Young African Leaders Journal of Development

Volume 3  Article 4

1-1-2021

Public Policy, A Catalyst For Silencing Financial crime And Corruption: The Case For Deployment Of Digital IDs In The Social Media Platforms

Donald Kbayi
University of South Africa

Follow this and additional works at: https://digitalcommons.kennesaw.edu/yaljod

Part of the African Studies Commons, Critical and Cultural Studies Commons, Growth and Development Commons, Peace and Conflict Studies Commons, and the Political Theory Commons

Recommended Citation
Available at: https://digitalcommons.kennesaw.edu/yaljod/vol3/iss1/4

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Young African Leaders Journal of Development by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.
PUBLIC POLICY, A CATALYST FOR SILENCING FINANCIAL CRIME AND CORRUPTION: THE CASE FOR DEPLOYMENT OF DIGITAL IDS IN THE SOCIAL MEDIA PLATFORMS

Donald Kubayi
University of South Africa, Republic of South Africa

ABSTRACT
The use of social media platforms such as Twitter, YouTube, Facebook, and Instagram for promoting criminal agendas (including global terrorism, transnational organised crime, and cyberattacks) is a rapidly growing phenomenon. Criminals are increasingly using social media as a platform for the recruitment of victims, clients, service providers, and to solicit donations that are normally channelled through the financial system. The National Defense University's Center for Complex Operations lists social media as “enabling a new category of professional ‘terrorist financiers’ within terrorist groups, as they rely more heavily on social media to solicit donations and communicate with both donors and recipient radicals” (Trabulsi & Reitano, 2016, p.223). In Africa, Somalia’s al-Shabaab is identified as a terrorist organisation that has “long had quite active campaigns on Twitter and Facebook, and spends considerable energy on propagating its radical ideology through slick propaganda” (Trabulsi & Reitano, 2016, p.217).

The complexity of a trillion-dollar financial crime industry requires a multidisciplinary collaborative approach to comprehend and counter. Effective cross border collaboration on intelligence sharing and border security among the African states, together with regional, continental and international organisations is key to the successful deployment of counter terrorism strategies (Ramdeen, 2017).

Digital identification, or “digital ID”, is becoming an essential tool for anti-corruption and financial crime efforts. The need for the deployment of digital ID systems to counter the various financial crimes through social media is becoming increasingly urgent. Deployment of digital ID systems by the social media companies is critical to silence the voices of those promoting criminal acts or terrorist agendas through these platforms. The paper seeks to make a meaningful contribution towards the global fight against financial crimes and corruption by making a case for public policy by governments and financial regulators around the world recognises as a catalyst for the take-up of digital IDs by the social media companies.

INTRODUCTION
Today, there is a growing recognition that social media has become an essential tool for organised crime groups in promoting their criminal agendas enabling terrorist groups to facilitate the financial crimes of money laundering and financing of terrorism (Piazza & Guler, 2019; United Nations Office on Drugs and Crime, 2012). Digital identification, or “digital ID” has been acknowledged globally as a new technology-based solution that has the potential to revolutionise the global fight against financial crimes and corruption (Mari & Davis, 2019). The collaboration to win the war on financial crime and corruption rests on the effective deployment of digital ID systems in both the social media and financial industries because organised crimes normally originate in the social media before it is committed through the financial industry (Muggah, 2015). The drawbacks and potential misuse of social media platforms have been recently documented as highlighted in the remarks of Amedie that “Another dangerous aspect of social media is the rapid adoption of this medium by terrorists groups” (Amedie, 2015, p.13).

For example, a UNDOC’s publication on the use of the Internet for terrorist purposes has stated that:

The promotion of extremist rhetoric encouraging violent acts is also a common trend across the growing range of Internet-based platforms that host user-generated content. Content that might
formerly have been distributed to a relatively limited audience, in person or via physical media such as compact discs (CDs) and digital video discs (DVDs), has increasingly migrated to the Internet. Such content is distributed using a broad range of tools, such as dedicated websites, targeted virtual chat rooms and forums, online magazines, social networking platforms such as Twitter and Facebook, and popular video and file-sharing websites, such as YouTube and Rapidshare, respectively. The use of indexing services such as Internet search engines also makes it easier to identify and retrieve terrorism-related content. (United Nations Office on Drugs and Crime, 2012, p.5).

The Institute of International Finance's (IIF) paper 2019 Digital Identities in Financial Services- Part 1: Embedding in AML Frameworks makes a strong argument for the adoption of Digital IDs for financial crime prevention as reflected in these remarks "Assuming the security standards are sufficiently high to prevent fraud and illegitimate generation of fake Digital IDs, bad actors will find it harder to gain access to the system." The literature on the significant role that Digital Identity can play in digital environments is extensive, and the adoption and use of digital identification networks by the public and private sector organisations are not new (Abelson et al., 1998). This sentiment is echoed by the Financial Action Task Force's (FATF) draft guidance on digital identity. In particular, the draft guidance publication states that:

The rapid pace of innovation in the digital identity (ID) space has reached an inflection point. Digital ID standards, technology and processes, have evolved to a point where digital ID systems are, or could soon be, available at scale. Some of these relevant technologies include: a range of biometric technology; the near-ubiquity of the Internet and mobile phones (including the rapid evolution and uptake of “smart phones” with cameras, microphones and other “smart phone” technology); digital device identifiers and related information (e.g., MAC and IP addresses; mobile phone numbers, SIM cards, global position system (GPS) geolocation; high-definition scanners (for scanning drivers licenses and other ID); high-resolution video transmission (allowing for remote identification and verification and proof of “liveness”); artificial intelligence/machine learning (e.g., for determining validity of government-issued ID); and distributed ledger technology (DLT) (FATF Guidance, 2019: 8).

The paper makes a case for public policy as a catalyst for the take-up of digital identity technologies by social media companies. The paper goes on to highlight some of the existing digital ID networks across public and private sectors that share some light on the potential of digital ID tools for facilitating the collaboration to win the war on financial crime and corruption.

**DEFINITION OF KEY CONCEPTS**

The concepts of digital Identity and public policy as predominately used in this paper are defined and clarified to provide an explicit understanding of these terms and the context they are used in this paper.

**Digital Identity**
“Digital Identity”- the most describing explanation for digital identity has been offered by the Association of Certified Anti-Money Laundering Specialists (ACAMS) as “data about persons stored and accessible through computer systems that closely link to their civil and national identities” (Mari & Davis, 2019). Through the use of digital ID systems, a person’s official identity in an online environment can be linked to a physical person.

**Public Policy**
Thomas Dye defines the concept of public policy in its simplest form as “anything a government chooses to do or not to do” (Howlett & Cashore, 2014, p.17). From Dye’s definition, public policy can be understood in a wide and narrow sense. In the wide sense, it refers in general to a government regulation to safeguard the
interests of the public. However, in the narrow sense, the term refers to an action or decision by the government to achieve a particular goal(s).

OVERVIEW OF KEY FINANCIAL CRIMES AND CORRUPTION
The Temenos and NetGuardians' e-book titled A-Z of financial crime in Africa reports an increase of 7% in economic crime for Africa estimated at 57% against a global average percentage of 36% over a period of 24 months (Temenos and NetGuardians, 2016). The Refinitiv's report on the true cost of financial crime focusing on Sub-Saharan Africa estimates that companies across the region spent 3.4% of turnover (against a globally average of 3.1%) to prevent financial crime over a period of 12 months (Refinitiv, 2019). Today there is a growing recognition that citizens have an important role to play in the war against financial crimes and corruption. As the general public becomes increasingly aware of financial crimes and corruption through the mass media, governments across African states are soon realising that the young population is fed up through rampant corruption and economic crimes that have been going on for many years. Chimezule (2015) makes a case for a greater involvement of civil societies to fight corruption and financial crimes in his country, as he states that:

Corruption is controlled only when citizens are no longer prepared to tolerate it. Private groups, professional organizations, religious bodies etc. all have stakes in the fight against financial crimes in Nigeria. Civil societies are watch dogs on the integrity of public office holders. Their independent stand on issues, acts as checks and balances on the public and private sectors. Thus it is obvious that when civil societies are strengthened, it can curb corruption and financial crimes (Chimezule, 2015, p.30).

Efforts by individual country governments, civil society organisations (CSOs) and international regulatory organisations are geared towards the promotion of transparency in various industries that are known for illicit and corrupt activities such as the extractive industry within their own countries. On a global level, transparency initiatives like the Publish What You Pay (PWYP) and Section 1504 of the Dodd-Frank Wall Street Reform and Consumer Protection Act are pushing for globally accepted transparency standards (Sovacool et al 2016).

The 'traditional' financial crimes like fraud and money laundering have been associated with criminals for many ages. Over the last two decades, criminals have invented new methods of committing the same 'traditional financial' crimes like fraud as well as cybercrime by using computer technology as tool (Brenner, 2012). There is a strong connection between modern crimes of corruption in the real world and financial crime via the cyberspace (Zadvornykh, 2018). The following prominent types of financial crimes have necessitated the deployment of fintech solutions:

Money laundering
The term 'money laundering' has been defined in general as referring to 'any acts that obscures the illicit nature or the existence, location or application of proceeds of crime' (de Koker, 1999). The definition adopted by the FATF (Financial Action Task Force) defines money laundering as the 'process of criminal proceeds to disguise their illegal origin' (van der Wolf, 2011). With the rise of technology, the crime of money laundering has become more complex because criminals have found a way of utilising shell companies and perhaps even fintech-enabling technologies to hide laundering financial transactions (The Financial Action Task Force, 2018). As a result money laundering and financing of terrorism are receiving more attention from international institutions, governments and law enforcements around the globe.

Cyber crime
Cybercrime is a computer-oriented crime that "involves a computer, networked device or a network" (Brush et al., 2020). Chambers-Jones (2012) states that, 'more criminals exploit the speech, convenience and anonymity modern technologies offer in order to commit a diverse range of crimes'. Criminals use a sophisticated form of cybercrime such as cyber-attacks as well as less sophisticated forms of cybercrimes such as spoofing, phishing, spamming and scams to commit various crimes. Cyber risk is emerging as a key
threat to financial stability, hackers directing their cyberattacks on the SWIFT network of central banks with Bangladesh's central bank losing nearly USD 100 million to hackers in February 2016 (Bouveret, 2018).
<table>
<thead>
<tr>
<th>Country</th>
<th>Digital ID system</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDIA</td>
<td><img src="" alt="AADHAAR" /></td>
<td><strong>Aadhaar</strong> has been described as the world's largest biometric identity system that has been operational since 2010. This unique identification system is used to provide a variety of public and private services.</td>
</tr>
<tr>
<td>ESTONIA</td>
<td><img src="" alt="REPUBLIC OF ESTONIA e-RESIDENCY" /></td>
<td><strong>e-Residency</strong> has been described as the first government issued digital identity that provides Estonia residents with access to various digital services such as e-Governance, e-Tax, e-Residency and e-Health.</td>
</tr>
</tbody>
</table>

(India. Ministry of Electronics and Information Technology. 2019. *Unique Identification Authority of India*)

| UNITED KINGDOM | GOV.UK VERIFY | GOV.UK Verify is the United Kingdom's identity assurance system used as a “secure way to prove who you are online” providing UK residents with access to government services. |
| NEW ZEALAND | RealMe | RealMe is a New Zealand government's login and identity verification service, and it provides a variety of government services as well as private services such as opening bank accounts to be accessed online without providing additional identification. |
| UNITED STATES | (the United States of America. Departments of Motor Vehicles. 2020 New driving licenses: from cards to mobile driver’s licenses, solutions, and services) | Digital Driver’s License U.S Pilot is a 2-year interoperable pilot development of a smartphone-based credential for implementation in five US states (Colorado, Idaho, Washington D.C, Wyoming and Maryland) to provide services such enrolment, updates to the document once it is in the field, attribute sharing and law enforcement. |

Source: *ACAMS Today Magazine – November 2019 Special for the web*

**Private sector digital identification networks**

Across the private sector, Verified. Me, Mastercard Digital Identity Services and Shyft are the most prominent existing private industry digital identification networks in operations that may serve as references. Table 2 below provides a list of digital identification networks across the private sector.
Table 2: Private industry digital identification networks in operations

<table>
<thead>
<tr>
<th>Digital ID system</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verified.Me</strong></td>
<td><strong>Verified.Me</strong> is a service offered by SecureKey Technologies Inc as a Canadian Digital identity that offers a secure and convenient way to help Canadians verify their identities online which was developed in cooperation with seven of Canada’s major financial institutions (BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD).</td>
</tr>
<tr>
<td><strong>Mastercard Digital Identity Services</strong></td>
<td><strong>Mastercard Digital Identity Services</strong> is a pilot digital ID verification services as first announced in March 2019 being developed by Mastercard in collaboration with Samsung Electronics Co., Microsoft Corporation, the Australian government, and Deakin University.</td>
</tr>
<tr>
<td><strong>Shyft</strong></td>
<td><strong>Shyft</strong> is a decentralised public network that has been described as “the world’s first modern, secure, multi stakeholder Blockchain-based digital identity ecosystem that enables Know Your Customer (KYC)/ Anti Money Laundering (AML) attested data transfers” (Business Wire, 2019). Data is provided to the network via shyft tru anchors, which are predominately financial services companies.</td>
</tr>
</tbody>
</table>

**Source:** ACAMS Today Magazine – November 2019 Special for the web

From the several digital identification networks operational today across public and private sectors, the implementation of these networks in the social media channels, Twitter, YouTube, Facebook, and Instagram is missing (Smith, 2020). The potential to solve many of the problems associated with organised crime that normally originates in the social media before it becomes a financial crime will be lost if social media companies do not work towards the implementation of digital identification on all these social media channels.

**Public Policy And Regulation Of Social Media Companies**
Public policy is an established concept of rule-making which, in lay terms, means government regulation to safeguard the interests of the public. The interpretation of what is regarded as in the public interest or for public purpose may vary from country to country. An important public policy question for governments is how to regulate the take-up of digital identity systems by the social media companies in order to prevent the promotion of organised crimes through the various social media platforms for the global fight against financial crimes and corruption? For digital identity, public policy for regulating the introduction and take-up of digital identity solutions by the social media companies must take into consideration a range of existing
regulatory frameworks for data protection, privacy, and surveillance issues.

Several terrorist financing cases that involved social media have unfolded during the last decade, and this has led to some governments proposing regulatory measures for the social media companies in an effort to combat organised crime, money laundering, and the financing of terrorism (All Answers Ltd., 2018).

The documented rise in live streaming of inappropriate content as well as serious crime on Facebook makes a compelling case for regulating the introduction and take-up of digital identity technology solutions by the social media companies. Cases of online hate targeted to certain groups of people or individual and broadcast killings on Facebook Live are not new. The New Zealand mosque massacre is one example of the documented livestream with more video uploads within 24 hours' time, “1.5 million videos and images of the killings were uploaded to Facebook's servers” (Grygiel, 2019). Media reports on the Rohingya refugees in India where it is reported that “But anti-Rohingya hate speech and falsehoods have since spread to India, where Facebook has 340 million users” (Rahman & Goel, 2019) and the trending hateful xenophobic hashtags in South Africa, to name but a few, reveal an unacceptable state of online hate (Chengeta, 2020).

Across the world, regulatory framework for the large social media platform operators is still in its infancy and the existing criminal regulatory regime for most countries does not specifically address the prevention of online criminal activities or behaviour facilitated through the major social media platforms. Australia, China, Germany, Russia, the United Kingdom, the United States and Canada are one of the few countries that have been regulating social media companies over what has been described as harmful content. Table 3 below provides a list of countries that legislates social media companies

<table>
<thead>
<tr>
<th>Country</th>
<th>Policy framework on social media companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIA</td>
<td>Australia’s 2019 criminal law (Sharing of Abhorrent Violent Material Act 2019) introduced criminal penalties for social media companies in relation to abhorrent violent material</td>
</tr>
<tr>
<td>CHINA</td>
<td>China has blocked social media sites such as Twitter, WhatsApp, and Google and employs cyber police to monitor social media platforms.</td>
</tr>
</tbody>
</table>

Table 3: Countries with regulations targeted to social media companies
<table>
<thead>
<tr>
<th>Country</th>
<th>Law</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>Germany’s 2018 Network Enforcement Act (NetzDG) requires social media companies to set up procedures to review complaints about content they are hosting and remove illegal material within 24 hours.</td>
<td>Böttcher, L. (2018). Network Enforcement Act (Netzrücksetzunggesetz, NetzDG). German Law Archive.</td>
</tr>
<tr>
<td>Russia</td>
<td>Russia’s 2015 Data Law requires all social media companies to store any data about Russian citizens on servers within the country.</td>
<td>KPMG (2020). The “localisation” of Russian citizens’ personal data. KPMG</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>The UK’s 2015 Counter Terrorism Security Act grants intelligence agencies the power to conduct mass surveillance and store data from social media companies</td>
<td>The United Kingdom National Archives. Counter Terrorism and Security Act 2015.</td>
</tr>
</tbody>
</table>
Canada’s 2018 Network Enforcement Act (known as “Facebook Law”) “legislates hefty fines of up to 50 million for social media companies that fail to remove obviously illegal content, including defamation, incitations to violence, and hate speech within 24 hours of the content being reported.”

THE CASE FOR DIGITAL IDs IN THE SOCIAL MEDIA PLATFORMS

The regulatory measures imposed on social media companies as presented in table 3 above illustrate the need for regulation of Internet-related services (e.g. social media platforms) and content control as a way of combating security threats such as organised crime, corruption and the financial crime of money laundering and the financing of terrorism. Social media companies have always worked on the principle of freedom of expression, which lacked checks and balances with regards to content that may be deemed to be contrary to public purposes or in the public interest. Long before the popularity of social media platforms, many countries already enacted laws that prohibited any form of expression that is likely to incite acts of violence or promote security threats such as global terrorism, organised crime, corruption, and cyber attacks (UNODC, 2012).

Allowing the free exchange of ideas and content on the social media platforms provided new financial crime and corruption opportunities simply through the misuse of well-intended social media innovations such as Live-Streaming. In order to provide effective technology innovation measures to threats presented by organised crime groups using the social media platforms, governments require clear public policy measures that prevent unlawful acts carried out over multiple social media channels taking into consideration a range of existing regulatory frameworks for data protection, privacy, and surveillance issues. This can be achieved through a public policy framework that encourages social media companies for the take-up of digital identity systems to counter organised crimes as these crimes normally originate in the social media space before they become a financial crime that is committed through the financial sector industry.

In practice, regardless of the existing legislative frameworks to combat security threats, the global fight against financial crime and corruption will not be easily won if the deployment of the digital ID systems is not implemented in the social media space. Credit should be given to Australia, China, Germany, Russia, United Kingdom, and the United States as well as countries that have shown commitment in curbing financial crime and corruption that is facilitated through social media platforms. It was through these regulatory policy measures by these few countries that forced social media companies to begin putting measures forbidding the posting of harmful material on their platforms (UNCTAD, 2016).

Taking down social media accounts that promote violence or terrorism-related propaganda is one step in the right direction in winning the war on financial crime and corruption. This action alone by social media companies will not produce great results if technologies such as digital identity are not implemented in the social media space. The fact that it is easy to open a new social media account in few minutes makes the monitoring of offensive accounts difficult because people can still promote their criminal acts by opening a
new account with a refined strategy to avoid being easily classified as offensive account while still being able to promote their criminal or terrorist agendas.

CONCLUSION AND RECOMMENDATIONS

Across the globe, there is an increasing awareness that the global fight against financial crimes and corruption can be won through the use of Information and Communication Technology (ICT) tools such as digital identity, big data, machine learning, distributed ledger technology, blockchain, and artificial intelligence. Digital identification, or “digital ID, is becoming an essential ICT tool for anti-corruption and financial crime efforts. The need for the deployment of digital ID systems to counter the various financial crimes facilitated through social media platforms such as Twitter, YouTube, Facebook, and Instagram is becoming increasingly urgent. Deployment of digital ID systems by the social media companies is critical to silence the voices of those promoting criminal acts or terrorist agendas through these platforms.

Effective regulation is key to the successful deployment of digital Identity technology solutions for fighting financial crime and corruption. The sentiment is reflected in the remarks made by the joint-authors, Adam Thierer, Andrea Castillo O'Sullivan, and Raymond Russell that ‘unless a compelling case can be made that a new invention will bring serious harm to society, innovation should be allowed to continue unabated and problems, if they develop at all, can be addressed later’ (Thierer, O'Sullivan & Russell, 2017, p. 3 & 5). The key advantage for deployment of digital ID systems by the social media companies is that it simplifies the verification of platform users' identities online making it easier for the platform operators to deal with million uploads that are regarded as inappropriate and the users' personal data on the social media platforms only needs to be cleaned up so that authentication online is made easier.

This paper advocates for the deployment of digital ID systems to counter the various financial crimes facilitated through social media platforms by making a case for a public policy framework that encourages social media companies to deploy digital identity systems to counter organised crimes. The prospect for successful prevention of financial crimes and corrupt practices is possible through the flexible and adaptable social media regulation. From the existing digital ID networks across the public and private sectors, various lessons are learned. A review of the literature showed that digital identity exists in certain parts of the world and has been instrumental in improving trustworthiness, security, privacy, and convenience of identifying natural persons in a variety of online settings. Based on the findings, it is safe to conclude that it is practically possible to use public policy regulatory framework similar to the mandatory SIM card registration laws as a catalyst for take-up of digital services by the social media companies as a valuable partner that can play a significant role in silencing the voices of those promoting criminal acts or terrorist agendas through these platforms. However, for this to be successful, it is recommended that the Financial Action Task Force (FATF) leads the campaign on the deployment of digital Identity systems by the social media companies in their various platforms as a tool for fighting financial crime and corruption.


