Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments

By

John Villasenor

Nonresident Senior Fellow
Governance Studies and the Center for Technology Innovation, The Brookings Institution

Cody Monk

Instructor/Lecturer
National Intelligence University and The Naval Postgraduate School

Christopher Bronk

Fellow in Information Technology Policy
James A. Baker III Institute for Public Policy, Rice University

August 29, 2011

This paper was written by a researcher (or researchers) who participated in a Baker Institute and Center for Technology Innovation at Brookings research project. The research and views expressed in this paper are those of the individual researchers, and do not necessarily represent the views of the James A. Baker III Institute for Public Policy or the Center for Technology Innovation at Brookings.

About the Center for Technology Innovation at Brookings

The Center for Technology Innovation at Brookings focuses on delivering research that impacts public debate and policymaking. Our work centers on identifying and analyzing key developments to increase innovation; developing and publicizing best practices to relevant stakeholders; briefing policymakers about actions needed to improve innovation; and enhancing the public and media's understanding of technology innovation.

The Brookings Institution is a private, nonprofit organization. Its mission is to conduct high quality independent research and to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the institution, its management, or its other scholars.

About the James A. Baker III Institute for Public Policy at Rice University

The mission of the Baker Institute is to help bridge the gap between the theory and practice of public policy by drawing together experts from academia, government, media, business and nongovernmental organizations. By involving policymakers and scholars, as well as students (tomorrow's policymakers and scholars), the institute seeks to improve the debate on selected public policy issues and to make a difference in the formulation, implementation and evaluation of public policy, both domestic and international. The Baker Institute is an integral part of Rice University, one of the nation's most distinguished institutions of higher education. The efforts of Baker Institute fellows and affiliated Rice faculty focus on several ongoing research projects, details of which can be found on the institute's website, http://bakerinstitute.org.

Executive Summary

The history of the movement of money is as complex and varied as the history of money itself, and includes ships laden with gold bullion, desert caravans carrying salt or cowry shells, armored trucks filled with banknotes, paper checks, and today, a large and quickly growing list of digital transfer methods. Secrecy and anonymity have always played roles in the movement of money, most commonly because they offer a strong measure of privacy and protection against being targeted by thieves, but also because the parties in financial transactions can have other reasons—some legitimate, some not—for keeping a low profile.

The combination of the enormous growth in social networks, the complexity of peer-to-peer systems and software, and the number of Internet and wirelessly connected devices is altering the landscape of financial transactions at a rate and to a degree that is unprecedented. Today, such transactions can be conducted not only using traditional, state-backed currencies, but also through purely digital currencies, virtual currencies, and virtual goods. In addition, mobile phone-based money transfer systems enabling traditional currencies to be moved in novel ways are experiencing rapid adoption, particularly in developing nations.

Almost no one would argue that governments do not have a right to track and trace digital financial transactions associated with activities such as terrorism and human trafficking. It is less clear, however, how governments can surmount the formidable technical and organizational challenges associated with detecting and monitoring these transactions. The solution will require a combination of self-regulation, government-industry collaboration, and change in both technology and culture within government agencies.

Introduction

"Follow the money. Always follow the money,"[1] advises Deep Throat in the 1976 Watergate film *All the Presidents Men*. "To where?" Bob Woodward's character responds. This exchange captures the essence of financial transactions, which, at their core, involve combining the concepts of money, movement, and location.

Today, information can be exchanged among billions of computers, mobile phones, tablets, and other Internet and wirelessly connected devices. There are robust online markets in virtual goods, sometimes paid for using virtual currencies. Computers across the globe can be used collectively to store information in a distributed manner so that the information is, in a sense, both nowhere and everywhere at the same time. Encrypted data that conveys or unlocks value can move thousands of miles in milliseconds. And all of this flexibility is being used to design new ways to move money.

As a result, the landscape of financial transactions today involves levels of complexity that would have been unimaginable in the Watergate era. Increasingly, this landscape also includes systems explicitly designed to deliver financial opacity. Using these systems, the proverbial suitcase filled with cash can now be handed to someone on the other side of the world as easily—or more easily—than it can be handed to someone in a city park in the dark of night.

While there is a wide spectrum of views regarding the right to digital privacy, almost no one disputes the notion that the right to digital financial privacy does not extend to providing an impenetrable legal shield for the online financial activities of terrorist groups, human traffickers, or drug cartels. Today, government agencies and other organizations that include monitoring of illicit financial activity within their charter face an environment in which the methods to track transactions are increasingly mismatched to the methods used to perform them. Resolving this mismatch will require new tools, increased cooperation within and across governments, and cultural changes.

Hiding in Plain Sight

While financial obfuscation can benefit from advanced technology, it does not require it. For example, *Hawala*[2] and other informal value transfer systems long predate the advent of computers and the Internet, and**,** in more recent years, have been of concern to authorities because of their potential to be used for money laundering and terror financing.[3] Modern technology changes the game, however, by enabling an almost endless list of new ways to facilitate financial opacity.

Technology-facilitated transactions can be designed to be invisible. Alternatively, they can be designed to be visible but anonymous. Amounts, sources, and destinations can be intentionally structured to be misleading. Transactions can be masked as other activities appearing to have nothing to do with money. The possibilities are limited only by the demonstrably high levels of imagination and skill of people who dream up new ways to use technology.

Obfuscation is possible, in part, due to a positive feedback loop with respect to scale. As the ecosystem designed to support opaque transactions grows in size and sophistication, such transactions will become easier and more efficient to conduct, thus attracting more participants to join the ecosystem and further increasing its power to obfuscate. The Internet and the profusion of wireless devices and networks greatly expands the ability to decentralize, and, therefore, to hide. As a result, while every digital transaction may in theory be available to find, tracing a specific suspect transaction that is intentionally buried “in the noise” can be like trying to find a pickpocket who just stole a wallet in a crowded market. The knowledge that the pickpocket is certainly among the hundreds of people within view is of little comfort if there is no practical ability to search every person in the market.

Scale enables vanishingly low transaction costs, which are an essential element in the ability to hide larger movements of money by conducting many smaller transactions. A movement of $900,000 conducted using 100 different electronic transfers of $9,000 might be easy to spot. If, however, the power of a large, distributed online network were used to move this money using

100,000 transactions with randomized amounts generally in the $6 to $15 range, detection would be much more difficult.

Increased scale also contributes to trust. The recipient of a payment must have confidence that the transaction is genuine, that it will hold its value, and that others will later accept it as a medium of exchange. A person making a payment places trust in the ability of the entities involved in delivering the payment to complete and verify the delivery. As digital approaches for hiding payments become more mature, they will have more liquidity and higher volumes and thus be trusted by larger numbers of users.

A Multiplicity of Currencies

In l996, physician Douglas Johnson started spending his evenings writing software to create e-gold, a new digital currency that, though not issued by any government, would be fully backed by gold stored at various locations around the world. By 2001, there were nearly 300,000 e-gold customer accounts with an aggregate value of about $16 million.[4] As it grew, Nevis-based e-gold drew attention from criminals who found it a convenient means to launder money and conduct transactions related to identity theft, and then from the U.S. Department of Justice, which in April 2007 unsealed an indictment charging Johnson and two principal e-gold directors with, among other crimes, money laundering and operating an unlicensed money transmitting business.[5] As the Department of Justice press release announcing the indictment stated:

> Persons seeking to use the E Gold payment system were only required to provide a valid email address to open an E Gold account – no other contact information was verified. Once an individual opened an E Gold account, he/she could fund the account using any number of exchangers, which converted national currency into E Gold. Once open and funded, account holders could access their accounts through the Internet and conduct anonymous transactions with other parties anywhere in the world.[6]

In addressing the indictment, FBI Cyber Division Assistant Director James Finch noted that "the advent of new electronic currency systems increases the risk that criminals, and possibly terrorists, will exploit these systems to launder money and transfer funds globally to avoid law enforcement scrutiny and circumvent banking regulations and reporting."[7] In July 2008, Jackson and the two indicted e-gold directors pleaded guilty to some of the charges and agreed to comply with federal and state money transfer laws.[8]

E-gold operated openly, had centralized operations, and was overseen by at least three principals resident in the United States. These attributes made it easier for U.S. authorities to investigate e-gold and bring it into compliance with U.S. banking laws—a lesson certainly not lost on those intent on creating the next generation of methods for anonymous money exchange.

Enter Bitcoin, a digital currency based on a paper[9] that was self-published on the Internet in 2009 by an author listed as Satoshi Nakamoto, and whose true identity and location has generated much speculation but much less concrete information. Bitcoin utilizes a peer-to-peer network to create multiple complete replicas of transactions conducted by people whose identities are hidden behind public-private key encryption pairs.[10]

While e-gold was backed by actual gold, Bitcoin is fully virtual, backed only by the confidence of the people who use it for transactions. A governmental entity attempting to shut down Bitcoin servers in its territory would almost certainly find that even more servers would spring up, Hydra-like, in other parts of the world. As of July 23, 2011, there were approximately 6.9 million Bitcoins trading at a value of more than $13 per Bitcoin, corresponding to a total supply of over $90 million.[11]

Perhaps unsurprisingly, the use of encrypted identities in Bitcoin has spurred the creation of an online market that accepts payments only in Bitcoins and links anonymous drug buyers with anonymous drug sellers.[12] As Senators Joe Manchin (D-WV) and Charles Schumer (D-NY) stated in a June 2011 letter sent to Attorney General Eric Holder and Drug Enforcement Administration Administrator Michele Leonhart, "after purchasing Bitcoins through an

exchange, a user can create an account on Silk Road and start purchasing illegal drugs from individuals around the world and have them delivered to their homes within days."[13]

The potential Achilles heel of Bitcoin—that each server in the network contains a complete record of all transactions—will almost certainly be addressed in future systems that distribute transaction information so that no single server or small collection of servers contains a complete transaction record. It is also possible to envision systems in which the transaction records are not only distributed, but evanescent, so that even the collective information stored on all the servers in the system at any given time would not enable a complete reconstruction of transaction history.

Virtual Worlds

Another trend with direct implications for financial transactions is the growth in virtual worlds, which has been accompanied by a corresponding growth in virtual goods, markets, and currencies. Virtual worlds are usually created to provide entertainment for their users and profit for their designers. However, as they have grown, they have evolved into economies with sufficient scale and complexity to enable the conduct of large**,** off-the-radar financial transactions.

One of the earliest virtual worlds to achieve significant scale is Linden Lab's Second Life, which uses a virtual currency called the Linden Dollar (L$). While the trade in L$ is not enormous, neither is it insignificant. The L$ transactions in Q1 2011 had an aggregate equivalent U.S. dollar value of US$30 million. The L$ money supply in Q1 2011 was equivalent to US$29.3 million, an increase of approximately 12 percent over the money supply in Q1 2010.[14]

The market in virtual goods transactions related to massively multiplayer online role-playing games (MMORPG), which includes purchases using virtual currencies as well as real currencies (called real-money trade, or RMT),[15] is much larger and somewhat less transparent than that of Second Life. This market has grown out of the ability in MMORPGs to generate currency—"gold," in the case of the popular World of Warcraft (WoW) game. WoW's gold currency has yielded prospectors—game players paid to collect gold through gameplay that can then be sold outside the game platform to other players in a process known as gold farming.[16] Often

concentrated in lower-wage countries with adequate bandwidth to service WoW online play, gold farming has become a genuine job option for growing numbers of people.

As of 2008, the gold farming economy was estimated to include 400,000 gold farmers earning an average of $145 per month and producing a global market valued at $500 million.[17] This is similar to the gross domestic product (GDP) of Samoa—still very small on a global scale, but many times larger than the output of Second Life.[18] The means of production for gold farming are relatively simple—computers, connectivity, and players. Given the continued growth in online gaming, the gold farming economy has undoubtedly grown significantly since 2008.

According to South Korean authorities quoted in an August 4, 2011, *New York Times* article,[19] North Korea has adopted gold farming as means to help address its perennial shortage of hard currency. A senior official at South Korea's International Crime Investigation Unit stated that North Korean hackers had created software to accumulate points in online games that were then converted to cash for the North Korean government. The scheme is alleged to have generated $6 million in under two years.

Facebook has become the hub for social-network-based games, most notably in relation to Zynga, the company behind Farmville, Cityville, and Mafia Wars. The mechanisms that create an external marketplace in the WoW model have in Zynga been captured as a primary source of revenue. As a result, Zynga has experienced spectacular growth, with expected 2011 revenues pegged at almost $1 billion.[20] Due largely to the growth in social-network-based games, the U.S. market for virtual goods is projected to exceed $2 billion in 2011.[21]

Virtual goods can be used in novel ways to facilitate financial transactions. If $15,000 is sent in support of criminal activity from the United States to a foreign country using a traditional interbank wire transfer, the transaction will be documented in accordance with various recording requirements. If ownership of virtual goods worth $15,000 is conveyed from a person in the United States to a person overseas who then exchanges those goods for cash, assembling the information linking the sender, recipient, and amount would be a far more difficult task. In addition to technology hurdles, there would be legal hurdles arising from the number and variety

of entities in two or more countries that might each have partial information related to the transaction, and from the differing laws in those countries. These hurdles would be even steeper if the transaction were conducted through large numbers of intermediaries, each located in a different country.

Mobile Money

In addition to enabling virtual currencies and virtual worlds, information technology is also making it possible to move traditional currencies in nontraditional ways. Over the last decade, considerable economic activity, particularly in developing countries, has migrated to mobile phones. In large parts of the developing world, what were once predominantly cash and barter economies are being transformed by the widespread adoption of mobile-phone-enabled payments in locales often having limited wireline telecommunications infrastructure, spotty electrical grids, few paved roads, and high numbers of "unbanked" people who do not hold traditional bank accounts.

M-PESA is a pioneering mobile money transfer (MMT) service offered by Kenya-based Safaricom and Vodaphone that has experienced spectacular growth. As explained in a recent *EE Times India* article:

> M-Pesa allows its users to load money on their mobile devices by making deposits with M-Pesa agents residing in rural and remote areas with limited or no banking facilities. The deposited money is exchanged for "e-float" which can be used for making payments or money transfers.[22]

The service, which was initially launched in early 2007, grew to more than 6 million users in 2009, more than 9 million users in 2010, and nearly 14 million users as of March 2011. In 2010, M-PESA was used to perform over 305 million transactions, with a daily average volume of over $24 million.[23]

In a survey of M-PESA users conducted in late 2009 and described in an October 2010 MIT report,[24] more than 80 percent of users reported using M-PESA as a means to store savings.[25]

When compared with an earlier round of the survey conducted in 2008, the 2009 results showed that the percentage of unbanked users had increased from 25 percent to 50 percent, and that the percentage of users in rural areas had increased from 29 percent to 41 percent.

The success of M-PESA in Kenya has not gone unnoticed in Nigeria, Africa's most populous nation, where telecom operator MTN plans to launch an MMT service modeled on M-PESA. In Nigeria, there are more than 85 million active mobile phone lines but only 28 million people with bank accounts in a population of 140 million.[26] Given M-PESA's growth rates in East Africa, it is likely there will be tens of millions of users of MTN's service in Nigeria within a few years.

MMT services are bringing banking to millions of people who have never held an account at a traditional bank, much in the same manner that many people in the developing world went from having no phone at all to having a mobile phone without ever taking the intermediate step of owning a landline telephone. The same demographic characteristics that favor the growth of MMT in Kenya and Nigeria are present across much of the developing world. For many people living in these regions, banking and mobile banking are, or will soon be, synonymous.

It is statistically inevitable that some fraction of the more than 300 million transactions performed using M-PESA in 2010, and of the much larger number of transactions that will be performed in 2011 and future years, will not be legitimate. And some fraction of those, in turn, may involve payments that bear on American national security or law enforcement concerns. The risk that MMT could be used for money laundering or terror financing was considered in a report issued by the GSM Association (GSMA),[27] an industry group representing the interests of more than 800 mobile operators across the world.[28] The report notes that "agents, intermediaries, and retail partners" are "in a position to falsify records, [and] ignore suspicions that may otherwise be reported."[29] The proposed mitigation methods include actions by MMT service providers to "assess compliance and integrity of their agents," to provide assistance and training in anti-

money laundering and in combating the financing of terrorism," and to "identify unusual activity and investigate an[d] take corrective action."[30]

While these approaches sound good on paper, they will be hard to deploy effectively on a large scale. According to Safaricom, there are over 23,000 M-PESA agents in Kenya alone.[31] With the continuing rollout of M-PESA and similar services across many countries in addition to Kenya, the global number of mobile payment agents will likely soon be in the hundreds of thousands. Even when MMT service providers act with the best of intentions in the agent vetting and monitoring process, it will be impossible to ensure universal integrity. Each of the many agents in MMT services sits at a nexus of transactions. MMT is too new to have generated a significant historical record of publicly disclosed investigations and prosecutions regarding its use to support illicit transactions. However, one of the most important lessons from the cybercrime investigations of the last decade is that those sitting at digital financial transaction nexuses are well positioned to support or engage in illegal activity.

For example, in the New York case *People v. Western Express International, Inc.*, Western Express was alleged to have provided credit and facilitated transactions for buyers and sellers of stolen credit card data using the unregulated digital currencies e-gold and WebMoney.[32] New York State Supreme Court Associate Justice David Saxe, writing for the majority in an April 2011 opinion in the *Western Express* case, explained that the use of digital currencies helped allow transactions to be conducted discreetly and without disclosing true identities:

> On each transaction, Western Express earned a commission of between two and five percent. By arranging for these transactions to be conducted in unregulated digital currencies, which were then exchanged for other unregulated currencies, and by knowingly permitting the transactions to be conducted using aliases, Western Express helped the participants avoid detection by governmental regulatory authorities, while itself profiting at each stage of the illegal process.[33]

In the *Western Express* case, the alleged crimes were financial. However, similar methods that exploit the decentralized nature of today's networks could be used to move money to or within a

terrorist organization, to carry out money laundering, or to support other types of criminal enterprises. Indeed, the April 2011 *Western Express* opinion addressed the broader implications of the Internet with respect to criminal organizations:

> Before the advent of widespread use of the Internet, organized criminal organizations were always tangible entities whose location could be pinpointed and whose members could generally be found in relatively close proximity to each other and their victims. The Internet has provided an extraordinarily useful new tool for criminals to perpetrate crimes in entirely new ways.[34]

The combination of MMT and mobile phone networks offers another "extraordinarily useful new tool for criminals to perpetrate crimes in entirely new ways." With the spread of MMT, the network of devices available for possible use in illicit financial transactions includes not only every Internet-connected laptop computer, but almost every mobile telephone as well. In 2010 alone, there were more than 1.6 billion mobile devices sold worldwide,[35] a remarkable number that corresponds approximately to one mobile device sale for every three people in the world aged 15 or over.[36] Notably, 81 percent of the mobile devices sold in 2010 were not smartphones[37]—an important consideration for MMT, which is designed to be usable through basic phone keypad entries.[38]

The Way Forward

Measurement of financial activity, whether at the macro level in terms of GDP or at the micro level in terms of specific transactions, has always been a difficult and highly error-prone exercise. Analysts at the CIA provided a GDP per head figure in the 1986 World Factbook for East Germany that was $100 higher than that of West Germany—a result that defied common sense and that was later attributed to a significant miscalculation of East German economic output.[39] Despite the dogged attempts by financial analyst Harry Markopolos[40] to alert the Boston and New York offices of the Securities and Exchange Commission to Bernard Madoff's impossible and impossibly consistent returns on investment, only when access to capital dried up during the 2008 financial crisis did Madoff's Ponzi scheme collapse. And, the 2008 financial

crisis illustrated that the economic picture constructed by the organs of the U.S. government tasked with financial and commercial measurement, oversight, and regulation can have significant blind spots.

These examples illustrate that the barriers to observing financial activity can be organizational as well as technological. Accordingly, successfully addressing the complexities of illicit financial transactions in cyberspace will require structural and technological steps taken by regulatory, intelligence, and law enforcement agencies, as well as the private sector.

The framework for interagency and international cooperation and regulation, which was largely drafted in a world before social networking, peer-to-peer networks, and the Internet itself, needs to be modified to address a financial environment in which technologies to facilitate illicit financial activity are proliferating. This means recognizing that multiple stakeholders in government and the private sector will need to collaborate and cooperate on evaluating new financial technologies and their potential for abuse, particularly by transnational terror and criminal organizations.

Fostering Self-Regulation

One potentially effective alternative to externally imposed regulation that is likely to gain support from the financial community is collaborative self-regulation with input from government. A recent paper from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a key global player in electronic transactions, acknowledged a "need to explore collaborative solutions . . . to address key regulatory challenges—in particular, to exploit open, flexible, standards-based solutions." The paper goes on to assert the need for entity identification and the capacity to understand which identities are transacting, stating:

> A key and tangible example is entity identification. In normal times this is a dull subject: the industry has muddled along for years with multiple identification systems, creating a bonanza for vendors offering data cross-referencing services. This situation now has to change, however, because the regulatory imperative for

> transparency dictates that more transaction-related information (especially about derivatives) must be supplied to regulators for risk management purposes (as well as the more traditional market abuse monitoring).[41]

While the above language emphasizes derivatives, the broad call for more transaction-related information has direct application to the tracking of illicit transactions. As an entity that has focused on international financial transactions for nearly four decades,[42] SWIFT has a wealth of experience that can be extremely valuable in addressing new modes of money movement. Self-regulation in SWIFT is aided by the common use of a proprietary communications platform by more than 9,000 banking organizations in more than 200 countries.[43]

It is also important to advocate for appropriate forms of self-regulation by MMT service providers, but**,** in doing so**,** to recognize how different that industry is from the traditional banking industry. While traditional banks have a common platform in SWIFT, MMT involves multiple platforms. In addition, while SWIFT participants are often traditional banks, MMT is rapidly turning companies originally structured to deliver mobile voice, data, and video into the primary, and often only, banking platforms for millions of people. MMT service providers do not have a decades-long institutional heritage of developing and deploying systems to identify illicit financial transactions.

Procedures for analyzing MMT transactions of critical national security importance need to be set up well in advance of their use. If, for example, the process of investigating information suggestive of an imminent terrorist threat calls for following a specific movement of money from a source in Europe through a series of MMT transactions, the ability to identify the chain of custody as the money moves in hours or days instead of weeks or months could prove critical.

Collaborative mechanisms should be established not only within but also across the various industries involved in the movement of money. This can enable the MMT providers, the traditional banks, Internet service providers, and governments to track illicit financial flows that may attempt to hopscotch across five, 50, or 500 intermediate points and**,** thus, to counter

obfuscation strategies that would have been prohibitively complex only a few years ago but are within easier reach today.

Government/Industry Collaboration

In addition to fostering self-regulation within the various industry sectors involved in the movement of money, the U.S. government should establish an interagency government/industry working group or expand the charter of an existing group to focus specifically on emerging financial threats. This group should include intelligence and law enforcement agencies as well as private sector participation from the banking industry and Internet-based businesses**,** including companies that provide or facilitate the use of virtual currencies.

Several existing efforts provide good examples to serve as models or perhaps to play a role in this effort. In December 2010, the National Institute of Standards and Technology, the Science and Technology Directorate of the Department of Homeland Security, and the Financial Services Sector Coordinating Council[44] announced a collaboration[45] to jointly, among other things, "identify and overcome cybersecurity vulnerabilities" and "develop more efficient and effective cybersecurity processes that benefit critical financial services functions and may also benefit other critical infrastructures."[46] Another potential model can be found in the FBI's Business Alliance and Academic Alliance partnerships[47] that engage the American business and academic communities on issues of counterintelligence. While the issues in both cybersecurity and counterintelligence can be different in nature and scope from those involved in tracking illicit financial transactions, there are clear areas of overlap as well. For example, identifying and eliminating vulnerabilities in financial transactions systems that might be exploited to delete or alter records of illicit transactions falls under the umbrella of cybersecurity.

Technology

Technology itself is a critical aspect of the solution in several respects. First, government agencies need to maintain an understanding of the novel methods being used to move money. On June 14, 2011, Bitcoin open source project lead Gavin Andresen gave a presentation to a CIA

conference on emerging technologies.[48] Afterward, Andresen had little to say about the meeting other that it "went well."[49] While there was ample speculation as to why Andresen was there, even on Andresen's own forum, the fact that the visit occurred shows that the importance of understanding virtual currencies—and by extension, the wider set of methods that can be used to mask illicit financial transactions—is understood in the intelligence community.

Second, information processing methods that can appropriately detect and trace illicit financial transactions should be developed or, if they exist already in other fields or applications, adopted. One useful precedent lies in methods for anonymizing customer data to allow analysis while simultaneously preserving privacy in more traditional consumer Internet applications.[50] Similarly anonymized data could be generated for transactions conducted using MMT or virtual currencies, and only under proper legal authority could attempts be made to reduce the anonymity of a particular transaction.

Another set of relatively low-tech but still useful solutions pertains to systems that can monitor the premises where MMT agents conduct business. Digital image and video recording is now routinely used in venues as diverse as banks, stores, and taxis. A properly designed system could aim to ensure that cash could only be accepted or disbursed when both the agent and the person providing or accepting the cash were on video. Even though there are various ways a video system could be temporarily disabled or circumvented, it could still provide a disincentive for the conduct of illicit transactions, either with or without agent complicity. As an ancillary benefit, such a system would also increase safety for agents.

Cultural Changes

Cultural shifts within government agencies are another important part of the solution. In many agencies, resources are associated with static, defined categories, strategic shifts are heavily scrutinized both internally and externally, and embracing new technology and new approaches can be politically risky. These characteristics are poorly suited to tracking criminal activity by entities that operate in borderless, streamlined, nonsystematic, multidisciplinary ways.[51] As a recent paper on the fight against terror observed, terrorists "are loosely organized into myriad

cells and flexible networks" and "have virtually no infrastructure for allied forces to target, and their capabilities outlast their leaders,"[52]—a description that needs only slight modification to be an apt description of the networks that are emerging to support obfuscated financial transactions on the Internet.

In particular, the concept of asymmetry, which is well recognized in the intelligence and military communities,[53] should be explicitly considered with respect to illicit financial transactions. One of the most important tools in addressing these issues relates to defining new ways to acquire and share information about these transactions. In doing so, however, it is important to also avoid creating systems that expose information to such an extent that it is more likely to be improperly divulged, as was the case with the leaks of classified information on Wikileaks.

Privacy

Finally, any discussion of acquiring and sharing information aimed at combating illicit financial activity conducted using new technologies will involve the issue of privacy rights. As the recent struggle to pass a House of Representatives bill that would have required Internet service providers to store certain types of information for 18 months shows,[54] there are highly divergent views in the legislative and broader community on how to achieve the proper balance between preserving privacy and preventing criminal activity.

There are no easy answers regarding how to achieve this balance. However, those involved in developing solutions to the challenges posed by illicit financial transactions can assist the legislative process by explaining the types of information available under different monitoring models and the extent and manner to which that information could possibly be tied to specific transactions or individuals. While this will not eliminate the existence of highly divergent views on privacy, it will at least help ensure that decisions regarding what solutions to implement are made with an informed understanding of their privacy implications.

Conclusions

For the United States to ensure its national and financial security, the ability to understand the massive flow of digital information that is the global financial system today, from micro to macro, and from *baht* to Bitcoins, is of fundamental importance. Where once the numbered Swiss bank account, the wire transfer to a shell corporation, or, as in *All the President's Men*, a paper bag containing $25,000 in cash were primary means for covert financial activity, the Internet and mobile phone networks are the potential setting for a vastly expanded set of new, digital avenues for conducting hidden transactions.

Given the rate of change of the digital landscape, any set of solutions constructed based on a single snapshot in time will quickly become obsolete. However, by creating the collaborations, regulatory frameworks, and technologies that reflect today's more fluid and diverse financial transaction environment, government and industry will be better positioned to address illicit transactions today and to adapt to address those of the future.

Notes

[1] William Goldman, script for *All The President's Men* (based on the book of the same name by Carl Bernstein and Bob Woodward), Internet Movie Script Database, accessed July 15, 2011, http://www.imsdb.com/scripts/All-the-President's-Men.html.

[2] Hawala is a money transfer system that has its roots in the Islamic world. In a Hawala transfer, money can be provided to an operator in one country and disbursed to the recipient by an operator in another country. See "Hawala Definition," *Duhaime Legal Dictionary*, http://www.duhaime.org/LegalDictionary/H/Hawala.aspx.

[3] Nikos Passas, "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?," Special Issue: Regulation, Risk and Corporate Crime in a "Globalised" Era, *Risk Management* 5, no. 2 (2003): 49-59.

[4] Kim Zetter, "Bullion and Bandits: The Improbable Rise and Fall of E-Gold," *Wired*, June 9, 2011, http://www.wired.com/threatlevel/2009/06/e-gold/all.

[5] "Digital Currency Business E-Gold Indicted For Money Laundering And Illegal Money Transmitting," U.S. Department of Justice, last modified April 27, 2011, accessed June 23, 2011, http://www.justice.gov/criminal/cybercrime/egoldIndict.htm.

[6] Ibid.

[7] Ibid.

[8] Robert Lemos, "E-Gold pleads guilty to money laundering," *SecurityFocus*, last modified July 23, 2008, accessed July 23, 2010, http://www.securityfocus.com/news/11528.

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," accessed July 23, 2011, http://www.bitcoin.org/bitcoin.pdf.

[10] Annie Lowrey, "My Money Is Cooler Than Yours: Why the new electronic currency Bitcoin is a favorite of libertarian hipsters and criminals," *Slate*, last modified May 18, 2011, accessed July 16, 2011, http://www.slate.com/id/2294980/.

[11] Detailed charts regarding recent bitcoin transactions and other statistics are available at *bitcoin charts*, accessed July 23, 2011, http://bitcoincharts.com/markets/.

[12] Michael Protos, "Digital currency makes cocaine and heroin deliveries as easy as Domino's," *Government Computer News*, last modified June 9, 2011, accessed July 17, 2011, http://gcn.com/articles/2011/06/09/bitcoins-digital-currency-silk-road-charles-schumer-joe-manchin.aspx?s=gcndaily_100611.

[13] "Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs," press release from the office of Senator Joe Manchin (D-W.V.), last modified June 6, 2011, accessed July 17, 2011, http://manchin.senate.gov/public/index.cfm/press-releases?ContentRecord_id=aeae6e96-7d88-4fed-811b-f0d7f3bc1636&ContentType_id=ec9a1142-0ea4-4086-95b2-b1fc9cc47db5&Group_id=e3f09d56-daa7-43fd-aa8b-bd2aeb8d7777.

[14] BK Linden, "Q1 2011 Linden Dollar Economy Metrics Up, Users and Usage Unchanged" *Second Life*, last modified May 6, 2011, accessed August 1, 2011, http://community.secondlife.com/t5/Featured-News/Q1-2011-Linden-Dollar-Economy-Metrics-Up-Users-and-Usage/ba-p/856693.

[15] Edward Castronova, "A cost-benefit analysis of real-money trade in the products of synthetic economies," *Info* 8, no. 6 (2006): 51-68.

[16] Richard Heeks, "Current Analysis and Future Research Agenda on 'Gold Farming': Real-World Production in Developing Countries for the Virtual Economies of Online Games" (IDPM Working Papers, Institute for Development Policy and Management, School of Environment and Development, University of Manchester, U.K., 2008): 2.

[17] Ibid., 64.

[18] "Samoa," *CIA World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/geos/ws.html.

[19] Choe Sang-Hun, "Seoul Warns of Latest North Korean Threat: An Army of Online Gaming Hackers," *New York Times*, last modified August 4, 2011, accessed August 5, 2011, http://www.nytimes.com/2011/08/05/world/asia/05korea.html.

[20] Ronny Kerr, "Zynga to make $500 million for Facebook in 2011," Vator News, accessed July 7, 2011, http://vator.tv/news/2011-07-07-zynga-to-make-500-million-for-facebook-in-2011.

[21] Justin Smith and Charles Hudson, "Inside Virtual Goods: The U.S. Virtual Goods Market 2010-2011," *Inside Network*, accessed July 22, 2011, http://www.insidevirtualgoods.com/us-virtual-goods/.

[22] "Mobile money users in India to reach 10 crore by 2015," *EE Times India*, last modified June 28, 2011, accessed July 17, 2011, http://www.eetindia.co.in/ART_8800645790_1800005_NT_8f80498c.HTM.

[23] "M-Pesa Moved Sh727 Billion Last Year," *Mobile Money Africa*, last modified July 5, 2011, accessed July 17, 2011, http://mobilemoneyafrica.com/?p=3757. The annual total of 727 Kenyan shillings corresponds to a daily average of 2 billion Kenyan shillings. The corresponding average daily volume figure of over $24 million is a conservative calculation using an exchange rate of 81 Kenyan shillings to the dollar. During 2010, the exchange rate varied from about 75 to about 82 shillings to the dollar and was below 81, often by a substantial amount, for much of the year. See "US Dollar (USD) in Kenyan Shilling (KES)," *Google Finance*, http://www.google.com/finance?q=USDKES for historical exchange rates between the two currencies.

[24] William Jack and Tavneet Suri, "The Economics of M-PESA: An Update," MIT, last modified October 2010, accessed July 17, 2011, http://www.mit.edu/~tavneet/M-PESA_Update.pdf.

[25] "Savings" was defined in the MIT survey as holding funds for more than 24 hours.

[26] Biodun Coker, "Safaricom's mobile money services rakes in N1.34trn," *BusinessDay*, last modified July 8, 2011, accessed July 17, 2011, http://www.businessdayonline.com/NG/index.php/markets/companies-and-market/24274-safaricoms-mobile-money-services-rakes-in-n134trn.

[27] Marina Solin and Andrew Zerzan, "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks," The GSM Association, last modified January 2010, accessed July 17, 2011, http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool10.11.GSMAMethodology-AssessingAMLRisk/$FILE/Tool+10.11.+GSMA+Methodology+-+Assessing+AML+Risk.pdf.

[28] "About Us," *GSM World*, accessed August 1, 2011, http://www.gsmworld.com/about-us/index.htm.

[29] Solin and Zerzan, "Mobile Money," 16.

[30] Ibid., 17.

[31] "M-PESA Agents," Safaricom, http://www.safaricom.co.ke/index.php?id=252.

[32] People v. Western Express Intl., Inc., N.Y. Slip Op 03136 (App. Div., 1st Dept. 2011).

[33] "Decision denying motion to dismiss appeal," New York Supreme Court, Appellate Division, First Department, last modified April 19, 2011, accessed July 20, 2011, http://www.courts.state.ny.us/REPORTER/3dseries/2011/2011_03136.htm.

[34] Ibid.

[35] "Gartner Says Worldwide Mobile Device Sales to End Users Reached 1.6 Billion Units in 2010; Smartphone Sales Grew 72 Percent in 2010," Gartner, Inc., last modified February 9, 2011, accessed July 21, 2011. http://www.gartner.com/it/page.jsp?id=1543014.

[36] The CIA World Factbook states that 73.8 percent of the global population of 6.9 billion is aged 15 or over. See "World," CIA World Factbook, accessed July 21, 2011, https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html.

[37] "Worldwide Mobile Device Sales," Gartner.

[38] Sending money in M-PESA is accomplished by selecting a menu option on the phone, entering the recipient's phone number, and a PIN. A confirmation is sent to both the sender and recipient via SMS. See "Send (Transfer) Money," Safaricom, accessed July 22, 2011, http://www.safaricom.co.ke/index.php?id=268.

[39] The CIA's economic analysts charged with estimating the economic output of the two Germanys employed different methodologies, and apparently did so in a state of relative isolation from one another. See "The Tyrannical Numbers," Central Intelligence Agency, last modified July 7, 2008, accessed July 19, 2011, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/cia-assessments-of-the-soviet-union-the-record-versus-the-charges/tyran.html.

[40] Ross Kerber, "The Whistleblower," *The Boston Globe*, last modified January 8, 2009, accessed July 16, 2011, http://www.boston.com/business/articles/2009/01/08/the_whistleblower/?s_campaign=8315.

[41] "Facing the Unknown: Building a strategy for regulatory compliance in an uncertain landscape," SWIFT white paper, last modified June 2011, accessed July 19, 2011, http://www.swift.com/resources/documents/SWIFT_Regulatory_White_paper_201106_FINAL.pdf.

[42] SWIFT was established in the early 1970s. See "SWIFT History," SWIFT, accessed July 22, 2011, http://www.swift.com/about_swift/company_information/swift_history.page.

[43] "Company Information," SWIFT, accessed July 22, 2011, http://www.swift.com/info.

[44] FSSCC members include many of the largest companies in the American financial industry. See "Council Members," Financial Services Sector Coordinating Council, accessed July 22, 2011, https://www.fsscc.org/fsscc/about/members.jsp.

[45] Elizabeth Montalbano, "Government, Financial Industry Launch Cybersecurity Collaboration," *InformationWeek*, December 7, 2010, accessed July 22, 2011, http://www.informationweek.com/news/government/security/228600170.

[46] "Memorandum of Understanding Between Department of Homeland Security Science and Technology Directorate and Department of Commerce National Institute of Standards and Technology and Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security," last modified December 2010, accessed July 22, 2011, http://www.whitehouse.gov/sites/default/files/microsites/ostp/_FSSCC_DHS_NIST_MOU_12062010.pdf.

[47] The Academic Alliance includes the National Security Higher Education Advisory Board. See "Counterintelligence Strategic Partnerships," Federal Bureau of Investigation, accessed July 18, 2011, http://www.fbi.gov/about-us/investigate/counterintelligence/strategic-partnerships.

[48] Gavin Andresen, "Gavin will visit the CIA," Bitcoin Forum, posted April 27, 2011, accessed July 14, 2011, http://forum.bitcoin.org/?topic=6652.0.

[49] Gavin Andresen, "@gavinandresen," *Twitter*, accessed July 14, 2011, http://twitter.com/#!/gavinandresen/status/80785477342478336.

[50] Mehmet Ercan Nergiz, Christopher Clifton, and Ahmet Erhan Nergiz, "Multirelational k-Anonymity." *IEEE Transactions on Knowledge and Data Engineering* 21, no. 8 (August 2009): 1104-1117.

[51] Anthony Zinni, "The New World Order," (lecture, Cornell University, Ithaca, NY, April 15, 2008): 11-12, accessed July 14, 2011, http://www.cornell.edu/video/transcripts/20080415-anthony-zinni.pdf.

[52] Diana Raschke, "Asymmetric Warfare Requires Intelligence Community Reorganization," SIGNAL Magazine (AFCEA.org), accessed July 14, 2011, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1553&zoneid=231.

[53] Colin Gray, "Thinking Asymmetrically in Times of Terror," *Parameters* 32, no. 1 (2002): 5-6.

[54] Declan McCullagh, "ISP data retention plan hits Capitol Hill snag," *CNET*, last modified July 12, 2011, accessed July 22, 2011, http://news.cnet.com/8301-31921_3-20078785-281/isp-data-retention-plan-hits-capitol-hill-snag/.