITF, these agencies convene routinely to coordinate federal policies that combat trafficking in persons and implementation of the Trafficking Victims Protection Act[92]. Given its unique role and global perspective, the State Department is a valuable source of information for law enforcement agencies in their work to combat child exploitation and human trafficking. Thus, whether it falls on the side of human rights, global development, security, or finance, the State Department is integral to any discussion on the digital economy.

U.S. Department of the Treasury

While law enforcement agencies and the State Department have primary oversight for the human rights implications of the digital economy, the financial aspects are presided over by the U.S. Department of the Treasury. Similar to law enforcement agencies and the State Department, Treasury also has several working groups and task forces dealing with the financial aspects of the digital economy, such as financial crimes. One of its leading components in the fight against money laundering, FinCEN, is the administrator of the Bank Secrecy Act, the law that requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering, and coordinates reporting between U.S. financial institutions and domestic agencies, such as the U.S. Federal Reserve and Department of Justice.[93] The Treasury Department's Money Laundering Threat Assessment (MLTA) working group provides a government-wide analysis of money laundering in the United States.[94] Composed of 16 federal agencies, bureaus and offices, the MLTA report is a vital resource for policymakers, regulators, and law enforcement in their strategic planning efforts to combat money laundering.[95] On an international level, the Treasury Department plays a key role in the G-8/G-20 and with other leading international organizations, such as the World Bank, International Monetary Fund (IMF), International Finance Corporation (IFC), and the Egmont Group. It is also a member of the Financial Action Task Force (FATF), an inter-governmental body that "set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering (AML), terrorist financing (CTF) and other related threats to the integrity of the international financial system."[96] In recognition of the changing financial landscape, including the impact of digital currencies, FATF recently adopted new guidance on pre-paid cards, mobile payment systems, and Internet-based payment services[97] and developed a new "effectiveness-focused" approach to mutual evaluations, which will scrutinize the effectiveness of a country's anti-money laundering regime for the first time, as well as technical compliance.[98]

While it is clear from the aforementioned examples that key departments and agencies collaborate on a range of issues related to the digital economy, there are remaining obstacles. Besides the ownership issue, growing anonymity in internet transactions and the emergence of the "deep web" as discussed in the earlier law enforcement section, is creating new challenges for enforcement and other governmental agencies. While DOJ for example, has successfully shut down websites such as Liberty Reserve, and there is a global

91 U.S. Dep't of State, Progress in Combating Trafficking in Persons: the U.S. Government Response to Modern Slavery (2013), *available at* http://www.state.gov/documents/organization/207421.pdf.

92 *Id.*

93 *FinCEN's Mandate from Congress,* Financial Crimes Enforcement Network, http://www.fincen.gov/statutes_regs/bsa/ (last visited Feb. 21, 2014).

94 U.S. Money Laundering Threat Assessment Working Group, U.S. Money Laundering Threat Assessment *(2005)*, *available at* http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf.

95 Financial Crimes Enforcement Network, Financial Crimes Enforcement Network Annual Report for Fiscal Year 2006 (2007), *available at* http://www.fincen.gov/news_room/rp/files/YEreport/AnnualReportFY2006.html#TOC.

96 *Who we are*, Financial Action Task Force (last updated 2014), http://www.fatf-gafi.org/pages/aboutus/.

97 *See* Financial Action Task Force, *supra* note 70.

98 Martin Coyle, *Mutual evaluations the top priority, but virtual currencies not being ignored, says FATF*, complinet.com (Jan. 10, 2014), http://www.complinet.com/global/news/news/article.html?ref=169175.

trend, led by an organization like FATF, to issue guidance on payment systems and promote, technology has outpaced current laws leaving significant policy and enforcement gaps. Even FinCEN's most recent MSB guidance, discussed in the Regulation section of this report, does not fully cover these products and their uses. In the absence of new laws, there is a strong case for an even more streamlined and collaborative interagency process in order to effectively meet the challenges of the digital economy.

Education/Training Programs and Reporting Mechanisms

The U.S. Government has long been at the forefront of using educational programs and training initiatives as a part of its wider foreign policy strategy. U.S. investment in promoting international standards and cooperation has made it highly influential and uniquely placed to effect change on an international policy level. As such, it is well positioned to set a standard on new, emerging phenomena, such as the emergence of the digital economy and non-fiat digital currencies. DHS, FBI, the State and Treasury Departments all have excellent training and liaison programs aimed at educating and assisting foreign partners.

In financial terrorism and integrity, DHS has successfully engaged foreign law enforcement, customs, financial intelligence units, regulatory, prosecutorial and judicial bodies in Asia, Africa, Middle East, and Latin America on cross border financial investigations and money laundering training activities.[99] DHS/HSI conducted over 30 Cross Border Financial Investigations Training (CBFIT) programs in fiscal 2013, and plans to conduct an additional 30 around the world in fiscal 2014. The CBFIT program provides specialized training, technical assistance, and best practices related to cross-border financial investigations to foreign law enforcement personnel, intelligence and administrative agencies, and judicial authorities. It is funded primarily through the State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL).[100] As it pertains directly to the digital economy, ICE HSI developed the Illicit Digital Economy Program (IDEP) which serves to address the challenges posed by the digital economy. In order to more succinctly focus resources, the illicit digital economy is divided into four sectors: the online traditional financial sector; the non-traditional and informal financial sector; online black markets; and third-party online money laundering facilitators. The investigative strategy centers on building internal capacity and engaging with interagency, academic, industry, and international partners.

Since 2002, the FBI has embedded cyber agents within law enforcement units in several key countries as a part of its 'Cyber Assistant Legal Attaché' program. The Legal Attaché program ("Legat") provides for a prompt and continuous exchange of information with foreign law enforcement and security agencies and coordination with U.S. federal law enforcement agencies that have jurisdiction over the matters under investigation. FBI personnel abroad serve under the authority of the Department of State, and their core mission is to establish and maintain liaison with principal law enforcement and security services in designated foreign countries. This liaison enables the FBI to effectively and expeditiously conduct its responsibilities in combating international terrorism, organized crime, cyber-crime, and general criminal matters. It also puts the FBI in a unique position to provide insight to foreign law enforcement authorities on the digital economy, including in countries where the legal infrastructures makes it more challenging to stay ahead of developments in this arena. The FBI maintains strong relationships with international partners, such as INTERPOL and Europol, giving it both access and influence within international discussions on the digital economy.[101]

In addition to the Legat program, the FBI's international law enforcement activities address international training. Funded by the Department of State or Department of Defense (and with participation from other agencies, including DHS/ICE), such training programs include the International Law Enforcement Academies in Budapest, Hungary, Bangkok, Thailand, and Gaborone, Botswana, as well as bilateral training programs targeting anti-terrorism, weapons of mass destruction, and terrorist financing. The FBI also participates in Bilateral Working Groups and in several additional counterterrorism training programs in the Middle East.[102]

The U.S. State Department is often able to provide input to foreign governments through educational programs and reporting. The department is widely recognized as being positioned at the forefront of international standard setting across many issues relevant to the digital economy discussion. Its country-by-country tiered report on trafficking-in-persons (TIP), for example, is one of the U.S. Government's principal tools in engaging foreign

99 *International Engagement Overview,* U.S. Dep't of Homeland Security, http://www.dhs.gov/international-engagement-overview (last visited Feb. 20, 2014).

100 *2013 International Narcotics Control Strategy Report*, U.S. Dep't of State (Mar. 5, 2013), http://www.state.gov/j/inl/rls/nrcrpt/2013/vol2/205251.htm.

101 Thomas V. Fuentes, Assistant Dir., Office of Int'l Operations, Fed. Bureau of Investigation, Statement before the Subcommittee on Border, Maritime, and Global Counterterrorism House Homeland Security Committee in Washington, D.C. (Oct. 4, 2007).

102 *Overview of the Legal Attaché Program*, Federal Bureau of Investigation, http://www.fbi.gov/about-us/international_operations/overview.

governments on human trafficking. The U.S. Government uses the TIP Report to engage foreign governments in dialogues to advance anti-trafficking reforms and to combat trafficking and to target resources on prevention, protection and prosecution programs.[103] International organizations, foreign governments, and nongovernmental organizations use the report as tool to examine where resources are most needed. Other reports with significant international impact include the department's "Annual Country Reports on Human Rights Practices" "Country Reports on Terrorism" and the "International Narcotics Control Strategy Report (INCSR)". At times, new reporting is included to update or broaden activities. In 2006, for example, a new section on Internet Freedom was added to the Human Rights report because of governments' ability to block content and monitor use of the Internet.[104] More recently, INCSR added a supplemental database to provide information on money laundering activities for a broader range of countries.[105] While expanding reports and capturing new information is not easy, it does provide additional needed context when evaluating these types of challenges on a global basis.

Meeting the Challenges of the Digital Economy through Changes to the Interagency Process

Integrating relevant digital economy issues into existing working groups, mechanisms and training initiatives is a good start. However, as stated previously, there are gaps in covering issues across agency lines. To address these issues and ensure the digital economy is being treated more holistically, there are three broad areas for consideration:

First, while recognizing departments and agencies have started defining aspects of the digital economy and issuing guidance (such as FinCEN's MSB guidance on virtual currencies) it would be helpful if either Congress or the White House to provide a clearer taxonomy and set of definitions and terms regarding the digital economy. This would empower government agencies unsure of their responsibilities and/or authority as it relates to the digital economy; it would provide consumers with more confidence when using non-fiat digital currencies. Below are just a few of the U.S. agencies that could have a role within in the digital economy discussion, which currently may not.

U.S. Consumer Financial Protection Bureau (CFPB): holds primary responsibility for regulating consumer products with regard to financial products and services in the U.S. The CFPB was created under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and is an independent bureau within the Federal Reserve System.[106] In 2010, the Dodd-Frank Act transferred consumer protection jurisdiction for banks and credit unions from federal banking regulators to the CFPB. It also gave the CFPB consumer protection jurisdiction over any company, not just banks and credit unions, involved in offering or providing a consumer financial product or service, as well as companies that are service providers to those that offer or provide consumer financial products or services (Public Law 111-517, Title X, §1002(6)).[107] Recently, the CFPB announced a proposed rule that would subject international money transfer providers to the same regulations as banks.[108] As consumers become more reliant on the digital economy and non-fiat digital currencies, it seems a reasonable assumption that there will be a role for the CFPB in protecting digital currency consumers.

U.S. Federal Trade Commission (FTC): has consumer protection jurisdiction over nearly every business in the United States, with a few significant exceptions – financial institutions regulated by federal banking regulators, insurance companies, and telecommunications companies among them.[109] While the Dodd-Frank Act created the CFPB and transferred consumer protection jurisdiction for banks and credit unions to them, the FTC retains jurisdiction over non-bank entities when it comes to unfair or deceptive acts or practices and has concurrent jurisdiction with the CFPB on the Fair Credit Reporting Act (FCRA). The FCRA is a federal law that regulates the collection, dissemination, and use of consumer information.[110] This seems particularly relevant to the discussion on non-fiat digital currencies given the ongoing contention between privacy and anonymity, and would necessitate involvement from the FTC.

103 *Trafficking in Persons Report*, U.S. Dep't of State, http://www.state.gov/j/tip/rls/tiprpt/ (last visited Feb. 21, 2014).
104 *Global Internet Freedom Task Force*, U.S. Dep't of State Archive, http://2001-2009.state.gov/g/drl/lbr/c26696.htm (last visited Feb. 20, 2014).
105 *2013 International Narcotics Control Strategy Report*, U.S. Dep't of State, http://www.state.gov/j/inl/rls/nrcrpt/2013/ (last visited Feb. 20, 2014).
106 *About us*, Consumer Financial Protection Bureau, http://www.consumerfinance.gov/the-bureau/ (last updated Dec. 10, 2013).
107 Mercedes Kelley Tunstall, *How the CFPB and the FTC interact (part 1)*, CFPB Monitor (July 7, 2011), http://www.cfpbmonitor.com/2011/07/07/how-the-cfpb-and-the-ftc-interact-part-i/.
108 Bureau of Consumer Financial Protection 12 C.F.R. § 1090 [Docket No. CFPB-2014-0003], *Defining Larger Participants of the International Money Transfer Market*, http://files.consumerfinance.gov/f/201401_cfpb_proposed-regulations_defining-larger-participants-intl-money-transfer-market.pdf.
109 *See* Tunstall, *supra* note 108.
110 Chris Jay Hoofnagle, *How The Fair Credit Reporting Act Regulates Big Data*, Future of Privacy Forum, http://www.futureofprivacy.org/wp-content/uploads/LEGAL-Hoofnagle-How-FCRA-Regulates-Big-Data.pdf.

U.S. Internal Revenue Service (IRS): the bureau responsible for collecting taxes in accordance with the Internal Revenue Code. The IRS has not yet issued tax guidance specific to non-fiat digital currencies, though income generated from any source– must be reported currently.[111]

U.S. Commodity Futures Trading Commission (CFTC) and the U.S. Securities Exchange Commission (SEC): The CFTC regulates futures and options markets,[112] while the SEC holds responsibility for enforcing federal securities laws and regulates the securities industry.[113] Their role within the digital economy discussion will become clearer depending on how non-fiat digital currencies are defined.

Second, the establishment of an overarching framework to capture the nuanced challenges of the digital economy would be helpful. One consideration would be the creation of a task force or working group at a department or agency level to coordinate policy throughout the government such as the National Security Council or National Economic Council. Existing mechanisms and working groups would have reporting lines to this new structure, which would be responsible for ensuring that intelligence relating to the myriad challenges associated with the digital economy is fed into a central source. For example, the Treasury Department would have a direct reporting line into the working group or task force while continuing to be the lead (along with law enforcement, international partners and domestic agencies) in the fight against financial crime. The same process would apply to DOJ and DHS. As key law enforcement agencies , such as FBI, USSS, and ICE HSI, continue to capture data and information related to the illicit uses of digital economy infrastructure, DOJ and DHS, through their various components, would be significant contributors to a centralized digital economy task force/working group. Ultimately, a centralized working group or task force within the U.S. Government would be well positioned to provide support to strategic and technical goals in the framework to address the digital economy.

Third, involving private sector stakeholders (law enforcement, financial sector, academia, etc.) can provide government with valuable resources and expertise as they consider some of the biggest challenges and opportunities associated with the digital economy. The value of these public-private partnerships has been demonstrated through a number of initiatives, such as the USAID-Booz Allen Hamilton Mobile Financial Services Risk Matrix, a research project that provides detailed analysis of the various risks involved in the different models of mobile financial services.[114] It brought together USAID, Booz-Allen Hamilton, the Kenya School of Monetary Studies (KSMS), key Kenyan central bank regulators, and included significant input from private sector stakeholders. The Better than Cash Alliance is another example. Founded by the Bill & Melinda Gates Foundation, Citi, Ford Foundation, Omidyar Network, USAID, U.N. Capital Development Fund, and Visa, it works with governments, the development community and the private sector to digitize cash payments to people in emerging economies.[115]

111 Robert A. Green, *The Tricky Business of Taxing Bitcoin*, Forbes.Com (Dec. 3, 2013) http://www.forbes.com/sites/greatspeculations/2013/12/03/the-tricky-business-of-taxing-bitcoin/.

112 *Mission & Responsibilities*, U.S. Commodity Futures Trading Comm'n, http://www.cftc.gov/About/MissionResponsibilities/index.htm.

113 *The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation*, U.S. Sec. and Exch. Comm'n (last modified June 10, 2013), http://www.sec.gov/about/whatwedo.shtml.

114 Kenya School of Monetary Studies, U.S. Agency for Dev. & Booz Allen Hamilton, Mobile Financial Services Risk Matrix (2010), *available at* http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf.

115 *Founding Members of the Better than Cash Alliance Pledge Deep Commitment on One Year Anniversary*, USAID (Sept. 24, 2013), http://blog.usaid.gov/2013/09/better-than-cash-alliance-one-year-anniversary/; *see also* Better Than Cash Alliance, http://betterthancash.org/ (last visited Feb, 11, 2014).

Recommendations:

1. The U.S. Government (Congress or the White House) should establish clear definitions for the digital economy to provide clarity within the U.S. structure on ownership and treatment within the interagency system.

2. The Administration should establish a high-level interagency task force or working group (to include broad participation) with a strategic mandate on the digital economy to coordinate policy throughout the U.S. Government.

3. Interagency resources should be dedicated for the purposes of better understanding the mechanics of new payment systems money movements in order to: identify specific risk points, establish indicators of potential illicit activities, and to develop mitigation strategies for interagency use and deployment.

4. Because of the emergence of the "deep web" and the anonymity that non-fiat digital currencies provide, the U.S. Department of State (and other organizations issuing reports on these issues, such as the United Nations) should to the greatest degree possible feature the use of these products in existing reports and publications.

5. Law enforcement agencies, such as the FBI, Secret Service and ICE HSI and International Programs (U.S. State Department/International Narcotics and Law Enforcement/ Democracy, Human Rights & Labor) should leverage their legal attaché programs (where appropriate) to expand analysis and information gathering on the digital economy. They should also examine whether there is potential to cooperate with foreign allies on producing joint briefings specifically on the digital economy.

6. Private sector stakeholders and academics should continue to form working groups to help inform, collaborate, and brainstorm with governments and international organizations faced with challenges and opportunities associated with the digital economy.

CONCLUSION AND FINAL RECOMMENDATIONS

The digital economy presents new and unique challenges for law enforcement, policymakers, industry and consumers. These innovative technologies require the adaptation of existing frameworks, as well as the development of new ones, to effectively ensure that they are not abused to the detriment of our children and our society. The compilation of recommendations below represents initial steps that can be taken to this end.

Defining the Issue

1. Conduct rigorous, validated studies of the sexual exploitation of children, its incidence, and prevalence, so that resources can be directed towards reducing the victimization of children as effectively as possible, with measurable results.

Law Enforcement

2. Conduct research on the following:

   a. Determine if there are methods accessible to law enforcement, including "clustering," that could be used based on probable cause and appropriate legal process to overcome criminal misuse of anonymizing tools.

   b. Identify lessons learned from recent network exploitations of anonymizing tools to develop more effective and lawful investigative tools and models.

   c. Assess current money transmitter laws and their applicability for child sexual exploitation investigations.

3. Develop enhanced law enforcement investigative protocols, techniques and methods, based upon these research results with a focus on cross-sector partnerships and collaboration. Draft model law and procedures regarding uniform cyber investigative techniques for law enforcement as an implementation guide for parliaments and legislative bodies worldwide.

4. Promote and facilitate international law enforcement coordination, information sharing, and cooperation to address problems associated with the digital economy, and ensure that entities like the Virtual Global Task Force and the Global Alliance Against Child Sexual Abuse Online are utilized to ensure broader global law enforcement cooperation in investigating these crimes.

5. Policymakers should become famailiar with AML/CFT rules and principles and encourage their application to digital economy money services businesses globally.

6. Develop reasonable regulatory definitions and limits to ensure that Internet anonymity does not become a safe harbor for criminal activity, including greater Raise awareness amongst the global law enforcement community regarding the need to proactively respond to the increased use of anonymizing tools in furtherance of child sexual exploitation.

Regulation

7. Regulation in this sphere should be done through a risk-based approach, identifying and addressing the unique and similar potential risks — including commercial sexual exploitation of children, money laundering, terrorist financing, fraud, consumer protection and other area of illicit finance and these must be weighed against the potential benefits of the digital economy. As with other regulations, a cost-benefit analysis should be conducted..

8. A specialized group should be formed with a mandate to research the following topics, among others:

    a. The process flows and critical control points in digital transactions. With regard to digital currency transactions, this should distinguish between centralized and decentralized currencies.

    b. Whether and where there is a need for regulation among aspects of the digital economy.

    c. Where regulation is deemed appropriate and whether existing rules and regulations may be applied effectively.

    d. If and where a need for regulation is found but there are no existing regulations, other regulatory remedies should be considered (subject to cost benefit analysis).

    e. The appropriate division of authority between state and federal regulatory agencies.

    This group should include representatives from across the digital economy and other affected industries; regulatory authorities at the state and federal level; academic experts; and consumer advocates.

9. Further clarification is needed with respect to FinCEN's guidance on the application of Bank Secrecy Act provisions toward digital currencies as well as explicit guidance from the Internal Revenue Service (IRS) on tax compliance, in accordance with the U.S. Government Accountability Office (GAO) report on virtual currencies. Current regulatory guidance has left open many questions.

Interagency Process

10. The U.S. Government (Congress or the White House) should establish clear definitions for the digital economy to provide clarity within the U.S. structure on ownership and treatment within the interagency system.

11. The Administration should establish a high-level interagency task force or working group (to include broad participation) with a strategic mandate on the digital economy to coordinate policy throughout the U.S. Government.

12. Interagency resources should be dedicated for the purposes of better understanding the mechanics of new payment systems money movements in order to: identify specific risk points, establish indicators of potential illicit activities, and to develop mitigation strategies for interagency use and deployment.

13. Because of the emergence of the "deep web" and the anonymity that non-fiat digital currencies provide, the U.S. Department of State (and other organizations issuing reports on these issues, such as the United Nations) should to the greatest degree possible feature the use of these products in existing reports and publications.

14. Law enforcement agencies, such as the FBI, Secret Service and ICE HSI and International Programs (U.S. State Department/International Narcotics and Law Enforcement/ Democracy, Human Rights & Labor) should leverage their legal attaché programs (where appropriate) to expand analysis and information gathering on the digital economy. They should also examine whether there is potential to cooperate with foreign allies on producing joint briefings specifically on the digital economy.

15. Private sector stakeholders and academics should continue to form working groups to help inform, collaborate, and brainstorm with governments and international organizations faced with challenges and opportunities associated with the digital economy.

GLOSSARY

It is helpful to establish a set of common terms regarding the digital economy to enable private sector entities, government officials, and law enforcement to analyze the uses – including the potential criminal risks – of new payment methods. The definitions provided below, for the purposes of this report, are a compilation of commonly accepted definitions. Some of the definitions set forth below were provided by the FinCEN. Others are included here to help provide a common language for developing conceptual tools to help provide a better understanding of how digital currencies operate, along with the risks and potential benefits they offer.

An **administrator** is a person/entity engaged as a business in **issuing** (putting into circulation) a centralized virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.[116]

AML/CFT - Anti-Money Laundering, Combating the Financing of Terrorism
Money laundering is the process by which proceeds from a criminal activity are disguised in order to conceal their illegal origin.[117] Terrorist financing is the soliciting, collection, or provision of funds with the intention that they be used to support terrorist acts or organizations.[118] Money-laundering and financing terrorism techniques are very similar, and in many cases, identical.[119]

Anonymizing networks provide a way to anonymize Internet communications by making it difficult to link communication parties.[120] Anonymizing networks route Internet traffic through independent nodes in separate administrative domains in order to hide the client's IP address.[121]

116 *See generally,* Financial Crimes Enforcement Network, *supra* note 69, at 2.

117 *Anti-Money Laundering/Combating the Financing of Terrorism-Topics*, International Monetary Fund, http://www.imf.org/external/np/leg/amlcft/eng/aml1.htm.
118 *Id*.
119 *Id*.
120 *Anonymizing Networks*, Privatics (last viewed Feb. 20, 2014), https://team.inria.fr/privatics/anonymizing-networks/.
121 Patrick P. Tsang et al., *Nymble: Blocking Misbehaving Users in Anonymizing Networks*, 8 Dependable and Secure Computing, IEEE Transactions on, 256, 256 (2011) available at http://freehaven.net/anonbib/cache/nymble-tdsc.pdf.

Bitcoin, launched in 2009, was the first decentralized convertible virtual currency and the first cryptocurrency. Bitcoins are mathematical tokens composed of unique strings of numbers and letters that constitute units of the currency and are oftentimes traded on a peer-to-peer basis. Bitcoins may be digitally traded between users with a high degree of anonymity and can be exchanged into U.S. dollars, Euros, and other currencies for goods and services. Anyone can download the open-source reference software to send, receive, and store bitcoins, and to monitor bitcoin transactions. Users can also obtain Bitcoin accounts at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in an online transaction ledger, called the blockchain, shared by all nodes running the Bitcoin protocol to participate in the Bitcoin mining and transaction validating system. Bitcoin is capped at 21 million bitcoins, projected to be reached by 2041. As of early February 2014, there were 12.4 million bitcoins, with total value of more than U.S. $8 billion.[122]

Bulletproof hosting is a service offered by companies allowing customers to upload and distribute material without risk of legal threats and blocks.[123]

Centralized Virtual Currencies have a single administrating authority (**administrator)**, i.e., a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either **floating,** i.e., determined by market supply and demand for the virtual currency – or **pegged,** i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralized virtual currencies.[124] Examples: e-Gold (defunct); Linden Dollars PerfectMoney; (Second Life); WebMoney; and World of Warcraft Gold.

Cryptocurrency refers to a math-based, decentralized convertible virtual currency that is protected by cryptography, i.e., it incorporates principles of cryptography to implement a distributed, decentralized, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers are ensured by a network of mutually untrusted parties (in Bitcoin, referred to as miners) who actively protect the network in a proof-of-work system by maintaining a high hash-rate difficulty often in exchange for the opportunity to obtain a randomly distributed fee (in bitcoin, a small number of newly created or mined bitcoins). Dozens of cryptocurrency specifications have been defined, most derived from Bitcoin as the first fully implemented cryptocurrency protocol.[125]

Convertible (or open) virtual currency[126] may be either centralized or decentralized. Convertible virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency. Examples include: Bitcoin[127]; e-Gold (defunct); Second Life Linden Dollars; and WebMoney.

The **deep web** or **dark net** is an area of the Internet that is characterized by the goal of providing complete anonymity.[128]

De-centralized Virtual Currencies (a.k.a. crypto-currencies) are distributed open-source, math-based peer-to-peer digital currencies that have no central administrating authority, no central third-party transaction ledger, and no central monitoring or oversight.[129] Examples: Bitcoin and LiteCoin.

122 *What is Bitcoin?,* Bitcoin.org, (last visited Feb. 20, 2014), https://bitcoin.org/en/faq#what-is-bitcoin.

123 *See* Bobbie Johnson, *Internet pirates find 'bulletproof' havens for illegal file sharing*, The Guardian (Jan. 4, 2010), http://www.theguardian.com/technology/2010/jan/05/internet-piracy-bullet-proof.

124 *See generally,* Financial Crimes Enforcement Network, *supra* note 69, at 4.

125 *See Definition of cryptocurrency*, PC Magazine Encyclopedia, (last visited Feb. 20, 2014), http://www.pcmag.com/encyclopedia/term/66379/cryptocurrency.

126 *See generally,* Financial Crimes Enforcement Network, *supra* note 69, at 2.

127 *See* FBI Directorate of Intelligence, *supra* note 35. "Bitcoin" (capitalized) refers to both the open source software used to create the virtual currency and the P2P network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.

128 Lev Grossman & Jay Newton-Small, *The Secret Web: Where Drugs, Porn and Murder Live Online*, Time (Nov. 11, 2013), http://content.time.com/time/magazine/article/0,9171,2156271,00.html.

129 *See generally,* Financial Crimes Enforcement Network, *supra* note 69, at 5.

Digital currency is a digital representation of either virtual currency (non-fiat) or e-money (fiat).[130]

Encryption masks data in order to prevent unauthorized visibility during data transfer or storage.[131]

An **exchanger (also sometimes called a virtual currency exchange)** is a person/entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency. Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, nonaffiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.[132]

Fiat Currency (a.k.a. **"real currency," "real money,"** or **"national currency"**), is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country.[133]

An Internet **identifier** is defined as "electronic mail addresses and other designations used for self-identification or routing in Internet communication or posting."[134]

An **IP address** is a binary number (i.e., consisting of ones and zeros) that uniquely identifies a computer or other device on a network.[135]

Non-convertible (or closed) virtual currency is specific toa particular virtual world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG), and cannot be exchanged for fiat currency under the rules governing its use.Examples: Project Entropia Dollars; Q Coins; and World of Warcraft Gold. All non-convertible virtual currencies are centralized: by definition, they are issued by a centralauthority that establishes rules making them non-convertible.[136]

A **proxy server**, also known as a proxy, is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet. Proxy servers provide increased performance and security. In some cases, they monitor employees' use of outside resources. A proxy server works by intercepting connections between sender and receiver. All incoming data enters through one port and is forwarded to the rest of the network via another port. By blocking direct access between two networks, proxy servers make it much more difficult for hackers to get internal addresses and details of a private network.[137]

The Tor Project – a 501(c)3 U.S. non-profit organization – "…aims to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention." Tor's global team works in active collaboration "… across scientific, charitable, civic, government and education sectors."[138]

130 U.S. Dep't of Homeland Security, *ICE Statement for the record for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies",* DHS.Gov (Nov. 18, 2013), https://www.dhs.gov/news/2013/11/18/ice-statement-record-senate-committee-homeland-security-and-governmental-affairs. "Bitcoin" (capitalized) refers to both the open source software used to create the virtual currency and the P2P network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.

131 Microsoft Corporation, *Privacy Guidelines for Developing Software Products and Services,* Version 3.1 (2008), at 48.

132 *See generally,* Financial Crimes Enforcement Network, *supra* note 69, at 2.

133 *See Definition of fiat money*, Financial Times Lexicon (last visited Feb. 20, 2014), http://lexicon.ft.com/Term?term=fiat-money, *see also* Franklin Noll, *The Birth of U.S. Fiat Currency*, Bloomberg (Apr. 2, 2012, 11:40 AM), http://www.bloomberg.com/news/2012-04-02/the-birth-of-u-s-fiat-currency.html.

134 KIDS Act of 2008, S.431, 110th Cong. § 2(e)(2) (2008).

135 *Understanding TCP/IP addresses and subnetting basics*, Microsoft Support (last visited Feb. 20, 2014), http://support.microsoft.com/kb/164015.

136 U.S. Gov't Accountability Office, Virtual Economies and Currencies, Additional Guidance Could Reduce Tax Compliance Risks 39 (2013), *available at* http://www.gao.gov/assets/660/654620.pdf.

137 *What is a proxy server?*, University Information Technology Services Knowledge Base, http://kb.iu.edu/data/ahoo.html (last modified Jan. 7, 2014).

138 Tor, *Annual Report 2012*, Tor Project, https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf (last visited Feb. 20, 2014).

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send remittances in a personal capacity to another person (for personal use), or who or holds the virtual currency as a (personal) investment. Users can obtain virtual currency in one of three ways. They can (1) purchase virtual currency (from an exchanger or, for certain centralized virtual currencies, directly from the administrator/issuer), using real money; (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); and (3) with some decentralized virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them, which involves running special software to solve complex algorithms in a "distributed proof-of-work system" used to validate transactions in the virtual currency system.[139]

Virtual currency is a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. Virtual currency is distinguished from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. Virtual currency is also distinct from **e-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency, i.e., it electronically transfers value that has legal tender status.[140]

139 *See generally,* Financial Crimes Enforcement Network, *supra* note 69, at 2.
140 *Id.* at 1.