Surveillance & Society

Article | Mobile Money Platform Surveillance

Aaron Martin

Tilburg University, The Netherlands
a.k.martin@uvt.nl

Abstract

Drawing on evidence from Sub-Saharan Africa, this paper explores the various forms of surveillance present on mobile money platforms. At the most basic level, mobile money is the provision of financial services through a mobile device. Over the past decade, these platforms have witnessed astonishing rates of adoption in Kenya, Tanzania, Uganda, Ghana, and elsewhere. While some authors have praised the transformative potential of mobile money, particularly in parts of the world in which large numbers of people remain "unbanked," more critical voices have expressed concerns about the economic risks and regulatory challenges associated with mobile money. This article focuses on an underexplored but nevertheless significant feature of mobile money platforms: the ways in which they facilitate surveillance by service providers and government authorities. Relatively established forms of surveillance include mandates for identifying customers prior to service provision. I also discuss the monitoring of mobile money agents, who receive a commission for turning cash into electronic value (and vice versa). Well-established mobile money providers are said to operate in-house "bank-grade" monitoring systems to identify suspicious transactions and comply with anti-money laundering regulations. Government agencies are also implementing bespoke monitoring solutions in countries where authorities, distrustful of mobile money providers' self-reported data, seek to more stringently enforce regulatory compliance while also maximizing tax revenues from mobile money transactions. An analysis of these different forms of surveillance reveals their multipurpose and multi-scalar nature. I argue that the impacts of mobile money platform surveillance need to be better understood, particularly from a financial inclusion perspective.

Introduction

At the most basic level, mobile money is the provision of financial services through a mobile phone (Donovan 2012: 61), typically via basic mobile devices rather than smartphones. Mobile money works like a simple bank account, with an individual's funds stored in a wallet on their mobile device. Customers are able to visit an agent to deposit or withdraw funds (cash-in/cash-out; i.e., loading value into the mobile money system, and then converting it back out), transfer money to other accounts, and pay for certain goods and services at points of sale. Increasingly, they can also apply for loans through the platform. While Vodafone's M-Pesa, launched in Kenya by Safaricom in 2007, is the most well-known mobile money service, ten years later there were over 276 active services and 690 million registered accounts worldwide—a 25% increase from 2016 (GSMA 2018a: 8). Kendall et al. (2011: 62) argue that mobile money has the potential to become a "catalytic platform" whereby the cash-based financial sector could be fundamentally realigned from being mediated by expensive retail infrastructure to greater use of electronic payments through mobile phones.

Many pundits have praised the transformative potential of mobile money, particularly in parts of the world where large numbers of people remain "unbanked." For the 1.7 billion people globally who remain financially excluded, mobile money is seen as an efficient means of helping people access basic financial

Martin, Aaron. 2019. Mobile Money Platform Surveillance. *Surveillance & Society* 17(1/2): 213-222.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

services. More critical voices have expressed concerns about the economic risks, including how mobile money facilitates "financialization" (Aitken 2017)— that is, how it increases the role of financial motives, markets, actors, and institutions in economic life (Epstein 2005: 3)—or emerging evidence that mobile money encourages over-borrowing (The Economist 2018). Others have explored the regulatory challenges raised by mobile money, such as that historically it was banks, not mobile service providers, which operated the payment systems that were the focus of regulation (Greenacre 2018: 3-6), as well as the limitations of privacy standards in the banking sector to protect mobile money data (Makulilo 2015). Civil society actors have started to examine the risks inherent in the sharing of mobile money data, particularly for vulnerable groups (ICRC and Privacy International 2018: 70-76).

Rather than reiterate these debates, this article addresses an underexplored but nevertheless significant feature of mobile money platforms: the ways in which they facilitate different forms of surveillance. It does so in light of contemporary observations on how "the rapid growth of mobile telephony has enabled the tracking and monitoring of many millions of previously unconnected individuals," particularly across Africa (Donovan et al. 2016: 34).

Mobile money platform surveillance is multipurpose and includes identification requirements for *customers*, aimed at preventing crime; the surveillance of mobile money *agents* by service providers as a means of mitigating fraud; and the monitoring of *transactions* by service providers for anti-money laundering (AML) and combating the financing of terrorism (CFT) and, increasingly, by governments for taxation purposes. This article understands the concept of platform surveillance to include both manual and automated forms of monitoring that are present in the case of mobile money. It is also multi-scalar in the sense that surveillance occurs at different points of intervention and scale (cf. Klauser 2017: 117-118).

In what follows, I analyze the various components of mobile money platform surveillance before turning to a short discussion summarizing the significance of these practices.

Identification Mandates for Mobile Money Customers

Two sets of government identification requirements constitute a form of surveillance of mobile money customers (cf. Lyon 2009). Subscriber Identity Mobile (SIM) registration is a telecommunications regulatory trend that has been widely embraced by governments in Global South contexts based on security and fraud reduction rationales. Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements emanate from an intergovernmental body, known as the Financial Action Task Force, via Central Banks and other financial regulators to mobile money providers at national levels for the purposes of preventing financial crimes. Together, they make the disclosure of one's identity a prerequisite for engagement on a mobile money platform, first, for connectivity and, then, again to activate a mobile money wallet.

SIM Registration

As of February 2018, SIM registration was mandatory in 147 countries worldwide (GSMA 2018). This regulatory trend has been most acute in jurisdictions in Africa (Donovan and Martin 2014). Prior to 2006, no African country had a SIM registration mandate; whereas as of February 2019, only a few countries had not introduced SIM registration laws. These mandates are often justified in terms of national security and crime prevention, though the evidence of their efficacy is disputed (Jentzsch 2012).

These regulations specify which forms of identification are legally valid to activate a SIM card, in addition to penalties for non-compliance for operators, agents, and/or customers who flout the rules. Enforcement of SIM registration rules was notoriously lax, following an initial wave of government mandates; however, this changed when MTN Nigeria was famously fined $5.2 billion USD in October 2015 for its failure to comply with a government order to disconnect improperly registered SIMs (BBC News 2015). Operators have since started complying more stringently with SIM registration rules, while governments continue to crack down on improper registration, including recently in Uganda (Kanobe et al. 2017: 13-14) and Kenya

(Musyoki 2018).

In most jurisdictions, SIM registration practices remain manual and involve taking photocopies or digital scans (stored locally) of a customer's identification documents, often without any verification of the credential against a government database. However, advancements in identification technology are enhancing registration processes, which more and more involve the real-time verification of identity information against government databases as well as biometric verification (GSMA 2018b: 28). As examples, Thailand and Bangladesh have introduced real-time biometric checks for activating SIM cards. In Kenya, Safaricom has announced that it will voluntarily incorporate a biometric component to its SIM registration efforts (based on thumbprints) to prevent SIM swap and mobile money fraud.

Know Your Customer/Customer Due Diligence

The globalization of rules for verifying a customer's identity as a prerequisite to accessing financial services has followed a different policy trajectory than SIM registration requirements. Established in 1989 by the Group of 7, the Financial Action Task Force (FATF) is an intergovernmental body whose objectives include the development of standards and policy recommendations for anti-money laundering (AML) and combating the financing of terrorism (CFT), as well as promoting the effective implementation of legal, regulatory, and operational measures in this area.

The FATF has developed recommendations that are widely recognized as the international standard for AML/CFT rules[1] and are the leading source of standards for Know Your Customer (KYC) and Customer Due Diligence (CDD) measures in the AML/CFT context. The relevant recommendations for KYC/CDD state that certain measures should be undertaken when business relationships are established or relevant occasional transactions are undertaken (e.g., when transactions are made that exceed a certain threshold), to include identifying the customer and verifying his/her identity using reliable, independent source documents, and to obtain information on the purpose and intended nature of the business relationship; in other words, financial surveillance.

FATF classifies non-bank mobile money as a "money or value transfer service," which means providers must comply with certain KYC/CDD measures and record keeping, monitoring, and reporting requirements (GSMA 2015: 30). In countries in which mobile money has been widely adopted, regulators have started issuing guidance to clarify KYC/CDD expectations for these platforms. Though specific practices vary across countries, in general this means requiring official proof of identification before one can open a mobile money wallet.

SIM registration and KYC/CDD practices result in mobile money consumers who are increasingly legible and whose financial transactions, datafied through the platform, are easily identifiable and commodifiable by service providers. Donovan and Martin (2014) note that "as calls and support for 'cashless' economies gather steam in Africa, the inevitable result will be everyday financial records that are auditable and traceable, and, doubtless, incentives to commodify personal information." We are just beginning to appreciate what these developments mean for economies where mobile money reigns, as well as the impacts on consumers.

Monitoring of Agents

A mobile money agent is a person or business that is contracted by a mobile network operator and paid a commission to facilitate user transactions. As of 2017, there were 5.3 million registered agents worldwide (GSMA 2018a: 9). The success of mobile money platforms is underpinned by the rapid deployment and growth of the agent network, which among other factors depends on the trustworthiness of its agents (Suri 2017: 506), making cases of agent fraud a major concern for the industry.

[1] The FATF recommendations: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

Fraud happens in different ways. Cash-in/cash-out transactions present an opportunity for malfeasance due to the cash-intensive nature of the business. Unassuming customers can also be defrauded by being overcharged for certain transactions. Agents may be in a position to register new customers, presenting opportunity for identity-related fraud. Unscrupulous agents sometimes unnecessarily ask customers for their mobile money wallet PIN, leading to unauthorized transactions.

The industry is well aware of the risks to customer trust of rampant mobile money fraud, particularly by agents who represent the frontline of customer service. In the absence of government regulations specific to the oversight of mobile money agents, on-site audits and "mystery shopping" by mobile network operator staff are common; these audits assess how well agents comply with the platform's codes of conduct and other policies.[2]

The monitoring of agents by mobile network operator staff represents a form of corporate workplace surveillance. What is particularly interesting in the case of mobile money is that agents often operate in geographically remote areas and in low-technology environments, necessitating in-person site visits and other prosaic forms of monitoring.

Suspicious Activity Monitoring

While KYC/CDD rules can be viewed as a front-end surveillance measure aimed at vetting customers, mobile money providers, such as Vodafone's M-Pesa, also operate in-house "bank-grade" AML monitoring systems[3] on the back-end to identify suspicious and fraudulent transactions.

M-Pesa's transaction monitoring software, called Minotaur, uses neural networks to analyze and investigate all types of user activity, including account openings, terminations, and changes, in order to identify suspicious behavior. It does so for all system users, including customers, agents, and staff. Minotaur can identify customers with multiple accounts under the same name or possible duplicate accounts under similar names. In addition, the software conducts transaction analysis to build unique behavioral profiles for every customer and agent. These profiles can be combined with account information to identify potentially suspicious activity, such as smurfing,[4] transactions inconsistent with previous behavior, changes in transaction "velocity", funds transfers to/from high-risk areas, or transfers to/from previously dormant accounts (GSMA 2015: 41). According to a GSMA survey, as of 2015, a reported 89% of mobile money providers had such an in-house monitoring solution in place, though the degree of sophistication no doubt varies across platforms.[5]

Despite the presence of these monitoring solutions, a 2018 US Department of State report noted that mobile money services in Kenya—one of the most advanced markets for electronic money—"remain vulnerable to money laundering activities" (2018a: 116). Likewise, the Department of State has also criticized Ethiopia's lax enforcement of AML/CFT measures in money mobile platforms (US Department of State 2018b: 24).[6]

---

[2] Agents themselves are also subject to fraud, by both cheats impersonating mobile network operator staff and wily customers (CGAP 2018: 2). In some cases they are subject to theft or assault (Agiresaasi 2018). A 2015 survey found that 53 percent and 42 percent of mobile money agents in Uganda and Tanzania, respectively, had experienced fraud in the past year (Bersudskaya and Kuijpers 2016).

[3] "How is the M-Pesa system monitored and regulated?" https://www.vodafone.com/content/index/what/m-pesa/m-pesa-faqs.html

[4] Smurfing, also known as structuring, is a method commonly used by money launderers whereby a transaction involving a large amount of money is broken up into smaller transactions to avoid reporting requirements and to evade scrutiny.

[5] Novikova and Kotenko point out that "apart from [the Minotaur system], there is not much publicly available information about fraud detection in mobile money transfer services" (2014: 65).

[6] "Ethiopia has made no apparent attempt to investigate and prosecute cases on suspicious or fraudulent mobile money transactions. This is especially significant since it appears that a large number of mobile money transactions occur

This disconnect between the stated capabilities of monitoring tools like Minotaur and reports from international authorities on the persistence of money laundering activities over mobile money platforms speaks to the intractability of financial crime and the ongoing challenges with regulating these activities through technological means.

Government Surveillance of Mobile Money Platforms

In this context, we are beginning to see bespoke monitoring solutions emerge in countries where authorities, distrustful of mobile money providers' self-reported data, seek to enforce regulatory compliance while also maximizing tax revenues from mobile money operations. In some cases, attendant controversies reveal elements of resistance to surveillance measures (Martin et al. 2009). Three cases of government surveillance of mobile money platforms are particularly instructive: Tanzania, Uganda, and Ghana.[7]

Tanzania

Tanzania deployed the world's first mobile money monitoring system for regulatory authorities in 2016. The Mobile Money Monitoring (M3) platform was jointly developed by Global Voice Group (GVG), a firm that works with African governments to implement technology to regulate the telecommunications sector and monitor tax revenues,[8] and Société Générale de Surveillance, a Swiss multinational. The Tanzania Communications Regulatory Authority (TCRA) uses the monitoring tool to collect and process data on mobile money transactions in the country. The system allows TCRA to closely monitor compliance with relevant laws and regulations as well as the evolution of the mobile money market (Next Billion 2016).

Tanzania's National Audit Office noted, in a 2016 report, that the M3 platform "provides visibility to mobile payment transactions over time" (91). In the same report, the Controller and Auditor General remarked that the Bank of Tanzania could also use the system to "dramatically improve regulations of mobile money banking," while noting that the "Tanzania Revenue Authority is not effectively using this module to establish tax revenue due from… mobile operators" (National Audit Office 2016: 92). Here, we observe potential scope creep in the M3 platform: a system that was originally adopted to enforce mobile money regulations possibly being extended for taxation purposes.

Uganda

In 2018, the US Department of State concluded in a country report on terrorism that "a significant portion of financial transactions in Uganda are in the form of 'mobile money' or payments and electronic funds transfers initiated through mobile phones,[9] which are vulnerable to exploitation by criminals and terrorists. While Uganda's Anti-Money Laundering (Amendment) Act requires financial institutions to conduct comprehensive customer due diligence, *it does not put the same requirements on mobile money transfers. Banking institutions do not monitor mobile money payments and transfers in Uganda; mobile money transactions are instead under the purview of the individual telecommunications company that facilitates the specific transaction*" (2018: 48, emphasis added).

Where the surveillance of mobile money platforms does exist in Uganda, it is more aimed at tracking operators' revenues for tax reasons than it is in preventing financial crime. The Uganda Communications Commission (UCC), the national telecommunications regulator, has acquired a so-called Intelligent

within the Somali region of Ethiopia, an area where the Ethiopian government has concentrated much of its counterterrorism efforts. The two mobile money platforms in Ethiopia reported growth in its revenues, especially from transactions originating in rural areas, and have expressed interest in cooperating with law enforcement on investigations under certain conditions" (US Department of State 2018b: 24).

[7] Other cases exist but will not be explored in this article, including Nigeria's Global Mobile Payments Monitoring and Regulation System.

[8] GVG has sought to market its monitoring tools in other countries, including Benin: https://www.globalvoicegroup.com/en/mobile-money-governance-to-boost-benins-revenues/.

[9] A reported $50m is transacted through mobile money every day in Uganda (Karugaba 2018).

Network Monitoring System to monitor the revenue of mobile network operators. Although the original expectation was that the system would only monitor the voice and data channels of networks, the regulator subsequently disclosed that it is monitoring other transactions, including mobile money and social media activity (following the introduction of a social media tax by government).

Mobile network operators MTN and Airtel had opposed the implementation of the system, partly due to its intrusiveness into their mobile money business. Prior to introducing the monitoring system, the UCC had relied on a self-declaration process by which operators would declare all information to the regulator (Daily Monitor 2018). However, the UCC accused operators of "under-declaring revenue and cheating the government" (Adepoju 2018).

Airtel responded to the UCC by raising concerns with the business secrecy of its customers. Airtel also noted that mobile money services are regulated by the Bank of Uganda and not the UCC (notwithstanding the aforementioned gap in AML/CFT oversight). The operator further contested the legal basis for granting access to data beyond the UCC to include the Uganda Police (Lee 2018), but to no avail.

Ghana

In Ghana, where the value of mobile money transactions rose to 34.6 billion USD in 2017 (Dzawu 2018), a political impasse between the Ministry of Communications and the Bank of Ghana over the monitoring of mobile money transactions persisted for several months, until a resolution was achieved in late 2018.

In May 2018, the Ministry of Communications demanded that mobile operators allow Kelni GVG (a joint venture with the Global Voice Group) to access their systems to monitor traffic, using the Common Monitoring Platform in order to ensure that the taxes declared by operators are accurate. The Ministry also wanted providers to disclose customer balances, transaction amounts, and the dates and times of transactions. The legislation granted Kelni GVG physical access to the nodes of operators' networks (Arthur-Mensah 2018).

On one side of the dispute, the Communications Minister had described resistance by operators as "completely unjustified, fanciful or smack of disrespect for our laws" (Joy Business 2018), while the director general of the National Communications Authority quizzed: "We have visited four countries where each of these telcos operate and they are happy to comply with real-time monitoring so why are they apprehensive about the same system in Ghana? Is it because they have something to hide" (Joy Online 2018)?

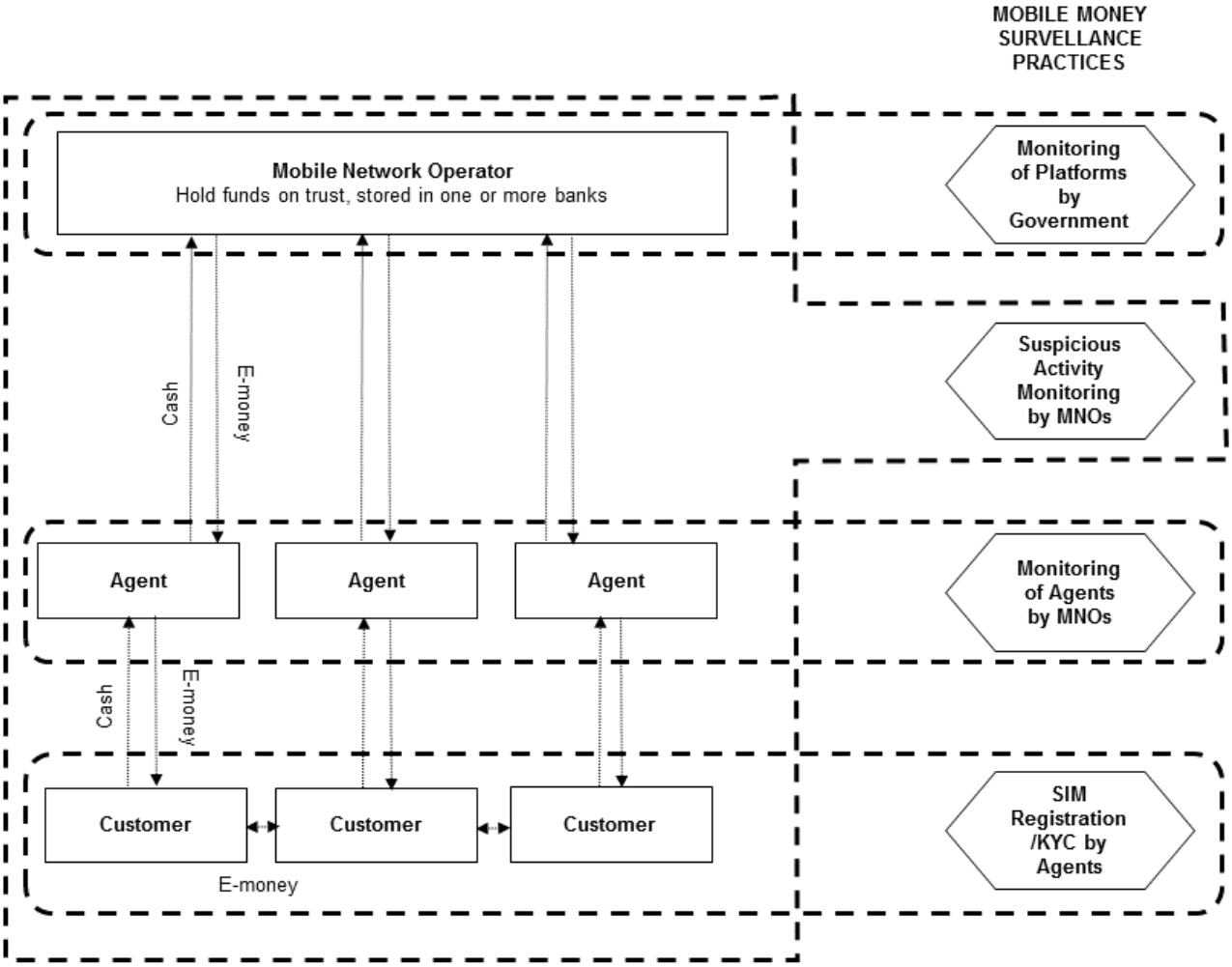
On the other side, the Central Bank had argued that handing over of such data to the Common Monitoring Platform would breach the country's *Guidelines for Electronic Money Issuers* and the *Data Protection Act* (Joy Business 2018) and instructed operators to disregard the Ministry of Communications. Ultimately, however, Kelni GVG assured that their system was built to conform to the relevant provisions of the *Data Protection Act* (Acquaye 2018), while the Communications Ministry stressed that all concerns raised by stakeholders had been addressed and the system was implemented.[10]

Whether the monitoring systems in Tanzania, Uganda, and Ghana ultimately meet regulatory expectations remains to be seen. It nevertheless appears likely that other governments will pursue similar monitoring powers, technologies, and methods as mobile money usage spreads and government concerns about regulatory compliance and taxation grow. For example, in Zimbabwe, where eight out of ten financial

[10] In a separate development on the technology supply side, a Ghanaian technology firm, Subah, has launched its own mobile money monitoring tool and even presented it at the 2017 International Telecommunication Union Telecom World conference in South Korea, a global meeting of telecommunications regulators. Subah's product can capture, analyze, and retain information on all mobile money transactions, such as the sender, receiver, and operator, automatically reports high value and repeat transfers to individuals and businesses, and summarizes service charges applied by all operators. Moreover, it claims to be "fully customizable for different mobile banking regulatory frameworks" (Communications Africa 2017: 4).

transactions are carried out over the EcoCash platform due to the country's gross shortage of cash (Steinhauser 2018), mobile money and other electronic transactions are now being taxed (MISA 2018). It is likely that sophisticated surveillance apparatus will follow suit. These phenomena are certain to expand across the continent and beyond (cf. Bangladesh Financial Intelligence Unit 2018).

Figure 1. *Mobile Money Platform Surveillance*[11]



Concluding Remarks

This article has surveyed the ways in which mobile money platforms have become an object of suspicion and surveillance. Identification practices embodied in SIM registration and Know Your Customer/Customer Due Diligence requirements make mobile money customers and their transactions legible to service providers and government. The monitoring of agents by mobile network operators aims to mitigate fraud at the human interface of the platform. Back-end monitoring systems attempt to spot suspicious activity on platforms, though money laundering and other illicit activities persist. Most recently, government bodies have taken a keen interest in more invasive forms of regulatory oversight by directly accessing mobile

[11] Adapted from Greenacre's Common Model of Mobile Money (2018: 10).

money platform data; however, this is increasingly driven by concerns about generating tax revenue and not security *per se*.

Why does this matter? For one, emerging evidence from the region suggests that perceptions of financial surveillance are significant enough to alter consumer behavior. Zambians have reportedly migrated from traditional banking services to mobile money partly due to concerns about surveillance based on the country's Taxpayer Identification Number (Phiri 2018). Will these countries revert to cash-based economies and "burying cash in backyards" (Ibukun et al. 2018) if mobile money begins to be perceived as essentially a surveillance platform?

It is an open empirical question whether the move to monitor these platforms more extensively will stunt the use of mobile money and similar payment innovations. We also do not yet understand the impacts of mobile money surveillance on financial inclusion. Further research is needed to explore whether and in what circumstances surveillance—or at least perceptions thereof—affects the adoption and usage of mobile money across contexts and users. On the advocacy side, there may also be an opportunity for civil society actors to develop principles for preventing regulatory overreach with respect to mobile money monitoring.

Acknowledgments

As a member of the Global Data Justice project at Tilburg University, the author has received funding from the European Research Council under the European Union's Horizon 2020 research and innovation programme (Grant Agreement n° 757247). The author would like to thank Kevin Donovan, Shaz Jameson, Hellen Mukiri-Smith, Linnet Taylor, and an anonymous reviewer for their comments on the article. An early version of the paper was presented at the 2018 Amsterdam Privacy Conference panel on Data and the Global South organized by Payal Arora and Linnet Taylor.

References

Acquaye, Nana Appiah. 2018. Kelni GVG Common Monitoring Platform Expected to Go Live on Monday. *BizTech Africa*, October 19. http://www.biztechafrica.com/article/kelni-gvg-common-monitoring-platform-expected-go-l/14045/.

Adepoju, Paul. 2018. Uganda's UCC, Telcos Clash over Network Monitoring Technology. *ITWeb Africa*, July 9. http://www.itwebafrica.com/ict-and-governance/400-uganda/244505-ugandas-ucc-telcos-clash-over-network-monitoring-technology.

Agiresaasi, Apophia. 2018. Mobile Money Is a Boon for Ugandans, But Payment Agents Fear Thefts, Attacks. *Global Press Journal,* January 29. https://globalpressjournal.com/africa/uganda/mobile-money-boon-ugandans-payment-agents-fear-thefts-attacks.

Aitken, Rob. 2017. "All Data Is Credit Data": Constituting the Unbanked. *Competition & Change* 21 (4): 274–300. https://doi.org/10.1177/1024529417712830

Arthur-Mensah, Goodwill. 2018. Government Rolls Out Platform to Monitor Telecoms Revenue. *Ghana News Agency*, December 13. http://www.ghananewsagency.org/print/143207.

Bangladesh Financial Intelligence Unit. 2018. Study Paper on AML/CFT Regulations for Mobile Money: Policy Options for Bangladesh. *Bangladesh Bank,* April. https://www.bb.org.bd/pub/research/sp_research_work/srw1704.pdf.

BBC News. 2015. Nigeria Telecom Giant MTN Fined $5.2bn. *British Broadcasting Corporation,* October 26. https://www.bbc.com/news/business-34638595 .

Bersudskaya, Vera, and Dorieke Kuijpers. 2016. Working Together To Fight DFS Fraud: Agent Network Accelerator Survey. *Helix Institute*. http://www.helix-institute.com/data-and-insights/agent-network-accelerator-survey-uganda-country-report-2015.

Communications Africa. 2017. Subah Launches Mobile Money Monitoring Suite. *Communications Africa* 6 (2017): 4.

CGAP. 2018. Fraud in Mobile Financial Services. *Consultative Group to Assist the Poor,* April. https://www.cgap.org/research/publication/fraud-mobile-financial-services.

Daily Monitor. 2018. Uganda Installs System to Track Telco Revenues. *The East African*, July 4. https://www.theeastafrican.co.ke/business/Uganda-installs-system-to-track-telco-revenues/2560-4646012-xnnij7/index.html.

Donovan, Kevin. 2012. Mobile Money for Financial Inclusion. *Information and Communications for Development 2012*: 61–73. https://doi.org/10.1596/9780821389911_ch04.

Donovan, Kevin P., and Aaron K. Martin. 2014. The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change. *First Monday* 19 (2). https://doi.org/10.5210/fm.v19i2.4351.

Donovan, Kevin P., Philippe M. Frowd, and Aaron K. Martin. 2016. Introduction: ASR Forum on Surveillance in Africa. *African Studies Review* 59 (2): 31-37. https://doi.org/10.1017/asr.2016.35.

Dzawu, Moses Mozart. 2018. Ghana's Mobile Money Transactions Double to $35 Billion. *Bloomberg,* February 5. https://www.bloomberg.com/news/articles/2018-02-05/ghana-2017-mobile-money-deals-almost-double-to-35-billion.

Epstein, Gerald A. 2005. *Financialization and the World Economy*. Cheltenham: Edward Elgar.

Greenacre, Jonathan. 2018. Regulating Mobile Money: A Functional Approach. *Pathways for Prosperity Commission Background Paper Series* 4.

GSMA. 2015. Proportional Risk-Based AML/CFT Regimes for Mobile Money: A Framework for Assessing Risk Factors and Mitigation Measures. *Mobile for Development,* August. https://www.gsma.com/mobilefordevelopment/programme/mobile-money/proportional-risk-based-amlcft-regimes-for-mobile-money-a-framework-for-assessing-risk-factors-and-mitigation-measures/.

GSMA. 2018a. State of the Industry Report on Mobile Money. *Mobile for Development*. https://www.gsma.com/mobilefordevelopment/sotir/.

GSMA. 2018b. Access to Mobile Services and Proof-of-Identity: Global Policy Trends, Dependencies and Risks. *Mobile for Development*. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf.

Ibukun, Yinka, Mustapha Muhammad, and Emele Onu. 2018. Nigerians Bury Cash in Backyards as Mobile Money Stumbles. *Bloomberg,* July 19. https://www.bloomberg.com/news/articles/2018-07-18/nigerians-bury-cash-in-backyard-banks-as-mobile-money-stumbles.

ICRC and Privacy International. 2018. The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era. *International Committee of the Red Cross,* October. https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era.

Jentzsch, Nicola. 2012. Implications of Mandatory Registration of Mobile Phone Users in Africa. *Telecommunications Policy* 36 (8): 608–620. http://dx.doi.org/10.1016/j.telpol.2012.04.002.

Joy Business. 2018. Communications Ministry Fights BoG over Mobile Money Data. *Joy Online*, November 14. https://www.myjoyonline.com/business/2018/November-14th/communications-ministry-bog-in-standoff-over-mobile-money-data.php.

Joy Online. 2018. Kelni GVG Equipment Not Capable of Spying—Minister, NCA Defend Controversial Deal. *Joy Online,* June 2. https://www.myjoyonline.com/business/2018/june-2nd/kelni-gvg-equipment-not-capable-of-spying-minister-nca-defend-controversial-deal.php

Kanobe, Frederick, Patricia Alexander, and Kelvin Bwalya. 2017. Policies, Regulations, and Procedures and their Effects on Mobile Money Systems in Uganda. *The Electronic Journal of Information Systems in Developing Countries* 83 (1): 1-15. https://doi.org/10.1002/j.1681-4835.2017.tb00615.x.

Karugaba, Mary. 2018. "We Were Not Consulted on Mobile Money Tax"—Mutabazi. *New Vision*, August 14. https://www.newvision.co.ug/new_vision/news/1483562/consulted-mobile-money-tax-mutabazi

Klauser, Francisco, R. 2017. *Surveillance and Space.* London: Sage.

Lee, Claire. 2018. Dispute in Uganda over Mobile Money Monitoring Continues. *DFS Observatory*, March 15. https://dfsobservatory.com/content/dispute-uganda-over-mobile-money-monitoring-continues.

Lyon, David. 2009. *Identifying Citizens: ID Cards as Surveillance.* Malden, MA: Polity.

Kendall, Jake, Bill Maurer, Philip Machoka, and Clara Veniard. 2011. An Emerging Platform: From Money Transfer System to Mobile Money Ecosystem. *Innovations: Technology, Governance, Globalization* 6 (4): 49–64. https://doi.org/10.1162/INOV_a_00100.

Makulilo, Alex B. 2015. Privacy in Mobile Money: Central Banks in Africa and their Regulatory Limits. *International Journal of Law and Information Technology* 23 (4): 372–391. https://doi.org/10.1093/ijlit/eav014

Martin, Aaron K., Rosamunde E. van Brakel, and Daniel J. Bernhard. 2009. Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework. *Surveillance & Society* 6 (3): 213–232. https://doi.org/10.24908/ss.v6i3.3282

MISA. 2018. Implications of Electronic Transactions Tax on Digital Rights. *Media Institute of Southern Africa,* October 3. http://zimbabwe.misa.org/2018/10/03/implications-of-electronic-transactions-tax-on-digital-rights/.

Musyoki, Miriam. 2018. SIM Cards That Will Be Blocked From Today. *Kenyans*, August 21. https://www.kenyans.co.ke/news/29826-communications-authority-kenya-ca-notice-sim-card-deactivation.

National Audit Office. 2016. Submission of the Annual General Report of the Controller and Auditor General on the Audit of Public Authorities and Other Bodies for the Financial Year 2014/2015. *United Republic of Tanzania*.

Next Billion. 2016. Tanzania Deploys the First Mobile Money Monitoring Solution for Regulatory Authorities in the World. *Next Billion,* April 25. https://nextbillion.net/news/tanzania-deploys-the-first-mobile-money-monitoring-solution-for-regulatory-authorities-in-the-world/.

Novikova, Evgenia, and Igor Kotenko. 2014. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. In *Availability, Reliability, and Security in Information Systems,* edited by Stephanie Teufel, Tjoa A. Min, Ilsun You, and Edgar Weippl, 63-78. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-10975-6_5.

Phiri, Prudence. 2018. Zambians, Wary of Taxpayer ID Rule, Opt for Mobile Money Rather Than Banks. *Global Press Journal*, September 13. https://globalpressjournal.com/africa/zambia/zambians-wary-taxpayer-id-rule-opt-mobile-money-rather-banks/.

Steinhauser, Gabriele. 2018. Virtual-Cash Treasure in Zimbabwe Sparks Fight Over Billions. *Wall Street Journal*, January 2. https://www.wsj.com/articles/virtual-cash-treasure-in-zimbabwe-sparks-fight-over-billions-11546430988.

Suri, Tavneet. 2017. Mobile Money. *Annual Review of Economics* 9: 497–520. https://doi.org/10.1146/annurev-economics-063016-103638.

The Economist. 2018. Borrowing by Mobile Phone Gets Some Poor People into Trouble. *The Economist*, November 17. https://www.economist.com/finance-and-economics/2018/11/17/borrowing-by-mobile-phone-gets-some-poor-people-into-trouble.

US Department of State. 2018a. International Narcotics Control Strategy Report, Volume II: Money Laundering. *Bureau for International Narcotics and Law Enforcement Affairs,* March. https://www.state.gov/documents/organization/278760.pdf.

US Department of State. 2018b. Country Reports on Terrorism 2017. *Bureau of Counterterrorism and Countering Violent Extremism,* September. https://www.state.gov/documents/organization/283100.pdf.