Washington Journal of Law, Technology & Arts

Volume 8
Issue 3 *Mobile Money Symposium*

Article 5

1-1-2013

Privacy and Security Concerns Associated with Mobile Money Applications in Africa

Andrew Harris

Seymour Goodman

Patrick Traynor

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 3 MOBILE MONEY SYMPOSIUM 2013

PRIVACY AND SECURITY CONCERNS ASSOCIATED WITH MOBILE MONEY APPLICATIONS IN AFRICA

Andrew Harris, Seymour Goodman, and Patrick Traynor[*]

Cite as: 8 WASH. J.L. TECH. & ARTS 245 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1198

ABSTRACT

The rapid adoption of mobile money use in Africa raises concerns regarding the privacy and security of users, particularly in light of Financial Action Task Force recommendations requiring user transparency and the collection of transaction data. The transparency required of the now-financially-included—particularly in nations with weak adherence to the rule of law and limited privacy protections—leaves users vulnerable to abuse. Further, the increasing complexity of mobile phone use that is indicative of mobile money applications raises concerns regarding Africa's preparedness for heightened security threats that come hand in hand with increased use. To address these problems, the authors of this Article recommend specific policy actions by African nations to improve consumer privacy and cybersecurity, supported by policies of

---

[*] Andrew Harris is a Foreign Affairs Officer at the U.S. Department of State. The views expressed in this paper are his own, and do not necessarily reflect those of the U.S. Department of State or the U.S. Government.

Seymour Goodman is a Professor in the Sam Nunn School of International Affairs and the College of Computing at the Georgia Institute of Technology.

Patrick Traynor is an Assistant Professor in the College of Computing at the Georgia Institute of Technology.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean's Innovation Fund.

industrialized nations like the United States and responsible corporate behavior.

TABLE OF CONTENTS

INTRODUCTION

Over the last decade, mobile telephony has enjoyed phenomenal adoption rates across most of Africa. Since 2005, there has been a five-fold increase in the number of African mobile phone subscriptions resulting in 53.1 mobile phone subscriptions per 100 inhabitants in 2011.[1] While other areas of the world have adopted mobile phones to an even greater degree, the relative impact in Africa, where fixed telephone lines are available to less than 2 percent of the population, is perhaps greater than anywhere else. As the primary means of communication for most Africans, mobile phones have become a source of significant economic growth and a platform for innovation. One of the most dynamic of these innovations has been mobile money, the use of mobile phones to purchase goods or services through funds connected to the user's account. With a broad base of mobile phone users

[1] *Key Global Telecom Indicators for the World Telecommunication Service Sector*, INT'L TELECOMM. UNION, http://www.itu.int/ITU-D/ict/statistics/at_glance/keytelecom.html (last visited July 28, 2012).

already in place, the widespread adoption of mobile money could have enormous positive impacts across Africa. On a continent with too few banking options necessary for a dynamic and modern economy, mobile money has the potential to address long-existing gaps in African economies.[2] Unfortunately, the rapid growth of mobile telephony in Africa has not been accompanied by appropriate consideration for privacy and security concerns, opening the door for abuse and erosion of the application's utility.

In light of limited privacy protections and a vulnerable cyber environment, the requirements of the Financial Action Task Force (FATF) raise a number of concerns associated with mobile money in Africa. As a financial service, the FATF Recommendations apply to mobile money just as with traditional banking services. The global effort to combat money laundering and terrorism is as applicable to mobile money services as to traditional banking. From a general security perspective, the identification, verification, and reporting requirements of the FATF Recommendations are a positive effort to ensure that mobile money applications do not become tools for money laundering. The requirements for user transparency, however, introduce a potential problem. FATF Recommendation 10 states that financial institutions must perform Customer Due Diligence, which includes confirming the identity of clients and scrutinizing client transactions.[3] Further, Recommendation 11 requires financial institutions to maintain records of all transactions for five years, "to enable them to comply swiftly with information requests from the competent authorities."[4] These requirements for transparency and record keeping pose a number of user privacy concerns for mobile money applications in Africa, particularly in those nations with weak adherence to the

---

[2] *Mobile Money in Africa: Press 1 for Modernity*, THE ECONOMIST (Apr. 28, 2012), http://www.economist.com/node/21553510.

[3] FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS 14-15 (2012), *available at* http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf.

[4] *Id.* at 15.

rule of law and limited privacy protections. Further, the increasing complexity of mobile phone use that is indicative of mobile money applications raises concerns regarding Africa's preparedness for heightened security threats that come hand in hand with increased use.

I. PRIVACY CONCERNS: TRANSPARENT USE WITHOUT PRIVACY PROTECTION

According to FATF Recommendations 10 and 11, financial institutions should not allow customers to conduct business anonymously; and they must maintain user transaction records for five years. In most traditional banking settings, this requirement is both sensible and non-controversial. It does, however, raise significant questions for African users of mobile money services, particularly considering the limitations of privacy protections in Africa. For instance, a recent UN report noted that amongst the members of the East African Community—Burundi, Kenya, Rwanda, Tanzania, and Uganda—there is no legislation "that clearly defines who can get access to a mobile money trail, and how, when or under what conditions such access may be obtained."[5] Inadequate privacy protections can lead to abuse by governments and data brokers as well as leave personal information susceptible to theft or leakage, ultimately damaging user trust and limiting adoption and use.

A. Limited Privacy Protections

There are a number of reasons to explain the limits of privacy protection in Africa. First, a strong communitarian strain exists throughout much of Africa. This mindset deemphasizes the rights of individuals in favor of those of community. In such a context, the privacy of individuals is given little consideration.[6] Second,

[5] U.N. CONF. ON TRADE & DEV., *Mobile Money for Business Development in the East African Community* 20 (2012), *available at* http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf [hereinafter UNCTAD].

[6] *See* Seymour Goodman & Andrew Harris, *Emerging Markets: The Coming African Tsunami of Information Insecurity*, COMM. OF THE ACM, Dec.

traditional economies with limited electronic communication and commerce have less need for individual privacy protection as there are few means to collect, use, and exploit sensitive information. Until very recently, the vast majority of Africans did not engage in data compiling transactions. For both of the reasons above, there are few established legal protections in African nations. Most nations do not formally recognize a right to personal privacy, and most do not have laws or regulators in place to monitor abuse.[7] Compounding the lack of legal protections is the relative absence of public interest groups to monitor government behavior, propose public policy, and promote awareness. This all leads to situations where serious abuses can occur with little impediment. Even in South Africa, where some legal protections are in place, illegal interception and abuse of electronic communications by intelligence agencies is routine.[8] While a limited privacy protection regime may have caused little concern just a short time ago, the African boom in mobile telephony significantly heightens the risk to consumers operating in an ecosystem without protection.

B. Potential for Abuse

In the context of limited privacy protections and because FATF requires identity verification and data collection, African mobile money users may find their privacy threatened by governmental and corporate abuse. In cash-based economies, the spending and savings activities of individuals are known to an interested third party only with great effort. This is the environment that most Africans have come to understand, developing social behaviors reflective of spending that is anonymous to government and corporate entities. Despite a lack of privacy protections, the

---

2010, at 24, *available at* http://dl.acm.org/citation.cfm?id=1859215&dl=ACM&coll=DL&CFID=111892502&CFTOKEN=79495868.

[7] *See* Hanno N. Olinger et al., *Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa*, 39 INT'L INFO. & LIBR. REV. 31 (2007).

[8] Heidi Swart, *Secret State: How the Government Spies on You*, MAIL & GUARDIAN (Oct. 14, 2011), http://mg.co.za/article/2011-10-14-secret-state/.

inherent anonymity of cash prevents any other entity from knowing the extent of an individual's transactions. Due to FATF requirements, however, the service provider can and must record every detail of a user's transactions in a mobile money environment. It is also important to note that the initial wave of mobile phone adoption was anonymous, as the vast majority of users purchased and used unregistered pre-paid phones. Many African nations are now reversing this initial trend by requiring SIM-card registration, further reducing anonymity and potentially limiting private use.[9] The availability of transaction data opens the door for abuse by an unscrupulous government, which could gain access to transaction records with little effort.[10] This information could then be used in a number of ways to harass, intimidate, or manipulate the violated citizen.

Corporate abuse of personal information can have similarly insidious effects in a mobile money environment without legal safeguards. Mobile money services necessarily operate in a data-rich environment that creates incentives for the commoditization of personal information and targeted advertising. A fully employed mobile money ecosystem can include a mobile network operator, financial institution, trusted service manager, marketer, retailer, and the customer. Each of these entities (other than the customer) has a growing interest in collecting personal information tied to mobile money transactions. With so many interested parties and little consumer protection, the opportunities for data leakage and subsequent abuse are abundant.[11] Liberal collecting and sharing policies result in electronic dossiers useful not only for providing targeted advertising, but also for making decisions regarding

[9] *See* Chikaodili Juliet Hemeson, Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective (Jan. 8, 2012), *available at* http://ssrn.com/abstract=1982033.

[10] *See* Louis de Koker & Nicola Jentzsch, Financial Inclusion and Financial Integrity: Aligned Incentives? (July 2011) (unpublished conference paper, The Shadow Economy, Tax Evasion and Money Laundering Conference), (on file with the University of Münster), *available at* http://dro.deakin.edu.au/view/DU:30041719.

[11] *See* Andrew Harris et al., *Emerging Privacy and Security Concerns for Digital Wallet Deployment*, *in* PRIVACY IN AMERICA: INTERDISCIPLINARY PERSPECTIVES 185 (William Aspray & Philip Doty eds., 2011).

employment or credit worthiness as well as for committing fraud.

It is important to note that the threats of data leakage are amplified in a mobile money environment because how we spend is a valuable predictor of who we are and how we will spend or possibly otherwise behave in the future. Since FATF requires financial institutions to record user transactions, this information is necessarily compiled and available for use. The ability to connect basic personal information to spending records obtained through mobile phones has great commercial use—and potentially misuse. In places where mobile money is not yet extensively used, like North America and Europe, a spending record connected to the user's mobile phone is less accessible or not available at all, so nations in these regions have not yet needed to wrestle fully with the implications of mobile money data. But in Africa, mobile money data sets are quickly growing. As Africans also begin to use their phones to access the Internet, the incentives to commoditize this data will grow and present challenges yet unseen in Western nations.

The potential for abuse of private information can harm not only the violated citizens, but also the overall economy. If governments and businesses abuse users' trust, they will restrain adoption and limit the utility of mobile money, thus limiting the application's utility and holding back their countries. Two of the authors witnessed a good illustration of this at a cybersecurity conference for East African government officials in Kenya.[12] During a discussion of African broadband adoption, a law enforcement official from one of the participating countries stood up to proclaim the virtues of Facebook for monitoring and catching criminals. Such behavior can have a chilling effect on technology adoption, and the brazenness of the statement in a room full of government lawyers and officials demonstrates the lack of regard for privacy that some in government demonstrate. Calls to monitor social media are certainly not confined to Africa, but when proposed in industrialized nations, monitoring is suggested only within tight restrictions and a devotion to the rule of law.[13] In most

[12] East African Cyberspace Workshop, Nairobi, Kenya (July 25-27, 2011).

[13] *See* SIR DAVID OMAND ET AL., # INTELLIGENCE (2012), *available at*

African nations, there is little to stop governments or corporations from pushing the boundaries of acceptable use with regards to revealing mobile money data. If widespread abuse becomes commonplace, users may walk away from mobile money and all its enormous benefits.

II. SECURITY

The growth of mobile money is indicative of a larger trend of greater and more sophisticated mobile telephony use—a trend that many African nations are ill prepared for, for a host of reasons. As user experiences grow richer and smart phone adoption increases—a trend well underway[14]—mobile phones will become a more appealing target to a wide range of cyber threats. The FATF requirements contribute to this trend by requiring user identification and transaction recording, meaning that mobile phones become directly linked to financial accounts and rich data sets, increasing the desirability for hackers. Smart phones are just as susceptible—if not more so—to the same viruses, worms, and botnets that plague PCs.[15] In this environment, the user might lose more than just personal information, but notably money, and be susceptible to other forms of crime through exposure via his mobile device. The FATF requirements are generally beneficial for security issues considering their focus on the serious threats associated with terrorism, money laundering, and weapons proliferation. Further, FATF may generate constructive pressure by forcing regulators to more deeply consider the range of risks associated with mobile money. The extent of African cybersecurity deficiencies is significant enough, however, that FATF requirements alone—which do not address cybersecurity—are unlikely to compel improvements. Without proper attention to

---

http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327.

[14] *Samsung Sees Smartphones Leading African Growth*, REUTERS (Mar. 22, 2012), http://www.reuters.com/article/2012/03/22/us-samsung-africa-id USBRE82L0RU20120322.

[15] GA. TECH INFO. SEC. CTR., EMERGING CYBER THREATS REPORT FOR 2009 5 (2008), *available at* http://www.gtisc.gatech.edu/pdf/CyberThreatsReport 2009.

security on the devices that enable mobile money, the user may be vulnerable to criminal activity.

A. Cybersecurity Limitations

This vulnerability is particularly pronounced in the African context due to a set of unique challenges that amplify the growing insecurity threat. First, most African nations have inadequate laws and institutions to confront serious cyber threats.[16] While various efforts are underway to encourage the adoption of national legal frameworks, even these steps have limited effects without institutions in place to monitor networks and remediate threats. Computer Emergency Response Teams (CERTs) have become valuable assets for performing these necessary functions, but they are either lacking or in nascent stages across much of Africa. Beyond the institutional and legal inadequacy, African nations suffer from a shortage of trained public-sector professionals needed in both the policy and operational spaces. This is a common problem for all nations, but one that is exacerbated in Africa where the number of individuals with advanced information security knowledge is relatively lower than elsewhere. Those with such knowledge tend to be drawn to the higher paying private sector, leaving little expertise for governments. Without capable CERTs in place with the commensurate technical expertise to operate them, African networks are more vulnerable to cyber threats, leaving mobile money users vulnerable to attack and fraud.

Awareness is another crucial piece of the security equation. The rapid adoption of mobile phones and applications like mobile money has placed these useful tools in the hands of users with little prior experience with technology. Users with limited digital literacy are more likely to be unaware of cyber threats, placing

[16] Eric Agwe-Mbarika Akuta et al., *Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice*, 1 J. PEACE, GENDER & DEV. STUDIES 129, 131 (2011), *available at* http://interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al.pdf.

themselves and the networks at greater risk.[17] Lack of cyber awareness is certainly a leading cause of infection across the globe, but African nations have a higher proportion of low-capacity users, and thus more users unfamiliar with the best practices that can limit vulnerability.[18] Awareness issues extend beyond the average user into the corporate setting as well. Because most African companies have evolved in an environment of limited interconnectivity, they have had little reason to focus on cybersecurity measures and best practices. But now that broadband connectivity is growing, it is essential that measures such as software standardization and network monitoring be implemented. With lax operating procedures in place, corporate behavior can open threat vectors, infecting networks and endangering users. It is important to remember that a user of a mobile money application connected to an infected network is far more vulnerable than a user engaging in basic web browsing and email. It is therefore essential that heavy network users such as corporations are actively protecting the network.

Because the Internet knows few political boundaries, international cooperation on cybersecurity issues is a necessity, but few African nations are engaged in cross border law enforcement efforts. Only South Africa and Senegal have joined the Council of Europe's Convention on Cybercrime, the most significant international law enforcement effort to address cybercrime.[19] Further, there are limitations to the assistance developed nations are able and willing to provide. First, it is uncommon for developed nations to devote significant resources to cyber assistance. Most assistance funds are directed at more traditional development projects such as health or education. Second, details

[17] *See* Steven Furnell et al., *Security Beliefs and Barriers for Novice Internet Users*, 27 COMPUTERS & SECURITY 235 (2008).

[18] Marthie Grobler & Joey Jansen van Vuuren, Broadband Broadens Scope for Cyber Crime in Africa (Aug. 2010) (unpublished conference paper, Info. Security for S. Afr. Conf.), *available at* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5588287&contentType=Conference+Publications&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A5588257%29.

[19] See the Council of Europe Convention on Cybercrime, *available at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

of cybersecurity efforts and methodologies are often considered classified or restricted information in western nations. These nations are reluctant or completely unable to cooperate with nations they regard as having lax information security standards. All too often this is the case in the African context, making western governments unlikely to meaningfully share information and cooperate with African states.

Finally, the state of cybersecurity in Africa is hindered by the low prioritization from national leaders. This is of course understandable in the African context where limited resources must first be allocated to address society's most fundamental problems. The low priority for cybersecurity in the face of other pressing issues means that solutions requiring strong governmental direction are absent from most African states, further endangering vulnerable networks and their applications. For this reason, and for the reasons described above, the African continent is likely the least safe place to operate a sensitive application like mobile money. Further, as mobile money grows more popular, it will inevitably become a greater target for criminal activity. If Africa's cybersecurity deficiencies are not addressed in a timely manner, the widespread adoption of mobile money may be accompanied by widespread mobile money abuse.

B. Examples of Specific Mobile Money Threats

Without proper attention to basic security features, mobile money users introduce themselves to numerous threats, the most damaging being the loss of money should an assailant gain physical control of the mobile device. Given that nearly 5 percent of smartphones issued to or used by employees are lost annually[20] and that only 30 percent of users protect their devices with passwords and data encryption,[21] the possibility of someone other

[20] PONEMON INST., THE LOST SMARTPHONE PROBLEM: BENCHMARK STUDY OF U.S. ORGANIZATIONS 2 (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-ponemon-lost-smartphone-problem.pdf.

[21] Carole Theriault, *Survey Says 70% Don't Password-Protect Mobiles: Download Free Mobile Toolkit*, NAKED SEC. (Aug. 9, 2011), http://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-

than a device's owner using it to gain access to mobile money is significant. It should also be noted that such mechanisms only offer protection against unsophisticated attackers. In particular, prior work has demonstrated that a technically adept adversary may be able to take advantage of poor security design within mobile money apps[22] or simply bypass poorly implemented encryption.[23] Accordingly, it is critical that both users and financial institutions consider a range of risk models.

More subtle digital attacks against users are also possible. For instance, mobile money applications could also be used to isolate or burden a potential target. Malicious applications within the phones themselves could easily target unsuspecting users. For instance, a "trojaned" application could simply fail to allow transactions from a target's phone to clear, dramatically limiting the target's ability to make purchases or move funds. Alternatively, the application could illegally track all the purchases made by the target, potentially giving the adversary information about the target's strategies and physical location. Finally, such an application could make arbitrary purchases on behalf of the target. Given that the avenues to contest the legitimacy of such purchases are generally lacking (e.g., the presence of the correct PIN made with a purchase virtually ensures that liability is held by the target and not their financial institution), such an application could slowly drain funds from the target's account. Performed in an inconspicuous fashion, such purchases would be unlikely to raise alarms in traditional fraud detection systems. With an increasingly appealing target for criminals and an environment of cyber insecurity, African mobile money uses face an uncertain future.

---

toolkit/.

[22] *See* William Enck et al., A Study of Android Application Security (Aug. 2011) (unpublished conference paper, USENIX), *available at* http://static.usenix.org/events/sec11/tech/full_papers/Enck.pdf.

[23] Ina Fried, *At Defcon, Hackers Show How to Hack Your Android Phone Encryption*, ALL THINGS D (July 28, 2012, 6:18 PM), http://allthingsd.com/20120728/at-defcon-hackers-show-how-to-bypass-android-encryption/.

III. WHAT SHOULD BE DONE?

Mobile money has enormous potential for the people and economies of Africa, yet users must ultimately trust the technology if its greatest impact is to be realized. Lurking issues associated with personal privacy and cybersecurity currently threaten that user trust. Both are global problems requiring global solutions with cooperation from all stakeholders.

A. African Solutions

First and foremost, African nations must recognize the importance of digital technologies to the future of their economies. While perhaps one of the most dynamic and compelling, mobile money is just one of many technologies with the power to help transform African economies. With financial resources understandably limited, national leaders should take policy actions that will increase user trust without requiring exceptional monetary and other resource allocations.

Primary amongst these steps is instituting comprehensive but flexible privacy regimes. In reviewing the lack of privacy regulation in East Africa, the United Nations Conference on Trade and Development (UNCTAD) declares that "simple and transparent mechanisms are needed through which users can authorize an entity to access" data associated with mobile money.[24] Individuals should be empowered through national legislation to control their personal information and corporations should be required to use that information only in contextually appropriate ways. Licensing for mobile money services should include explicit rules for the collection and sharing of personal information. Crucially, it is imperative that lawmakers implement comprehensive regulations rather than taking a sectoral approach, as has unfolded in the United States. Sector-specific laws may prove inadequate for converged technologies like mobile money, leaving banks, telecommunications companies, and data brokers

[24] UNCTAD, *supra* note 5, at 20.

with differing requirements leading to inconsistent treatment of user data.[25]

There have been some recent positive steps regarding privacy legislation in Africa. In February 2012, Ghana passed a comprehensive data protection bill establishing users' rights of data access, control, and consent of use.[26] The bill also creates a Data Protection Commission to enforce and regulate the new law.[27] Further, a draft bill in Kenya specific to electronic retail requires user consent for any information sharing.[28] Both are positive steps and serve as recognition from these two nations of the necessity to protect users and promote trust in order to maximize utility of new technologies like mobile money. Further these efforts may serve to encourage other African nations to explore privacy legislation. While protecting citizens should be a primary concern for policymakers, they must also seek balance in any law, working to ensure that new legislation is not overly prescriptive or burdensome for corporations bringing innovative tools to the marketplace. For instance, while many international businesses welcome the European's new privacy plans to streamline privacy rules in a more centralized manner, these same companies also protest the regulation's more stringent guidelines such as the proposal for an individual's "right to be forgotten."[29] While the proper balance between adequate protection and flexible business operations is certainly delicate, African leaders must act in order to ensure the ultimate success of mobile money.

To address the lack of technical capacity, policy makers should stress the study of security, privacy, computer science and information programs in universities. There is a growing demand for African app developers, and universities will train many of

---

[25] *See* Harris et al., *supra* note 11.

[26] Daily Guide, *Data Protection Bill Passed*, GHANAWEB (Feb. 10, 2012), http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=229717.

[27] Data Protection Act 843 of 2010 (Ghana), *available at* http://www.parliament.gh/assets/file/Bills/Data%20Protection%20Act,%202010.pdf.

[28] UNCTAD, *supra* note 5, at 20.

[29] *Privacy Laws: Private Data, Public Rules*, THE ECONOMIST (Jan. 28, 2012), *available at* http://www.economist.com/node/21543489.

them. These universities should insist on strong privacy and security backgrounds. These courses of study should be promoted as holding particular import for future development with incentives created to draw in prospective students. To help facilitate a greater emphasis on privacy and security at the university level, policy makers should encourage empowering partnerships with international institutions that excel in the field. For instance, the Rwandan government recently sponsored a Carnegie Mellon University campus in Kigali with the government committing to offer substantial scholarships to qualifying applicants. Carnegie Mellon's Rwanda campus offers Masters of Science in Information Technology with the option to focus on cybersecurity and began classes in the fall of 2012.[30] This action by the Rwandan government demonstrates a clear understanding from national leaders that technological advances must be accompanied with sufficient human capacity. Similar partnerships coupled with the promotion of security and privacy studies can help African nations make strides in addressing human capacity issues.

African application developers and service providers can of course begin to place a greater emphasis on personal privacy and security by designing solutions to protect networks and data and providing users tools to protect themselves and their devices. In considering the problems of transparency in mobile money applications in the African context, developers could explore some of the benefits of e-cash, a primarily conceptual digital currency in which transactions are anonymous and funds cannot be double spent. Bitcoin is the most prominent manifestation of e-cash, although numerous technical and regulatory problems exist with this particular implementation.[31] With proper research, mobile money applications may find some of the principles and features of e-cash useful in introducing layers of anonymity and protection for users. Finally, African nations should commission public awareness campaigns focused on cybersecurity and personal data. With relatively little money, public awareness campaigns can

[30] See Carnegie Mellon University in Rwanda, http://www.cmu.edu/rwanda/.

[31] See Bitcoin Project, http://bitcoin.org/.

increase digital literacy, informing consumers of basic dos and do nots to protect themselves and others.

B. United States Policy

Developed nations should pursue policy solutions as well. The safe and effective employment of mobile money across Africa is clearly in the interest of countries like the United States. Indeed, the United States has a number of applicable polices in place. Joining these policies with specific action to assist African nations can serve to address some of the potential problems. One of the most vocal proponents for a free and open Internet has been Secretary of State Hillary Clinton: "The United States will continue to promote an Internet where people's rights are protected and that it is open to innovation, interoperable all over the world, secure enough to hold people's trust, and reliable enough to support their work."[32] These words have provided leadership for the United States to increase diplomatic pressure on offending governments and raise the costs of bad behavior. Because of her initiative, American embassies are poised to monitor for and respond to governmental abuse of digital technologies like mobile money.

The forward leaning posture of Secretary Clinton should be matched with a clear policy on dual-use technology controls. The U.S. government needs to put careful thought into the export of technologies that can be used to block, monitor, or filter digital content as well as performing more benign and easily marketable tasks. Rebecca MacKinnon points out this fact and criticizes the U.S. government's complicity: "American corporations are major suppliers of software and hardware used by all sorts of governments to carry out censorship and surveillance—and not just dictatorships."[33] Therefore, a policy is needed to sufficiently deter

---

[32] Hillary Clinton, U.S. Sec'y of State, Remarks at George Washington University, Internet Rights and Wrongs: Choices & Challenges in a Networked World (Feb. 15, 2011), *available at* www.state.gov/secretary/rm/2011/02/156619.htm.

[33] Rebecca MacKinnon, *Internet Freedom Starts at Home*, FOREIGN POLICY (Apr. 3, 2012), http://www.foreignpolicy.com/articles/2012/04/03/The_Worlds_

repressive regimes from obtaining these tools and encouraging democratic governments not to abuse the capabilities of dual use technologies. While the United States has taken direct action in some of the most extreme cases, such as President Obama's Executive Order banning the transfer of certain technologies to Iran and Syria,[34] uniform guidance and consistent enforcement would offer more effective protection.

The United States can and should also make efforts to assist African nations protecting individual privacy. The recently released White House Blueprint on Consumer Privacy protection identifies the needs for both consumer control of personal information and for the free flow of international data: "The United States is committed to engaging with its international partners to increase interoperability in privacy laws by pursuing mutual recognition, the development of codes of conduct through multi-stakeholder processes, and enforcement cooperation."[35] If pursued with African partners, this policy can help ensure that African consumers are protected and African economies are equipped to engage in the global digital marketplace.

Finally, the United States—and indeed other developed nations—must begin to prioritize cybersecurity cooperation with Africa. Appropriate high-level U.S. policies are in place,[36] but significant implementation of those policies is yet to occur. The President's *International Strategy for Cyberspace* commits the United States to working with developing countries to build cybersecurity capacity, develop and share best practices, offer cybercrime training, and to develop and deepen governmental ties

---

No_1_Threat_to_Internet_Freedom.

[34] Exec. Order No. 13,606, 77 Fed. Reg. 24,571 (Apr. 22, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-04-24/pdf/2012-10034.pdf.

[35] THE OBAMA ADMIN., THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 31 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[36] *See* THE OBAMA ADMIN., THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

with counterparts and subject matter experts. To adequately achieve these commitments, Congress must first acknowledge and address the global nature of cyber insecurity in Africa. Then, significant additional resources are needed to allow U.S. experts to provide technical assistance to partner nations. Finally, there is a need to reconcile conflicts between the value of information sharing and the necessity of ensuring the integrity of classified material. American action alone cannot address the potential problems facing Africa, but the United States has adopted promising policies in the last few years that can serve to guide both American and global action in providing needed assistance.

C. Public Advocacy and Corporate Responsibility

As new technologies proliferate, particularly in African settings with large populations of users less accustomed to these technologies, it is essential that public advocacy groups focus their attention on possible governmental or corporate abuse. Under the banner of Internet Freedom, human rights groups can monitor for abuse and apply international pressure to those most egregious abusers. Freedom House's "Freedom of the Net" report is an excellent example of such an effort.[37] By reporting broadly on the state of government Internet restrictions, Freedom House is providing an essential tool in helping to hold governments accountable. As African users adopt sophisticated and specific applications like mobile money, similar monitoring of governmental interference in these spaces should be established as well.

Corporate responsibility is another vital piece in ensuring user safety and privacy. Service providers and banks have a responsibility to protect users' data and finances through technical means as well through appropriate behavior and policies that do not expose users to abuse at the hands of repressive governments or unscrupulous third parties. Beyond a moral issue, widespread

[37] *See* FREEDOM HOUSE, FREEDOM ON THE NET 2011: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA (Sanja Kelly & Sarah Cook eds., 2011), *available at* http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf.

adoption of mobile money requires user trust. The necessity of trust should provide sufficient incentive for responsible corporate behavior. A positive example of companies proactively committing to responsible behavior is the Global Network Initiative (GNI), a multi-stakeholder group that includes Google, Microsoft, and Yahoo!.[38] GNI attempts to assist technology companies in protecting privacy and free expression in the face of repressive regimes and can serve as a model for self-organized corporate commitment making. Where corporations are complicit in abuse, other institutions or legal mechanisms, as mentioned above, are appropriate.

CONCLUSION

There can be no doubt about the enormous potential for mobile money in Africa. For a continent plagued by limited banking options, mobile money has in just a short time brought millions to the ranks of financial inclusion. As part of the global effort to counter money laundering and terrorism, FATF requirements demand transparency of all financial services customers, including mobile money. The increased data collection associated with this transparency renders mobile money users in Africa particularly vulnerable to governmental or corporate abuse of the data generated by mobile transactions. Equally troubling are cybersecurity concerns, leaving African mobile money users in a doubly precarious position. Should mobile money platforms come to be inundated with privacy breaches and malware, users will lose trust in the application, reversing adoption trends and eliminating potential gains. It is therefore incumbent for all to act—government, human rights watchdogs, corporations, and individual citizens—to address existing deficiencies and ensure that the power of mobile money will be enjoyed across Africa.

[38] See Global Networking Initiative, http://www.globalnetworkinitiative.org/.