https://dspace.org/

AJIC Issue 23, 2019 - Full Issue

2019-06-28
LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://hdl.handle.net/10539/27538
The African Journal of Information and Communication (AJIC). (2019). Issue 23. https://doi.org/10.17159/2077-7213/2019/n23

Downloaded from a DSpace repository. https://dspace.org/

THE AFRICAN JOURNAL OF INFORMATION AND COMMUNICATION (AJIC)

ISSUE 23, 2019

RESEARCH ARTICLES

Asymmetry in South Africa's Regulation of Customer Data Protection: Unequal Treatment between Mobile Network Operators (MNOs) and Over-the-Top (OTT) Service Providers – *Stanley Shanapinda*

Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework – *Uche M. Mbanaso, Lucienne Abrahams, and Oghenevovwero Zion Apene*

A Proposed "Agricultural Data Commons" in Support of Food Security – *Jeremiah Baarbé, Meghan Blom, and Jeremy de Beer*

Towards a Tiered or Differentiated Approach to Protection of Traditional Knowledge (TK) and Traditional Cultural Expressions (TCEs) in Relation to the Intellectual Property System – *Chidi Oguamanam*

Treatment of Kenya's Internet Service Providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017 – *John Walubengo and Mercy Mutemi*

The Role of Discursive Constructions in Nigeria's ASUU-FGN Labour Conflict of 2013 – *Samuel Alaba Akinwotu*

PUBLICATION REVIEW

Book Review: Telecommunications Law and Regulation in Nigeria – *Reviewer: Peter Chukwuma Obutte*

Published by the LINK Centre
University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

The African Journal of Information and Communication (AJIC)

Issue 23, 2019

Published by the LINK Centre, School of Literature, Language and Media (SLLM)
Faculty of Humanities, University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre/ajic

Published since 2000, *The African Journal of Information and Communication (AJIC)* is a peer-reviewed, interdisciplinary, open access academic journal focused on information and communication ecosystems in Africa, elsewhere in the developing world, and at global level. Accredited by the South African Department of Higher Education and Training (DHET), *AJIC* pursues its open access objective by publishing online, free to the user, under a Creative Commons licence, and by not imposing article processing charges on its contributors.

Editorial Advisory Board

The journal is supported by an international editorial advisory board, comprising:
Lucienne Abrahams, University of the Witwatersrand, Johannesburg, South Africa
Hatem Elkadi, University of Cairo, Egypt
Nagy K. Hanna, author and international development strategist, Washington, DC, US
Joseph Kizza, University of Tennessee at Chattanooga, TN, US
Tawana Kupe, University of Pretoria, South Africa
Gillian Marcelle, Resilience Capital Ventures, Washington, DC, US
Uche M. Mbanaso, Nasarawa State University, Keffi, Nigeria
Caroline B. Ncube, University of Cape Town, South Africa
Tunji Oloapa, Ibadan School of Government and Public Policy (ISGPP), Nigeria
Ewan Sutherland, University of the Witwatersrand, Johannesburg, South Africa

Editors

Managing Editor: Tawana Kupe, Vice-Chancellor, University of Pretoria, South Africa, tawana.kupe@up.ac.za

Corresponding Editor: Lucienne Abrahams, Director, LINK Centre, Faculty of Humanities, University of the Witwatersrand, PO Box 601, Wits 2050, Johannesburg, South Africa, ajic.submissions@gmail.com

Publishing Editor: Chris Armstrong, Research Associate, LINK Centre, University of the Witwatersrand, Johannesburg, South Africa, chris.armstrong@wits.ac.za

Peer-Reviewing
AJIC acknowledges with gratitude the following peer reviewers of articles in this issue: Lucienne Abrahams, Ufuoma Akpojivi, Chris Armstrong, Pria Chetty, Victor Jaquire, Mike Madison, Manoj Maharaj, Robert Muthuri, Bitange Ndemo, and Marisella Ouma.

Production
Sub-editing: LINK Centre
Desktop-publishing: LINK Centre

This work is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

AJIC is published by the LINK Centre, School of Literature, Language and Media (SLLM), Faculty of Humanities, University of the Witwatersrand (Wits), PO Box 601, Wits 2050, Johannesburg, South Africa. The LINK Centre is headquartered at the Wits Tshimologong Digital Innovation Precinct, 41 Juta St., Braamfontein, Johannesburg, https://www.tshimologong.joburg

Past issues of *AJIC*, and its precursor *The Southern African Journal of Information and Communication (SAJIC)* are available at https://www.wits.ac.za/linkcentre/ajic and https://www.wits.ac.za/linkcentre/sajic

CONTENTS

RESEARCH ARTICLES

Asymmetry in South Africa's Regulation of Customer Data Protection: Unequal Treatment between Mobile Network Operators (MNOs) and Over-the-Top (OTT) Service Providers – *Stanley Shanapinda*

Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework – *Uche M. Mbanaso, Lucienne Abrahams, and Oghenevovwero Zion Apene*

A Proposed "Agricultural Data Commons" in Support of Food Security – *Jeremiah Baarbé, Meghan Blom, and Jeremy de Beer*

Towards a Tiered or Differentiated Approach to Protection of Traditional Knowledge (TK) and Traditional Cultural Expressions (TCEs) in Relation to the Intellectual Property System – *Chidi Oguamanam*

Treatment of Kenya's Internet Service Providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017 – *John Walubengo and Mercy Mutemi*

The Role of Discursive Constructions in Nigeria's ASUU-FGN Labour Conflict of 2013 – *Samuel Alaba Akinwotu*

PUBLICATION REVIEW

Book Review: Telecommunications Law and Regulation in Nigeria – *Reviewer: Peter Chukwuma Obutte*

RESEARCH ARTICLES

Asymmetry in South Africa's Regulation of Customer Data Protection: Unequal Treatment between Mobile Network Operators (MNOs) and Over-the-Top (OTT) Service Providers

Stanley Shanapinda
Research Fellow, Optus La Trobe Cyber Security Research Hub, La Trobe University, Melbourne; and Research Associate, LINK Centre, University of the Witwatersrand (Wits), Johannesburg

https://orcid.org/0000-0003-3961-2306

Abstract
This article examines the asymmetry that currently exists in South Africa in the regulatory treatment of customer data usage by mobile network operators (MNOs) and over-the-top (OTT) service providers. MNOs and OTTs must receive customer "consent", in terms of the Protection of Personal Information Act (POPI Act) and its Regulations, before sharing the customer's "personal information" with a third party. But MNOs have an additional requirement to meet, in terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), which is not applicable to OTTs: a requirement whereby a customer must provide "written authorisation" to an MNO before the MNO can share "communication-related information which relates to the customer concerned" with a third party. In this article, I examine and analyse provisions of the POPI Act, POPI Act Regulations, RICA, other relevant legislation, court decisions, records of a Parliamentary hearing, the standard terms and conditions and privacy policies of two South African MNOs (Vodacom and MTN), and two international OTT service providers (Google and Facebook). Based on the analysis, I argue that the unequal regulatory treatment between the MNOs and OTTs, if allowed to persist, threatens to undermine the growth of key elements of South Africa's digital economy.

Keywords
data protection, South Africa, regulatory asymmetry, mobile network operators (MNOs), over-the-top (OTT) service providers, Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), Protection of Personal Information Act (POPI Act), digital economy, competition, personal information, privacy, consumer protection, compliance, enforcement, regulatory uncertainty

DOI: https://doi.org/10.23962/10539/27536

Recommended citation
Shanapinda, S. (2019). Asymmetry in South Africa's regulation of customer data protection: Unequal treatment between mobile network operators (MNOs) and over-the-top (OTT) service providers. *The African Journal of Information and Communication (AJIC), 23,* 1–20. https://doi.org/10.23962/10539/27536

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: https://creativecommons.org/licenses/by/4.0

Acknowledgement
This article draws on content from the author's presentation at the 4th Annual Competition and Economic Regulation (ACER) Week Southern Africa conference in Johannesburg, 16-20 July 2018 (Shanapinda, 2018).

1. Introduction

The rise and rise of multinational content and communications service providers is evidence of the power of the digitally-enabled economy (Stoller, 2018). One feature of this digital economy is the erosion of mobile network operators' (MNOs') voice and SMS revenues due to their customers' increasing use of over-the-top (OTT) services such as WhatsApp (Facebook-owned), Google Hangouts, Skype (Microsoft-owned), and FaceTime (Apple-owned). These services are "over-the-top" in the sense that they operate via the internet, bypassing the MNOs' telecom platforms (BEREC, 2016). In South Africa, the two market-leading MNOs, Vodacom and MTN, have lobbied strongly, including at Parliament, for international OTT service providers to be regulated more heavily than they are at present, so as to make competition fairer between South African MNOs and the international OTTs (PMG, 2016).

When they were initially introduced, OTT services actually contributed to the bottom line of the MNOs. Customers used more mobile data when connecting to OTT services, and the MNOs were able to bill accordingly. But with mobile data becoming cheaper, this has led to reduced MNO data revenues, and when coupled with the decreased usage of traditional MNO SMS and voice services, this has begun to pose an increasing threat to the business models of the MNOs (see PMG, 2016; Stork et al., 2017). Accordingly, South Africa's MNOs are bundling OTT service offerings with their voice and SMS subscriber packages. The examples include the bundling of mobile money services, and zero-rated access to OTT web applications developed by the technology giants or their third-party associates (Stork, et al., 2017).

At the same time, South African MNOs are increasingly seeking to enter the realm of the digital economy that revolves around use of customer data, including use of customer personal information. For example, Vodacom's Vision 2020 strategy calls on it to develop deep insights about customer needs, wants, and behaviours, and to provide personalised service offerings, through the use of big data analytics, machine learning, and artificial intelligence (Vodacom, 2017a, pp. 24, 28; 2018a; 2018b). A key Vodacom strategy is "[m]onetising mobile data" via its digital products and services (Vodacom 2017b, pp. 24–25). Vodacom aims to collaborate with third-party partners to deliver services relating to social media, music, gaming, and social data-sharing, supported by personalised offers. One such partnership is with Microsoft and its Azure cloud platform, allowing development, testing, management, and storing of mobile web apps (Microsoft, n.d.; Vodacom 2017b, p. 24).

To this end, in May 2018, Vodacom advertised the position of "Senior Specialist Information Security", an employee who would ensure that information security-related policies were drafted and reviewed periodically, and that Vodacom complied with local and international laws regarding information security and data privacy. On the same day, Vodacom advertised the position of "Senior Insights Manager", an employee who would research customers, profile them, and seek ways to monetise the findings (Vodacom, 2018c).

Competing MNO and OTT provider positions in Parliamentary hearings

Meanwhile, as they attempt to compete with international OTT service providers, South African MNOs contend with certain domestic regulatory requirements that the international OTT service providers do not face, including universal service and access regulations, tariff regulations, taxation, and—the focus of this article—heavier-touch regulation in respect of the sharing of customer data (PMG, 2016).

Leading South African MNOs Vodacom and MTN, made their objections to this apparently lighter-touch treatment of OTT service providers known in the 2016 hearing of the Parliamentary Portfolio Committee on Telecommunications and Postal Services (PMG, 2016). They contended that OTT service providers were being granted an unfair advantage over legacy networks and services. They claimed the MNOs' regulatory burden was "excessive" and created competitive disadvantages for them compared to international OTT services (PMG, 2016). At the same 2016 Parliamentary hearing at which the South African MNOs complained of unfair treatment, representatives of international OTT service providers argued that MNOs and OTT service providers are in a symbiotic relationship, and that OTT service providers should not be burdened with the same "cumbersome" regulations that the South African MNOs carry. OTT service providers suggested that, instead, the "cumbersome and outdated regulation holding back the network operators" should be removed (PMG, 2016).

Stork, Esselaar, and Chair (2017) argue—broadly in line with one of the core arguments put forward by the international OTT service providers in the 2016 Parliamentary hearing—that although OTT services present a threat to domestic MNO voice and SMS revenues, they also present opportunities for the domestic MNOs (through, for example, zero-rating of OTT services) to gain market share. Other writers, meanwhile, share the MNOs' concern that MNOs are over-regulated in comparison to OTT service providers (Ganuza & Viecens, 2014; Jayakar & Park, 2014; Krämer & Wohlfarth, 2018; Peitz & Valletti, 2015; Sujata et al., 2015).

One of the complaints from the MNOs at the 2016 Parliamentary hearing was that OTT service providers sell on subscriber personal information that they collect while providing OTT services to South African MNO subscribers (PMG, 2016). However, international OTT service provider representatives at the hearing denied that they engaged in this practice. It is this matter—the treatment of customer personal data—that is at the heart of this article. Specifically, this article engages with the reality that, in the South African regulatory dispensation, domestic MNOs face more stringent requirements in their treatment of customer data than the requirements faced by the international OTTs.

Research outline

The focus of my research for this article was not on the full range of South African regulatory matters potentially affecting both MNOs and OTT service providers. Rather, my focus was on one regulatory element: the regulatory requirements regarding the treatment of customer data, and specifically the requirements that must be followed before an operator can share customer data with a third party.

My research focused on the data-sharing provisions of two South African statutes: the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA) of 2002 (hereafter "RICA", as amended by the Electronic Communications Act (ECA) of 2005 and the RICA Amendment Act of 2008); and the Protection of Personal Information Act (POPI Act) of 2013 (hereafter "the POPI Act"). RICA has been in force since September 2005, while the POPI Act is not yet, at the time of finalising this article in June 2019, in force, and is expected to come into force in late 2019 or in 2020, with a 12-month grace period.

In addition to examining the provisions of these two South African Acts, I examined the POPI Act Regulations of 2018, other relevant South African laws, records from the proceedings of the aforementioned 2016 Parliamentary hearing on OTT regulation, the standard terms and conditions and privacy policies of two South African MNOs (Vodacom and MTN), and the standard terms and conditions and privacy policies of two international OTT service providers (Google and Facebook).

In the remainder of this article, I outline my findings from the above-listed primary documents, and I provide my argument, based on the findings, that: (1) there is clear regulatory asymmetry in South Africa, in respect of customer data protection regulation, between the treatment of domestic MNOs and international OTT service providers; and (2) this asymmetry potentially undermines the South African MNOs' ability to compete with OTT services and, more generally, to adapt to, and prosper in, fast-changing national and international digital economies. (At the same time, I am cognizant of, and in agreement with, arguments (see, for example, Krämer & Wohlfarth, 2018) that data protection regulation is necessary and that, when correctly calibrated, such regulation can be pro-competitive.

2. Data-sharing authorisation/consent provisions in RICA and the POPI Act

RICA written authorisation requirement

In terms of South Africa's RICA of 2002 as amended, South African electronic communication service providers,[1] including MNOs, are required to store "communication-related information" for law enforcement purposes (sects. 30(1)(b), 40(3)(b), 40(4)(a), 40(9), 40(10)). RICA defines communication-related information as:

> […] any information relating to an indirect communication which is available in the records of an electronic communication service provider, and includes switching, dialing or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, if each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such an electronic communication service provider and, where applicable, the location of the user within the electronic communication system; […] (RICA, sect. 1(1)).

In terms of RICA's sections 1, 39(1)(a), and 39(2), communication-related information includes internet protocol (IP) addresses; uniform resource locators (URLs); location information for mobile devices; international mobile subscriber identity (IMSI) numbers (serial numbers of SIM cards); and international mobile equipment identity (IMEI) numbers (serial numbers on mobile devices) (see Shanapinda, 2016a; 2016b; Sutherland, 2017, p. 102). (A customer's communication-related information is hereafter referred to in this article as "RICA data").

1 RICA's references, in the original 2002 Act, to "telecommunication service provider", "telecommunication service", and "telecommunication system", were amended, respectively, to "electronic communication service provider", "electronic communication service", and "electronic communication system", by section 97 of the Electronic Communications Act (ECA) 36 of 2005.

Section 12 of RICA sets out restrictions on the sharing of RICA data:

> Subject to this Act, no electronic communication service provider or employee of an electronic communication service provider may intentionally provide or attempt to provide any real-time or archived communication-related information to any person other than the customer of the electronic communication service provider concerned to whom such real-time or archived communication-related information relates. (RICA, sect. 12)

In section 14, RICA sets out an exception in terms of which RICA data can be shared with a third party:

> Any electronic communication service provider may, upon the *written authorisation* given by his or her customer on each occasion, and subject to the conditions determined by the customer concerned, provide to any person specified by that customer, real-time or archived communication-related information which relates to the customer concerned. (RICA, sect. 14) (emphasis added)

In terms of RICA's written authorisation requirement, MNOs may not, without "written authorisation" from the customer, provide, or attempt to provide, any RICA data to any third party—except for provision to a law enforcement agency (sects. 12, 14, 42 and 43). In terms of section 14, the customer's written authorisation must be provided "on each occasion" of data-sharing, under "conditions determined by the customer", and in cases of sharing of information "which relates to the customer concerned." This RICA requirement that the customer provide written authorisation for third-party sharing of her or his RICA data is hereafter referred to in this article as the "RICA written authorisation requirement".

Of relevance to the matter of "written authorisation" are the provisions in sections 12 and 13(1) to 13(3) of South Africa's Electronic Communications and Transactions (ECT) Act of 2002. In terms of these provisions, an authorisation could be considered to be in writing, and signed, even if the written document or the written information is in the form of an electronic data message, such as an e-mail, provided that the information is accessible in a manner that is usable. Also of relevance is South Africa's *Spring Forest Trading CC v Wilberry* case of 2014, in which the Supreme Court of Appeal decided that e-mail communications can form legally binding agreements—when the contract is required to be in writing and the parties have agreed on the need for signatures but have not explicitly stated how the signatures must be executed. The implications of the ECT Act and the *Spring Forest Trading CC v Wilberry* decision are that customers of MNOs could potentially provide "written authorisation", via email, to have their data shared, without signing a hard-copy instruction. However, the standard terms and conditions of South African MNOs Vodacom and MTN,

and their privacy policies, make no reference to this mode of obtaining a customer's written authorisation.

In the absence of written authorisation by the customer or a law enforcement requirement, RICA specifies that an electronic communication service provider (e.g., an MNO, for the purposes of this article) may not provide a customer's RICA data directly to any other entity apart from the customer. The "customer" is defined as:

> […] any person-
> *(a)* to whom an electronic communication service provider provides an electronic communications service, including an employee of the electronic communication service provider or any person who receives or received such service as a gift, reward, favour, benefit or donation;
> *(b)* who has entered into a contract with an electronic communication service provider for the provision of an electronic communications service, including a pre-paid electronic communications service; or
> *(c)* where applicable-
>
> (i) to whom an electronic communication service provider in the past has provided an electronic communications service; or
>
> (ii) who has, in the past, entered into a contract with an electronic communication service provider for the provision of an electronic communications service, including a pre-paid electronic communications service;
>
> [Definition of 'customer' substituted by s. 1 *(b)* of Act 48 of 2008.] (RICA, sect. 1(1))

These requirements in RICA do *not* apply to OTT service providers, because OTT service providers are not electronic communication service providers in terms of RICA and the ECA.

Meanwhile, there is convincing evidence that OTT service providers share the IP addresses, location information, IMSIs and IMEIs of South African customers with third parties (Binns et al., 2018; Dance, 2018; Facebook, 2018; Google, n.d.). During the aforementioned 2016 Parliamentary hearings, OTT service providers specified that they do not "sell" customer data to third parties. But the terms and conditions of Facebook and Google state that they "share" customer data, leaving unstated whether such sharing is in effect "selling". This lack of clarity is further complicated by the vagueness displayed by OTT service providers in respect of distinctions between what is *personal* data and what is *anonymised* data. Is it perhaps the case that personal data are not "sold" to third parties, while anonymised data are sold on? Is personal data anonymised and then "shared" but not "sold"? What precisely constitutes the "selling" of data? If a tech giant and a third party agree on a revenue-sharing arrangement, based on the development of a product reliant on the "exchange" of data (i.e., via use of neutral terms that do not specify "sale" of the data or that the data are "personal"),

does that not still constitute sale of the data? My argument, for the purposes of this article, is that the data, whether arguably personal or not, is, in such exchanges, shared in a manner that results in a commercial arrangement, regardless of whether the data is directly or indirectly "sold"—because both parties benefit commercially in the end.

POPI Act consent requirement

The POPI Act of 2013, which is expected to come into force in late 2019 or 2020, aims, among other things, to level the competitive playing field in respect of data protection regulation in South Africa. Both the domestic MNOs and international OTTs will equally be subject to the provisions of the POPI Act when it comes into force. The Act states that two of its purposes are as follows:

> (a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—
>
> (i) balancing the right to privacy against other rights, particularly the right of access to information; and
>
> (ii) protecting important interests, including the free flow of information within the Republic and across international borders;
>
> (b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information; [...] (POPI Act, sect. 2(a)-(b))

The Preamble to the POPI Act states that it regulates the flow of information:

> […] consonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information; […] (POPI Act, Preamble)

Under the POPI Act, MNOs and OTT service providers are considered "responsible parties" in respect of their processing of "personal information", and "personal information" may only be collected and shared by "responsible parties" when "[…] necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied" (POPI Act, sect. 11(1)(f)).

A key test under the POPI Act in respect of sharing customer data—a test that must be applied by both MNOs and OTTs—is whether or not any given set of customer data constitutes "personal information" in terms of the Act. Only data that does *not* constitute "personal information" in terms of the Act can be "processed" without customer "consent" (with "processing" being a set of activities that includes "dissemination"). Sect. 1 of the POPI Act defines "personal information" as:

> […] information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
> (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social
> origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
> (b) information relating to the education or the medical, financial, criminal or employment history of the person;
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
> (d) the biometric information of the person;
> (e) the personal opinions, views or preferences of the person;
> (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
> (g) the views or opinions of another individual about the person; and
> (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person; […] (POPI Act, sect. 1)

As stated above, the Act prohibits the "processing", without customer "consent", of "personal information", with "processing" defined as:

> […] any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
> (b) dissemination by means of transmission, distribution or making available in any other form; or
> (c) merging, linking, as well as restriction, degradation, erasure or destruction of information; […]. (POPI Act, sect. 1)

However, section 6 of the POPI Act states:

> 6. (1) This Act does not apply to the processing of personal information—
> […]
> (b) that has been de-identified to the extent that it cannot be re-identified again; […]. (POPI Act, sect. 6(1)(b))

The effect of section 6(1)(b) is that "personal information" is no longer treated by the Act as "personal information" if it has been anonymised ("de-identified"). Thus, no consent is required to engage in "processing", including sharing, of such data. The "consent" that is required for sharing of "personal information" is defined in section 1 as:

> […] any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information. (POPI Act, sect. 1)

This POPI Act requirement is hereafter referred to as the "POPI Act consent requirement".

Section 69 of the POPI Act deals with one specific type of data-sharing with third parties: processing for the purposes of "[d]irect marketing by means of unsolicited electronic communications". In terms of section 69(1), MNOs and OTT service providers, as "responsible parties", must obtain the consent of the individual customer to collect and share the customer's personal information for direct marketing purposes by means of electronic communications such as email and when automated decisions are made about the individual:

> 69.(1) The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject—
>
> (a) has given his, her or its consent to the processing; or
>
> (b) is, subject to subsection (3), a customer of the responsible party.

In respect of data processing for direct marketing, the POPI Act Regulations of 2018 specify that a data subject (i.e., a customer) must provide "written" consent, via a form ("Form 4") provided in the Regulations, for processing of personal data for direct marketing. But instances of sharing of data with third parties for purposes other than direct marketing, the Regulations do not specify the form that the consent must take.

Regulatory asymmetry

Table 1 summarises the contrasting requirements, under RICA and the POPI Act respectively, in respect of operators' sharing of customer data with third parties.

Table 1: RICA and POPI Act requirements for sharing customer data

RICA requirements	**POPI Act requirements**
Requirements apply to MNOs, but *not* to OTTs.	Requirements apply to *both* MNOs and OTTs.
Requirements apply to "communication-related information which relates to the customer concerned".	Requirements apply to "personal information".
In order to share "communication-related information which relates to the customer concerned" data, MNOs must secure "written authorisation by [the] customer".	In order to share a customer's "personal information", both MNOs and OTTs must secure "consent" in the form of "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information". Consent must, in terms of the POPI Act Regulations, be *written* when the processing of personal information is for the purposes of "direct marketing". The form of consent is *not specified* for other kinds of processing and third-party sharing of personal information.

Under the POPI Act consent requirement, MNOs and OTT service providers have the same obligations. Meanwhile, MNOs are, at the same time, required to also comply with the RICA written authorisation requirement. Thus, when the POPI Act comes into force, MNOs will be required to comply with two tests, the RICA test and the POPI Act test, when sharing customer data with third parties. When the POPI Act comes into force, MNOs will be required to continue to obtain customer written authorisation in terms of RICA *and* to start to obtain customer consent in terms of the POPI Act. OTT service providers, meanwhile, will only need to start to comply with the POPI Act consent requirement. There is clear regulatory asymmetry here.

There is also the potentially significant difference, as seen in Table 1, between the two Acts' wordings in respect of what customer information is being dealt with, i.e., the potential difference between the phrases "communication-related information that relates to the customer concerned" and "personal information". Under RICA, the scope of customer data is apparently broad, covering many types of communication-related data—whether potentially *personal* information or not—as long as the data is "communication-related" and also "relates to the customer concerned". This is

arguably a significantly higher hurdle to jump than the hurdle presented by the narrower "personal information" specification under the POPI Act. In other words, the MNOs are likely, in terms of RICA, to need to obtain authorisation for data-sharing with third parties in a broader range of cases than the cases in which OTTs and MNOs will be required to obtain consent in terms of the POPI Act.

The legal meaning of the POPI Act's "consent" and "personal information" provisions will almost certainly require interpretation by the courts, along with RICA's "written authorisation" and "communication-related information which relates to the customer concerned" provisions. And these provisions may also need to be legally interpreted in relation to each other, e.g., a judicial ruling is likely to be necessary to decide the extent to which the term "communication-related information that relates to the customer concerned" under RICA equates to "personal information" under the POPI Act. Where it is determined that the information to be shared with a third party does *relate to* the customer (in terms of RICA), the MNO would apparently be bound to obtain written authorisation from the customer. And where the same information is determined to be *personal* (in terms of the POPI Act), the MNO would apparently need to also obtain the consent of the customer—with that consent needing to be in writing if the data is to be used for direct marketing.

The OTTs must comply with one act, while the MNOs must comply with two, and, as demonstrated above, there is every reason to believe that the compliance realities will be different between the two Acts (see also Mayer et al., 2016; Shanapinda, 2016a; 2016b). This higher compliance threshold for MNOs than for OTT providers is clearly to the benefit of the OTTs. There will be, in effect, two "tests" at play here, outlined in two separate but complementary pieces of law, and it would seem to be inevitable that the two tests will, in many instances, produce two different outcomes—and therein lies the South African regulatory asymmetry between the treatment of MNOs and OTT service providers in respect of sharing of customer data with third parties.

Enforcement of the RICA and POPI Act provisions

It is also important to note that RICA does not provide for oversight to ensure that the written authorisation requirement is complied with prior to an operator sharing RICA data with a third party. Moreover, there is no enforcement mechanism in cases where data-sharing with a third party occurs without the required written authorisation (RICA, sect. 50(2)). This leaves customer privacy poorly protected under RICA. The POPI Act creates a body called the Information Regulator, mandated to educate on, monitor, and enforce compliance (sects. 39, 40). The Information Regulator will have the power to impose fines or imprisonment (sects. 107 and 109). Thus, in the future, when the POPI Act is in force, the Information Regulator will monitor and enforce POPI Act compliance equally for both MNOs and OTT service providers.

3. MNO and OTT data-sharing policies and practices

I found, through my primary document analysis, that the privacy policies and standard terms and conditions, of the leading South African MNOs (Vodacom, MTN), and of the leading OTT service providers (Facebook, Google), were materially similar. They all claim to obtain the consent of the customer before sharing customer data with third parties to, for instance, research, develop and deliver existing or new digital products and services (Facebook, n.d.; Google, n.d.; MTN, n.d.; Vodacom, n.d.a). The MNOs appear to have adopted similar terms and conditions to those of the OTT service providers. And a key similarity I was able to identify—a key similarity for the purposes of the focus of my research—was that the privacy policies of both the MNOs and the OTT service providers lacked any reference to a written authorisation requirement.

Google shares customer data with third parties, e.g., third parties identify and track user devices in the Google Play store's mobile ecosystem. The nature of the business of identifying, tracking, and sharing data about users and their devices is a transnational business (Binns, et al., 2018; Dance, 2018). The Vodacom and MTN privacy policies, as with the Facebook and Google policies, state that the operators disclose customer information to third parties. But the policies do not specify whether or not this information is disclosed based only on conditions set by the customer, and only to third parties specified by the customer—i.e, the practices required by the RICA written authorisation requirement (Vodacom, n.d.a; n.d.b; n.d.c; MTN, n.d.; Facebook; n.d.; Google, n.d.). Thus, it would appear that the RICA written authorisation requirement is not being fully met by existing MNO standard terms and conditions and privacy policies. This apparent lack of compliance with the RICA written authorisation requirement contradicts RICA's apparent anticipation of a scenario whereby there is a form of dialogue and consultation between customers and South African communication service providers, i.e., a situation where customers know their rights and are in a position to influence the terms of how their RICA data are shared, as opposed to having the terms dictated by the MNOs.

It was also noted above that RICA does not provide for any oversight or enforcement of its written authorisation requirement. According to the OTT service providers, South African customers could rely on protection under their local laws and court systems if seeking to challenge whether an OTT's data-sharing behaviour obeyed local laws (Facebook; n.d.; Google, n.d.). But in respect of OTT data-sharing behaviour, since only RICA (and not the POPI Act) is currently in effect—and since the RICA written authorisation requirement does not regulate OTT service providers—there is at present no clear legal protection for the South African customer in respect of sharing of its MNO data with third parties. Since the OTT service providers are not required to comply with the RICA written authorisation requirement, the standard terms and conditions of the OTT service providers would be difficult to challenge. The privacy policies of the OTT service providers are therefore essentially unregulated and

unchecked at present in South Africa, allowing the OTT service providers to participate in third party data-sharing arrangements without any limits.

The longer the commencement of the POPI Act is delayed, the longer the OTTs' practices become entrenched and increasingly difficult to review. At present, and up until the POPI Act takes effect, the OTT service providers can be regarded as self-regulatory in respect of how they treat the data they collect from South African customers. And the OTT service providers can, on their own initiative, update their terms and conditions at any time (Facebook, n.d.; Google, n.d.).

An example of OTT service providers' resistance to the regulation of their data-handling practices was provided by Facebook's transfer of customer data out of Ireland in April 2018, in order to avoid having the data fall under the EU's General Data Protection Regulation (GDPR), which came into force on 25 May 2018 (Hern, 2018).

4. RICA, the POPI Act, and regulation of the digital economy

RICA and the POPI Act outline legal requirements, and limitations, in respect of privacy, data protection, and data access for law enforcement. These laws seek to encourage competitive participation in the digital economy and, at the same time, to set restrictions on such participation.

The RICA written authorisation requirement imposes data protection regulations directly on private and public entities, thus potentially modifying, indirectly, the economic behaviour of these businesses. The aim is to ensure that digital services are created and delivered in a secure environment that respects privacy and allows legitimate businesses to function effectively and profitably. The RICA written authorisation requirement is a measure that potentially, indirectly, influences the economic behaviour of South African MNOs, potentially helping to achieve the public interest aims of: customer control over use of personal data; and the prevention of misuse of customer personal data.

As discussed above, it would appear that South African MNOs are at present not fully compliant with the RICA written authorisation requirement. It would appear that they are deploying digital products and services using RICA data and sharing the data with third parties, seeking to realise forward-looking digital economy strategies—with, it would seem, little regard for the RICA regulatory requirements, and/or with an absence of good faith effort towards ensuring minimal or material compliance. This may be because the compliance burden is too heavy to bear, or it may be a calculated business decision by MNOs to not comply and deal with allegations of non-compliance if and when they arise. Not moving ahead with digital strategies grounded in the sharing of customer data may be seen by MNOs as a business imperative, with, accordingly, the risks of RICA non-compliance seen as

negligible given the absence, in RICA, of monitoring and enforcement mechanisms. At present, it seems fair to say that RICA is allowing MNOs to use RICA data, originally collected for possible sharing for law enforcement purposes, for commercial purposes. The non-enforcement of the RICA written authorisation requirement appears to be allowing the MNOs to share the data about their customers with third parties, in an effort to more fully participate in the digital economy, without fear of penalties for misuse of the RICA data.

5. Potential future impacts of the asymmetric RICA written authorisation requirement

As long as RICA's written authorisation requirement remains in place for the sharing of customer data with third parties, there are several possible scenarios that could emerge—all potentially impacting the digital services ecosystem—and they are not mutually exclusive.

Continued MNO non-compliance

Not complying with the RICA written authorisation requirement enables MNOs to more realistically consider: developing their own OTT services; entering into partnerships with OTTs to deliver OTT services; entering into data-processing mergers and acquisitions; and commercially sharing RICA data with third parties able to process the data to research and develop innovative products and services. Non-compliance provides the MNOs with enhanced opportunities to diversify their businesses in the mobile ecosystem, to advance their participation in digital services and the digital economy, and to enter into revenue-sharing arrangements.

Consumer activism and corporate citizenship requirements

Despite the absence, in RICA, of monitoring and enforcement mechanisms for the written authorisation requirement, MNO non-compliance could nevertheless subject the MNOs to potential legal risks. A consumer association or privacy protection organisation could legally challenge MNOs under South Africa's Consumer Protection Act (CPA) of 2008. Under the CPA, the customer has the right to fair, just, and reasonable terms and conditions (sects. 48–52), and the customer is protected against improper trade practices and deceptive, misleading, unfair, or fraudulent conduct (sect. 3(1)(d)). Under the CPA, MNOs must act responsibly and inform customers of their rights (CPA, sect. 3(1)(a), (c)–(f)). The privacy policies and standard terms and conditions of the MNOs, in omitting references to the RICA written authorisation requirement, could be questionable in terms of the CPA. Consumer rights in this area could be enforced by the National Consumer Tribunal if complaints against the MNOs were to be lodged with the Tribunal (CPA, sects. 69, 71).

Additionally, under South Africa's King IV Code, in terms of which South African companies must act ethically and establish ethics committees, MNOs should in fact incorporate the RICA written authorisation requirement in their privacy policies,

standard terms and conditions, and risk assessment and management policies (PwC, 2017, p. 30).

MNO compliance

Complying with the RICA written authorisation requirement would likely be extremely burdensome, both operationally and financially, for South African MNOs. Compliance could negatively impact MNOs' efforts to more fully partake in the digital economy, while OTT service providers would be able to continue to operationalise their data-sharing arrangements with complete freedom (until the POPI Act comes into force, and with relative freedom even under the POPI Act).

Increased MNO take-up of zero-rated OTT services

According to Stork et al. (2017) and Feasey (2015), South African MNOs may adopt the strategy of increasingly bundling zero-rated products from OTT service providers into their MNO offerings. Vodacom followed this approach by bundling a zero-rated music-streaming OTT offering into its packages—but found, however, that it was not able to effectively compete in the digital content space because of a lack of access to content at reasonable rates (Vodacom, 2017b, p. 23). This may have contributed to Vodacom's adoption of its aforementioned Vision 2020 push to more aggressively seek a leading place in the digital content ecosystem.

Regulatory uncertainty

Under the CPA, MNOs face regulatory uncertainty, as informed customers may rebel and lobby for regulatory action to protect their privacy and data usage rights. OTT service providers, meanwhile, have minimal concerns of this nature, as they are not subject to the RICA written authorisation requirement that makes MNOs vulnerable under the CPA. MNOs need regulatory certainty, just as OTT service providers do, in order to fully partake in the digital economy, i.e., in order to partake without fearing unpredictable regulatory interventions that affect their digital economy strategies.

6. Conclusion

As this study has shown, RICA's written authorisation requirement, which requires MNOs but not OTT service providers to get customer written authorisation before sharing data with third parties, creates a regulatory asymmetry. This asymmetry imposes an unfair regulatory burden on the MNOs as they face competition from OTT service providers and, more generally, seek to grow digital businesses not reliant on traditional voice and SMS offerings.

The MNOs appear, at present, to be disregarding the RICA written authorisation requirement—a course of action made possible by the absence, in RICA, of monitoring or enforcement mechanisms for the requirement, and by the absence, to date, of consumer complaints raised and submitted to the National Consumer Tribunal. The

privacy policies of South Africa's two market-leading MNOs, Vodacom and MTN, do not make any reference to the RICA written authorisation requirement.

MNOs appear to be left with a dilemma, whereby they must choose either (1) to continue to disregard the RICA written authorisation requirement, and risk sanction, so as to push aggressively forward with digital propositions reliant on the sharing of customer data with third parties; or (2) to seek to comply with the RICA written authorisation requirement, so as to avoid the risk of sanction, and, accordingly, be less aggressive in the pursuit of new digital business models based on customer data-sharing.

Based on the findings and analysis produced by this study, it seems clear that the RICA written authorisation requirement needs to be harmonised with the POPI Act's lighter-touch consent requirement. Such harmonisation would: (1) reduce the severity of RICA's current asymmetric burden on MNOs in respect of the customer consent threshold for third-party-sharing of customer data; and (2) allow for the elimination of the asymmetry entirely when the POPI Act's consent requirement, which applies equally to both MNOs and OTT service providers, comes into effect in the near future. Once the POPI Act comes into force, consideration could then be given to removing the customer authorisation requirement entirely from RICA and making customer authorisation under RICA subject to the provisions of the POPI Act.

References

South African Acts and Regulations

Consumer Protection Act 68 of 2008.

Electronic Communications and Transactions (ECT) Act 25 of 2002.

Electronic Communications Act (ECA) 36 of 2005.

Protection of Personal Information Act (POPI Act) 4 of 2013.

Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA) 70 of 2002.

Regulation of Interception of Communications and Provision of Communication Related Information Amendment Act (RICA Amendment Act) 48 of 2008.

Information Regulator: Protection of Personal Information Act, 2013 (Act No. 4 of 2013): Regulations Relating to the Protection of Personal Information, 2018. *Government Gazette*, No. 42110, No. R. 1383, 14 December.

Other Sources

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. In WebSci '18: 10th ACM Conference on Web Science, May 27–30, Amsterdam. New York: ACM. https://doi.org/10.1145/3201064.3201089

Body of European Regulators for Electronic Communications (BEREC). (2016). *Report on OTT services*. Retrieved from https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services

Dance G. J. X., Confessore N., & LaForgia, M. (2018, June 3). Facebook gave device makers deep access to data on users and friends. *New York Times*. Retrieved from https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html

European Union (EU). (2016). General Data Protection Regulation (GDPR) 2016/679 (implementation date: 25 May 2018).

Feasey, R. (2015). Confusion, denial and anger: The response of the telecommunications industry to the challenge of the Internet. *Telecommunications Policy*, *39*(6), 444–449. https://doi.org/10.1016/j.telpol.2014.08.007

Facebook. (n.d.). Terms of service. Retrieved from https://www.facebook.com/legal/terms/update

Ganuza, J. J., & Viecens, M. F. (2014). Over-the-top (OTT) content: Implications and best response strategies of traditional telecom operators. Evidence from Latin America. *Digital Policy, Regulation and Governance*, *16*(5), 59–69. https://doi.org/10.1108/info-05-2014-0022

Google. (n.d.). Google privacy policy. Retrieved from https://policies.google.com/privacy

Hern, A. (2018, April 19). Facebook moves 1.5bn users out of reach of new European privacy law. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law

Jayakar, K., & Park, E.-A. (2014). Emerging frameworks for regulation of over-the-top services on mobile networks: An international comparison. Paper presented to TPRC Conference, 31 March. https://dx.doi.org/10.2139/ssrn.2418792

Krämer, J., & Wohlfarth, M. (2018). Market power, regulatory convergence, and the role of data in digital markets. *Telecommunications Policy*, *42*(2), 154–171. https://doi.org/10.1016/j.telpol.2017.10.004

Mayer, J., Mutchler, P., & Mitchell, J. C (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences of the United States of America*, *113*(20), 5536–5541. https://doi.org/10.1073/pnas.1508081113

Microsoft. (n.d.). Microsoft Azure. Retrieved from https://azure.microsoft.com/en-us/services/app-service/

MTN (n.d.). Terms and conditions. Retrieved from https://www.mtn.co.za/Pages/Termsandconditions.aspx?pageID=26

Peitz, M., & Valletti, T. (2015). Reassessing competition concerns in electronic communications markets. *Telecommunications Policy*, *39*(10), 896–912. https://doi.org/10.1016/j.telpol.2015.07.012

Parliamentary Monitoring Group (PMG). (2016) Over-the-Top (OTT) policy and regulatory options Meeting Summary. 26 January. Cape Town: Portfolio Committee on Telecommunications and Postal Services, Parliament of South Africa. Retrieved from https://pmg.org.za/committee-meeting/21942/

PricewaterhouseCoopers (PwC). (2017). Governing structures and delegation – A comparison between King IV TM and King III. Retrieved from https://www.pwc.co.za/en/assets/pdf/king-iv-comparison.pdf

Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4

Shanapinda, S. (2016a). Retention and disclosure of location information and location identifiers. *Australian Journal of Telecommunications and the Digital Economy*, *4*(4), 251–279. https://doi.org/10.18080/ajtde.v4n4.68

Shanapinda, S. (2016b). The types of telecommunications device identification and location approximation metadata: Under Australia's warrantless mandatory metadata retention and disclosure laws. *Communications Law Bulletin*, *35*(3), 17–19.

Shanapinda, S. (2018). OTT wars in South Africa: The privacy and cybersecurity regulatory asymmetry and how it complicates advancing the digital economy fairly - a theoretical perspective. Presentation to the 4th Annual Competition and Economic Regulation (ACER) week Southern Africa conference in Johannesburg, 16-20 July. Retrieved from https://www.competition.org.za/acer-conference-papers

Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and Another (725/13) [2014] ZASCA 178; 2015 (2) SA 118 (SCA) (21 November 2014). Retrieved from http://www.saflii.org/za/cases/ZASCA/2014/178.pdf

Stoller, K. (2018, June 6). The world's largest tech companies 2018: Apple, Samsung take top spots again. *Forbes*. Retrieved from https://www.forbes.com/sites/kristinstoller/201nu898/06/06/worlds-largest-tech-companies-2018-global-2000/#6354683c4de6

Stork, C., Esselaar, S., & Chair, C., (2017). OTT - threat or opportunity for African MNOs? *Telecommunications Policy*, *41*(7–8), 600–616. https://doi.org/10.1016/j.telpol.2017.05.007

Sujata, J., Sohag, S., Tanu, D., Chintan, D., Shubham, P., & Sumit, G. (2015). Impact of over the top (OTT) services on telecom service providers. *Indian Journal of Science and Technology, 8*(S4), 145–160. https://doi.org/10.17485/ijst/2015/v8iS4/62238

Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication (AJIC), 20*, 83–112. https://doi.org/10.23962/10539/23574

Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015)

Vodacom. (2017a). *Best technology*. Retrieved from http://www.vodacom-reports.co.za/integrated-reports/ir-2017/best-technology.php

Vodacom. (2017b). *Vodacom Group Limited integrated report for the year ended 31 March 2017*. Retrieved from http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf

Vodacom. (2018a, April 18). Vodacom accelerates digital transformation with first-to-market launch of suite of Azure solutions. Press release. Retrieved from http://www.vodacom.com/news-article.php?articleID=4472

Vodacom. (2018b, May 10). Vodacom puts its partners in the driving seat of digital transformation. Press release. Retrieved from http://www.vodacom.com/news-article.php?articleID=4476

Vodacom (2018c). Senior specialist information security. Job advertisement. LinkedIn. Retrieved from https://www.linkedin.com/jobs/view/686527109

Vodacom (2018d). Senior insights manager. Job advertisement. LinkedIn.

Vodacom. (n.d.a). Privacy policy. Retrieved from http://www.vodacom.co.za/vodacom/terms/privacy-policy

Vodacom. (n.d.b). Vodacom app store terms and conditions. Retrieved from https://myvodacom.secure.vodacom.co.za/vodacom/terms/vodacom-app-store-terms-and-conditions

Vodacom. (n.d.c). Groups. Retrieved from https://www.vodacombusiness.co.za/cs/groups/public/documents/document/azure-brochure.pdf

Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework

Uche M. Mbanaso
Director, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria; and Visiting Researcher, LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://orcid.org/0000-0003-2784-7415

Lucienne Abrahams
Director, LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://orcid.org/0000-0002-5219-8448

Oghenevovwero Zion Apene
PhD student, Computer Science Department, Nasarawa State University, Keffi, Nigeria
https://orcid.org/0000-0001-8051-2695

Abstract
African countries are at high risk with respect to cybersecurity breaches and are experiencing substantial financial losses. Amongst the top cybersecurity frameworks, many focus on guidelines with respect to detection, protection and response, but few offer formal frameworks for measuring actual cybersecurity resilience. This article presents the conceptual design for a cybersecurity resilience maturity measurement (CRMM) framework to be applied in organisations, notably for critical information infrastructure (CII), as part of cyber risk management treatment.

The main thrusts of the framework are to establish, through assessment in terms of quantitative measures, which cybersecurity controls exist in an organisation, how effective and efficient these controls are with respect to cybersecurity resilience, and steps that need to be taken to improve resilience maturity. The CRMM framework we outline is conceptualised as being applicable both pre- and post-cyber attack. Drawing on the NIST cybersecurity framework (NIST CSF) and other relevant frameworks, the CRMM approach conceptualised in this article would be able to depict an organisation's cybersecurity practices and gauge the organisation's cybersecurity maturity at regular intervals. This CRMM approach is grounded in the idea that, by quantifying an organisation's current practices against established baseline security controls and global best practices, the resulting status measurement can provide the appropriate basis for managing cyber risk in a consistent and proportionate fashion. The CRMM framework defines four cybersecurity resilience quadrants (CRQs), which depict four different degrees of organisational preparedness, in terms of both risk and resilience.

Keywords
cybersecurity, cybersecurity resilience maturity measurement (CRMM), cybersecurity resilience quadrants (CRQs), critical information infrastructure (CII), NIST cybersecurity framework (NIST CSF), cyber risk management, cybersecurity resilience, cybersecurity controls

DOI: https://doi.org/10.23962/10539/27535

Recommended citation
Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. *The African Journal of Information and Communication (AJIC), 23*, 1–26.
https://doi.org/10.23962/10539/27535

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:
https://creativecommons.org/licenses/by/4.0

1. Introduction

Cyber threats create high levels of economic and safety uncertainty across African countries. Consulting house Serianu noted, in its *Africa Cyber Security Report 2017,* that the top cybersecurity threats on the continent in 2017 were: fake news; insider threats; ransomware; cyber bullying; the cybersecurity skills gap; theft of funds from mobile and internet banking customers; weak security infrastructure; phishing, cyber pyramid frauds; and hacking of government systems (Serianu, 2017a). The estimated cost of cybercrime to African businesses in 2017 was USD3.5 billion (Serianu, 2017a, p. 58). In five countries (Ghana, Kenya, Nigeria, Tanzania and Uganda), Serianu found that the most costly type of cybsersecurity breach (costing an estimated USD352 million across the five countries in 2017) was insider threats (Serianu, 2017a, p. 59). Individual Serianu country reports are available for Kenya, Nigeria, Tanzania and Uganda (see Serianu 2017b; 2017c; 2017d; 2017e). Serianu concluded that "over 90% of African businesses are operating below the 'cyber security poverty line'", i.e., below the minimum level of security required (Serianu, 2017a, p. 9).

Cyber threats have generated significant shifts in policy that are changing political and economic debates (Mbanaso & Dandaura, 2015), noting, for example, Nigeria's Cybercrime Act of 2015 and South Africa's Cybercrimes Bill of 2018.

Organisational cybersecurity frameworks tend to prescribe generic guidelines for *how* to secure an organisation's critical information infrastructure (CII), without providing ways of measuring precisely *what* the strengths and weaknesses are, as the basis for specific improvements. There is currently no tool to measure the current maturity level of an organisation's cybersecurity resilience. Thus, the research problem

informing our work is the absence of available tools for precise measurement of organisational cybersecurity resilience maturity.

Effective cybersecurity risk management requires attention to organisational-level resilience, in order to build country-level resilience. The cybersecurity resilience maturity measurement (CRMM) framework we propose in this article is conceived as a maturity framework tool to help organisations ascertain their cybersecurity status by matching their current cybersecurity practices against baseline security controls and best practices. The implementation version of the CRMM framework, to be developed based on the conceptualisation outlined in this article, would address the full cybersecurity ecosystem within an organisation. The framework would enable organisations to identify where their practices are weak, or not adequately implemented, and would provide for security controls to be proportionately entrenched throughout the cyber risk management process.

A CRMM approach can, we contend, provide a unique way to measure organisation-wide progress made in embedding cybersecurity controls in day-to-day and strategic operations. It can measure a range of activities—including risks associated with leadership and governance, human resources management, procurement management, operations and technology management, processes and people—in a fashion that, when quantified, can indicate the cybersecurity maturity level of an organisation.

The core outcomes of the CRMM framework that we conceptualise in the article are the cybersecurity resilience quadrants (CRQs), which indicate an organisation's cybersecurity maturity level. These indicator quadrants, when analysed with reference to the relevant quantitative data, can reveal which controls and processes are under-achieving, or need to be fine-tuned, in order to achieve the expected maturity level. In this fashion, the CRMM framework can guide improvement across an organisation in a more consistent, coherent and measurable manner than is presently the case in most organisations' cyber risk treatments.

2. Research questions

In researching the necessary components for the CRMM conceptual framework, we were guided by several key questions, applicable in any organisation, which the framework would have to provide answers to. The overarching question was: What should be the structure, and key components, of a cybersecurity resilience maturity measurement framework?

We were guided, in our development of the CRMM structure and components, by our determination that the CRMM would, through its implementation by an organisation, need to answer the following questions for the organisation:

- What is the organisation's current stage in terms of cybersecurity resilience maturity?
- What is the organisation's desired next stage of maturity?
- What are the factors, causes or defects responsible for the current stage where the organisation is positioned?

- How does the organisation need to improve in order to achieve the next stage of maturity?
- In particular, what are the necessary security controls required for improvement?
- How can the organisation create momentum to ensure that its cybersecurity is consistently and constantly improved?

Guided by these questions, we sought to conceptualise quantifiable ways to measure, as accurately as possible, the variable factors that affect cybersecurity resilience. The conceptualised framework needed to accurately and consistently quantify the state of affairs with respect to an organisation's cybersecurity status at any given point in time, i.e., the degree to which the organisation's current practices and controls in place are appropriate to achieving improved cybersecurity resilience maturity.

The next section of this article provides background and underlying concepts, followed by a section on the phases of design, and refinement, of the CRMM. We then provide a detailed explanation of the CRMM framework, as conceptualised to date based on our research. After that, we provide a draft mathematical model developed for the framework, followed by conclusions.

This article provides the initial conceptual design for a CRMM framework. The detailed content of the framework, and its testing and refinement via data collection, will be presented in subsequent publications.

3. Background: The need for a cybersecurity resilience maturity measurement (CRMM) framework

Cyber attacks have become ubiquitous throughout society, drawing attention to the need to manage cyber risks (Hartwig & Wilkinson, 2014; HPE, 2016; Serianu, 2017a). Globally, advanced technologies have enabled malicious entities to commit cybercrime more easily than anticipated, while crippling cyber attacks are putting many organisations in disarray. The increase in data breaches is motivated by financial, political, revenge, espionage, identity theft and other motivations, resulting in long-term financial consequences, reputation and customer loss, loss of competitive advantage, and other liabilities (Marinos, 2013).

A significant cyber attack can result in loss of valuable assets, including personal data, commercial data, customers, intellectual property, and other assets (BIS, 2012). According to a 2016 Identity Theft Resource Centre (ITRC) report, 1,093 data breaches were documented in that year across five industries in the US (ITRC, 2016). Van Heerden, Von Solms and Vorster (2018) report on expert views that personal information disclosure and data breaches are among the top future threats for African countries. Van Heerden et al. (2018) quote one of their survey respondents as saying that corporations are "not always placing enough emphasis on securely storing and managing sensitive and private information", primarily due, according

to the authors, "to the exploitation of unpatched systems and poorly secured systems holding Personal Identifiable Information (PII)" (p. 8).

Cyber risk management has emerged as a vital component of the corporate risk management portfolio, requiring effective steps to deal with and minimise risk exposure (ITU, 2017; NIST, 2017). As part of cybersecurity preparedness, an organisation's board and top management should be fully aware of cyber risk exposure and the degree of cybersecurity maturity needed to inform proportionate investment in cybersecurity. However, many organisations and institutions are not mindful of the cyber risks they face, due to lack of available scientific tools to quantify cyber risks and their severity. There is speculation about managing cyber risks, rather than deep understanding of the key drivers, variable factors, and effects that are relevant.

Cyber risks are top national priorities in many countries, as individuals, businesses, and governments increasingly face cyber attacks (Hartwig & Wilkinson, 2014). All countries need to increase their levels of cybersecurity resilience maturity, because the concentration of digital activities has incentivised cyber criminals to grow increasingly innovative, enabling them to persistently breach cybersecurity. Classes of cyber criminals have emerged with diversified interests and motivations, further complicating the threat landscape (Mbanaso, 2016). The effect of a single cyber attack, when it succeeds, may have debilitating effects of national magnitude, making it evident that cyber risk needs to be addressed at national levels. Cyber risk has prompted countries to devise a variety of approaches aimed at balancing the need to sustain the gains of the digital revolution with the need to combat the menace of cyber criminals (Powers, Fancher, & Silber, 2016), including: national cybersecurity strategies and policies, cybersecurity frameworks, cybersecurity agencies, and defence mechanisms. Increasing attention is being given to cybersecurity measurement frameworks and surveys, as a means to assess and advance maturity at country levels (see, for example, DTCC, 2014; ITU, 2015; 2017). However, because these approaches operate at national levels, they do not offer comprehensive solutions for application at the institutional level.

For example, Peter (2017) applies a Cyber Resilience Preparedness Index (CRPI) to 12 African economies,[1] where Egypt, Kenya, Nigeria, Tunisia, Morocco and South Africa show reasonable levels of preparedness with respect to their critical systems, industries, and classified documents. The five areas scrutinised in this 2017 Index are: (1) legislation, regulations, policies and articulation of a national cybersecurity strategy; (2) collaborations, cooperation and partnerships; (3) technical measures; (4) information-sharing mechanisms; and (5) capacity-building. This Peter (2017) CRPI framework operates at country level, drawing on three frameworks: the

1 South Africa, Tunisia, Egypt, Kenya, Ghana, Morocco, Nigeria, Zimbabwe, Algeria, Libya, Angola, Sudan, listed here in order of Networked Readiness Index ranking.

DTCC (2014) cyber risk white paper; the ITU (2015) Global Cybersecurity Index and Cyber Wellness Profiles; and the Potomac Institute's Cyber Readiness Index (Hathaway, Demchak, Kerben, McArdle & Spidalieri, 2015). The Peter (2017) CRPI framework, like the three frameworks it draws on, "only measures the existence of each indicator in a country. Thus, the ranking is based on the existence, not the quality, extent or effectiveness, of the indicators for protecting each nation's cyber investments and critical infrastructure" (Peter, 2017, p. 50). These broad frameworks offer some limited perspective at country level, but do not assist organisations to adequately defend themselves against cybercrime.

In institutions of any kind, whether large corporate institutions, or small and medium-sized enterprises (SMEs), or governments, greater attention is needed to institutional-level cyber risk management. Yet too many of the current institutional-level cybersecurity frameworks (e.g., COBIT 5, NIST CSF) offer only broad guidelines for organisations to apply, rather than detailed, quantitative frameworks. Hence insufficient attention to cyber risk management is often present in organisational cybersecurity approaches.

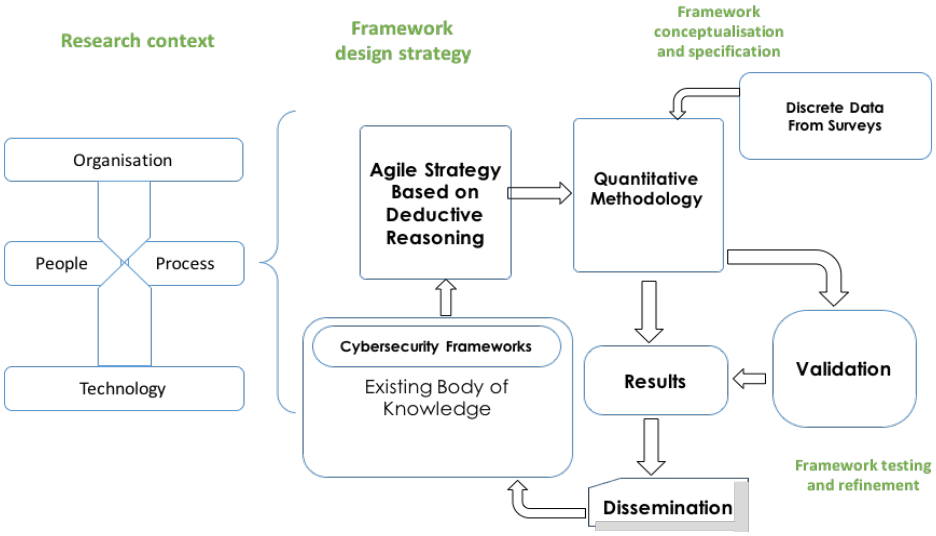
4. Research phases: Design and refinement of a CRMM framework

Cybersecurity can arguably no longer be viewed solely through the lenses of disciplines such as information systems or computer science, but should rather be understood as a multi-disciplinary domain spanning disciplines in both the sciences and humanities. At the same time, it is important, in both conceptual work and empirical work on cybersecurity matters, to adopt agile research strategies designed to enable researchers to continuously improve their frameworks (Dark, Bishop, Linger, & Goldrich, 2015).

We decided upon a quantitative approach for the conceptual framework we researched, on the grounds that a quantitative framework could generate replicable measurements able to establish the relationships between organisations' current cybersecurity practices and their targeted resilience maturity levels. Equally, it was clear to us that resilience should possess the characteristics of measurability, i.e., the resilience framework would need to be able to quantify the variable factors in numerical, logically computational form. This is in line with the dictates of quantitative empirical explorations, whose outputs must be computable, independent, numerical data that can be statistically analysed (Hassani et al., 2011; Salhin et al., 2016). Accordingly, the conceptual CRMM framework we set out in this article seeks to combine strengths found in various existing cybersecurity frameworks into a quantitative framework that can guide the design of instruments to allow logical computation of various effects or variables.

Figure 1 provides an illustration of the phases we decided would need to be followed in the design and refinement of a CRMM framework.

Figure 1: Design and refinement of a CRMM framework



The discussion below provides detail on the steps taken to date, in terms of the phases outlined in Figure 1, for reference by any researchers wishing to follow similar phases in their own work on conceptualisation of quantitative measurement frameworks for application in organisational contexts. We cover only the first three phases—*research context*, *framework design strategy*, and *framework conceptualisation and specification*—as those are the phases we have completed and which produced the content for this article.

Phase 1: Research context

Contextually, the cybersecurity ecosystem should be observed through the variable factors that contribute to cybersecurity effects or risk. From a design perspective, the causal factors that affect cybersecurity can be viewed within the context of *organisation/enterprise*, *people, process*, and *technology* (ISF, 2016). These environments form the basis for comprehensive definition of causal factors and quantitative effects, as explained below:

- Organisation/enterprise: Corporate governance is key to effectiveness of operational cybersecurity aimed at minimising organisations' cyber risk exposure. In the organisational context, the executive management must set the policy direction and governance structure that provide assurance that cybersecurity actions are consistently and correctly executed.

- People: The people element seems often to be the weakest link, due to the inherent human fallibility (McAndrew, 2018; Sundström & Holmberg, 2008). Everyone with access to cyber infrastructure needs to be aware of their cybersecurity responsibilities, to have their effectiveness evaluated continually, and to be consistently managed.
- Process: Corporate processes, applications and data that support the operations and decision-making of cybersecurity must be assessed to assure effectiveness and consistency.
- Technology: This is concerned with assessment of physical and technical infrastructure, i.e., the network, hardware and software components required to support cybersecurity measures.

Phase 2: Framework design strategy

Events shaping cybersecurity risks are unpredictable and require continuous monitoring. Thus, we concluded that the philosophy and characteristics of agile strategy would need to be incorporated into the design of the CRMM framework. Various researchers (see Dark et al., 2015) have incorporated ideas and themes from agile strategy set out in the *Agile Strategy Manifesto* (Agile Helpline, 2011) into their work on the agile research process. Among the key characteristics of agile strategy is emphasis on an iterative or adaptive approach. We determined that the CRMM framework we conceptualised would need to be grounded in agile research strategy, i.e., it would need to be able to continually respond to the unpredictability of cybersecurity events and effects. Incorporating an agile approach into the framework would, we concluded, require inclusion of data analysis techniques that use deductive reasoning, in order to encourage agility based on reliable and objective data. Also required for the framework would be specification of regular, possibly annual or bi-annual, organisational application of the framework, in order to enhance agility.

Our framework design strategy also called for incorporation of relevant components from the existing body of knowledge with respect to cybersecurity frameworks and standards. As discussed in more detail in this article's section 5 below, it was decided that COBIT 5, CIS security controls, SoGP for IS, the ISO/IEC 27005, and NIST CSF should be examined, and selected components built into the design of the CRMM framework. For example, we built on the COBIT 5 achievement rating.

Phase 3: Framework conceptualisation and specification

Determining cybersecurity resilience maturity level requires measurement of events, and/or measurement of levels of occurrence of variable factors and effects. We determined that utilising relevant components from the five frameworks cited above and discussed in more detail below (hereafter referred to as the "combined core") would provide an appropriate foundation for a CRMM framework, noting that any identified gaps could be filled progressively as the framework is implemented and tested in actual organisations. Subsequent publications will report on the trial

implementation of the framework in selected institutional settings, with the objective of testing the framework, and adapting it, if necessary, based on lessons learned.

We also concluded that cybersecurity resilience determinations would require that the framework, when applied, could generate discrete data with finite number values. This made the quantitative paradigm the necessary approach, since this would allow for numeric quantification of the resilience maturity values, and would allow for CRMM scores to be generated, disseminated, and compared, in a widely understandable fashion.

We also determined that the framework's data components would need to be selected from the five frameworks in such a way that they addressed the stated research problem as best as possible, and in a manner that could be validated. This meant that each data component chosen would have to be both relevant and quantifiable.

As a first step, COBIT 5, CIS security controls, SoGP for IS, and ISO/IEC 27005 would need to be examined and selected components mapped to the five functional pillars of the NIST CSF, thereby adapting the existing CSF, which is a guiding framework, to make it part of a quantifiable framework. As a second step, components of the combined core of the adapted NIST CSF would need to be examined to decide which should be selected and which should be deselected, based on clear reasons. As a third step, the full set of selected components would need to be used to craft a cybersecurity resilience maturity survey instrument. The survey instrument would need to use defined metrics for the combined core—an example of which is set out in Figure 3 below using the "protect" functional pillar of the NIST CSF.

We determined that the process of gathering relevant quantitative data in an established systematic way, for each of the components of the combined core, will be critical to the quality of the survey data, including the integrity, accuracy and reliability of the data. The result produced via a framework grounded in quantitative data needs to be quantifiable, objective, and consisting of numerical datasets that can be computationally and statistically analysed. Accordingly, our conceptualisation of the CRMM framework had to include provision for a computational mechanism based on computational mathematics, data structures, and algorithms. When developed as a software artefact, this computational mechanism would have to have the capability to process the data inputs and present the cybersecurity resilience quadrant (CRQ) indicator as an output. A brief outline of the key elements conceptualised for the mathematical model to be applied to the survey data is presented in this article's section 7.

(The full set of specific data collection components required for this third phase (framework conceptualisation and specification), and a discussion of the fourth phase (framework testing and refinement, as shown in Figure 1) will be published separately from this initial conceptual article.)

5. More detail on phase 3: Framework conceptualisation and specification

A range of frameworks and standards deal with cybersecurity from similar but distinct philosophical stances, each providing guidelines, principles, procedures, standards and best practices for effectively managing cybersecurity risks in organisations. These frameworks provide sequences of activities that can contextually manage cyber risk in a systematic fashion. Among these frameworks are the main foundation for our framework, the NIST cybersecurity framework (NIST CSF) (NIST, 2014), and four other influential frameworks in the field, namely, in chronological order of publication: version 5 of the control objectives for information and related technology (COBIT 5) (ISACA, 2012); the Centre for Internet Security (CIS) security controls (CIS, 2016); the standard of good practice for information security (SoGP for IS) (ISF, 2018); and the ISO information security risk management (ISO/IEC 27005) standard (ISO/IEC, n.d.). All five of these frameworks are applicable at organisational level.

Building on these five frameworks, the framework we devised focuses on the measurement of cybersecurity effectiveness at institutional level; in other words, creating a framework to measure actual resilience, rather than simply providing guidance. The sub-sections that follow introduce the five frameworks we drew on.

Control objectives for information and related technology (COBIT 5)

The control objectives for information and related technology (COBIT) framework has been developed by the Information Systems Audit and Control Association (ISACA), and the latest version, COBIT 5, is formulated using five principles and seven enablers. The principles are: meeting stakeholders' needs; covering the enterprise end-to-end; applying a single integrated framework; enabling a holistic approach; and separating governance from management. The enablers are: processes; organisational structures; culture, ethics and behaviour; principles, policies and frameworks; information; services, infrastructure and applications; and people, skills and competencies (ISACA, 2012). COBIT 5 is a comprehensive framework for the treatment of information technology governance and management, and includes but is not specific to cybersecurity matters. We determined that COBIT 5's principles and enablers can be accommodated within a framework grounded in NIST CSF.

Centre for Internet Security (CIS) security controls

The Centre for Internet Security provides a set of 20 security controls that establish a critical set of actions specific to handling aspects of cybersecurity threats in a wide range of sectors. These controls represent a collection of best practices, including six basic controls (including inventory and control of hardware assets; inventory and control of software assets; and continuous vulnerability management); 10 foundational controls (including email and web browser protections; malware defences; and data recovery capabilities) and four organisational controls (including security awareness and training; application software security; and penetration tests and red team exercises) (CIS, 2018). The CIS controls are specific to cybersecurity and contributed to our establishment of the building blocks for cybersecurity resilience.

Standard of good practice for information security (SoGP for IS)

The Information Security Forum (ISF) has formulated a standard of good practice for information security (SoGP for IS) to support organisations in addressing information security concerns based on six elements: technology, process, people, compliance, risk, and governance (ISF, 2018). The SoGP for IS also provides principles with respect to security governance, security requirements, control frameworks, and security monitoring and improvements. Furthermore, it addresses emerging concerns such as: threat intelligence; cyber attack protection and industrial control systems; enhancement of risk assessment approaches; security architecture; and enterprise mobility management. The SoGP for IS adds complementary dimensions to COBIT 5 and the CIS security controls.

ISO information security risk management standard (ISO /IEC 27005)

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) provide a suite of information security standards, known as ISO/IEC 27005, which offer guidelines on information security risk management (ISO/IEC, n.d.). In particular, ISO/IEC 27005 is a risk-based approach to the treatment of cybersecurity: first, by establishing the cybersecurity context including the scope and the methods (either qualitative or quantitative); and second, by taking cognizance of the organisation's defined risk tolerance or appetite. It considers assets, threats, existing controls, and vulnerabilities as the basis for determining the probability of incident occurrences and anticipated level of risk. This standard is explicit with respect to risk management.

The NIST cybersecurity framework (NIST CSF)

The NIST cybersecurity framework (NIST CSF) provides three main components: (1) *framework core*, (2) *implementation tiers*, and (3) *framework profile* (NIST, 2018). The framework core primarily consists of a set of five cybersecurity functional categories (with subcategories) as essential activities for effective cybersecurity risk management. The five functions—*identify*, *protect*, *detect*, *respond*, and *recover*—define characteristics of security controls and activities that are implementable (NIST, 2018). The implementation tiers enable organisations to foster understanding of the cybersecurity treatment approach and the context upon which control measures can apply (Barrett et al., 2017). The framework profile provides the guidance for implementing the framework, and for tracking the organisation's requirements for improving its cybersecurity resilience posture.

The NIST CSF provides four implementation tiers—(1) *partial*, (2) *risk-informed*, (3) *risk-informed and repeatable*, and (4) *adaptive*—as the basis for choosing a target maturity profile, and for evaluation of progress (Almuhammadi & Alsaleh, 2017). According to NIST, the four tiers do not represent maturity, but rather the basis to support how organisations can view their maturity level. In other words, the tiers are meant to help inform top management's view of cybersecurity and its determination of the phases of action necessary to achieve a particular maturity target. NIST's

notions of *current profile* and *target profile* are meant to address identified gaps consistently, but do not provide scientific or empirical ways to quantify cybersecurity resilience maturity.

In the African context, the NIST CSF is broadly followed by consultancy Serianu in construction of its Africa Cyber Security Framework, which includes four domains (Serianu, 2017a, p. 78). Domain 1 is *cybersecurity risk management (anticipate risks)*; domain 2 is *cybersecurity vulnerability management (detect vulnerabilities)*; domain 3 is *cybersecurity incident management (respond to incidents)*; and domain 4 is *cybersecurity visibility management (contain)* (Serianu, 2017a, p. 78). Serianu has also set out an Africa Cyber Security Maturity Framework, with five levels of cyber maturity: level 1 (*ignorant)*, level 2 (*informed*), level 3 (*engaged*), level 4 (*intelligent*), and level 5 (*excellent*) (Serianu, 2017a, p. 9).

Analysis

In as much as these frameworks and standards provide ways to treat cybersecurity risks, they do not provide means to *measure* actual cybersecurity resilience. Nonetheless, we found that many of the elements of these five frameworks and standards could be used as building blocks for the CRMM framework we propose.

6. Conceptualisation of a CRMM framework

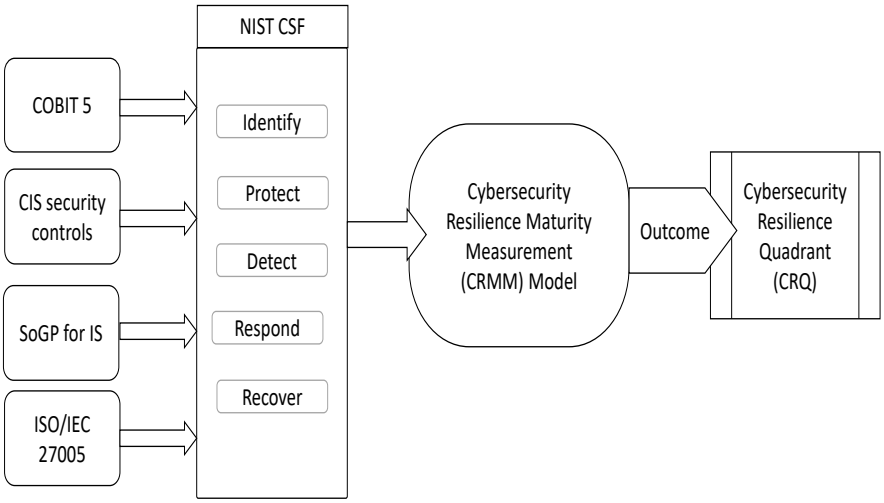
As explained above, our objective in conceptualising—and, at a later stage, piloting and refining—a CRMM framework is to enable quantitative measurement of cybersecurity resilience maturity, i.e., ascertaining the resilience posture of an organisation. This we consider necessary in order to ensure that an organisation's underperforming controls can easily be identified, prioritised, consistently managed, and improved upon. Due to cyberspace's continuously shifting threat environment, effective organisational operation in cyberspace requires a way of formally evaluating and measuring the cybersecurity resilience maturity level of an organisation, based on a comprehensive and actionable set of quantifiable effects and metrics. Such cybersecurity metrics can then be the basis for balanced understanding of cybersecurity resilience at the necessary level of granularity. Understanding cybersecurity resilience maturity requires analysis of actual organisational practice; hence the need for a suitable framework to quantify current practice against established baseline security controls and global best practices.

Accordingly, we have conceptualised our CRMM framework as a predictive tool that can provide quantification of various cybersecurity operational activities, can highlight areas that are under-performing, and can indicate the actions necessary to effect changes necessary to improve cybersecurity functions.

The CRMM framework we have conceptualised adapts the aforementioned NIST CSF five functional pillars—identify, protect, detect, respond, recover—and their respective subcategories, by mapping and integrating selected framework elements from COBIT 5, CIS controls, SoGP for IS, and ISO/IEC 27005 into the NIST

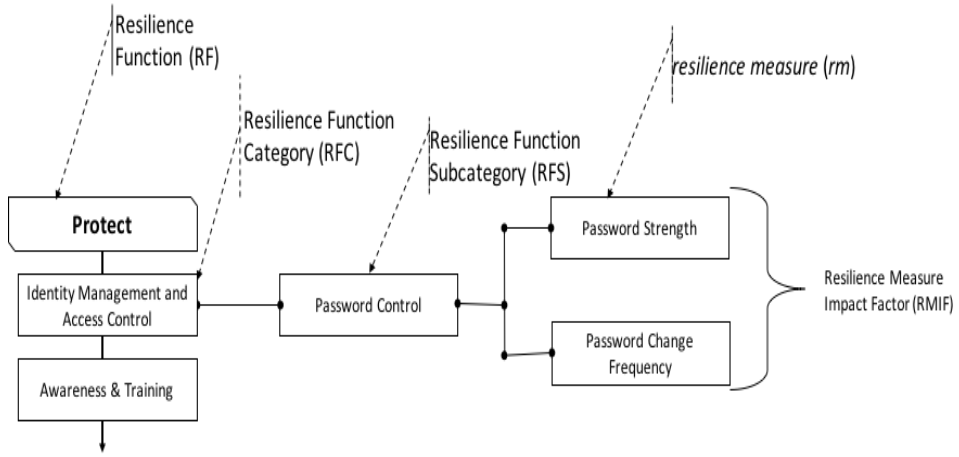
CSF. The result is the aforementioned *combined core* for the CRMM framework, which is aimed at ensuring that the framework is robust. The combined core, and the elements flowing from it, are illustrated below in Figure 2.

Figure 2: Combined core, and elements flowing from it, in proposed CRMM framework



Flowing from the conceptual design in Figure 2 above, Figure 3 below presents a magnified view of the structural organisation of one of the components of the framework and its categories and subcategories, using the "protect" functional pillar as the specific framework component. (This initial representation will be further refined, and applied with respect to all five NIST CSF functional pillars, at the next stage of our research endeavour.)

Figure 3: Example of draft CRMM functional pillar: "Protect"



As depicted in Figure 3 for a single function ("protect"), a computational mathematical model design will be applied to each of the five functional pillars, with each of the five adapted NIST CSF functional pillars denoted as resilience functions (RFs), and with each RF underpinned by a resilience function category (RFC) and a resilience function subcategory (RFS). Additionally, for each RFS, a resilience measure (*rm*), and a resilience measure impact factor (RMIF), will be assigned.

7. Mathematical model for CRMM framework

The following are the elements we have initially developed for a mathematical model corresponding to the CRMM conceptual framework outlined above:

- Definition 1: Cybersecurity resilience function index (CRFI) is the sum total quantification of the resilience functions (or the sum of RFs) (explained in more detail below);
- Definition 2: Resilience function factor (RFF) defines the summation of resilience function categories (or RFCs) under a particular function;
- Definition 3: Resilience category factor (RCF) defines the summation of resilience function subcategory activities (or sum of RFSs) under a subcategory;
- Definition 4: Resilience function subcategory (RFS) factor is the sum total quantification of resilience measure impact factors (RMIFs);
- Definition 5: Resilience measure impact factor (RMIF) is the summation of resilience measures (*rm*s) for a specific subcategory; and
- Definition 6: Resilience measure (*rm*) is the unit quantification that measures a precise control (or depicting current practice) (explained in more detail below).

In the sections that follow, we provide the conceptual assumptions that underpin the construction of the mathematical model.

Cybersecurity resilience function index (CRFI)

The CRFI is the weighted summation of the quantification of the five functional pillars controls—identify, protect, detect, respond, recover—based on the contributing elements of the RFs. The weighted elements are grounded in the assumptions of what we determined to be percentage weights of the risk-contributing function factors (RCFFs) of the core functions, as shown in Table 1.

Table 1: Weightings of risk-contributing function factors (RCFFs)

	Function	Abbrev-iation	Description	Weight (%)	w_f
1	Identify	*idf*	identify factor effect	20%	0.20
2	Protect	*prf*	protect factor effect	25%	0.25
3	Detect	*def*	detect factor effect	20%	0.20
4	Respond	*ref*	respond factor effect	20%	0.20
5	Recover	*rcf*	recover factor effect	15%	0.15
	Total		total factor effect	100%	1

The rationale for the weights assigned to the risk-contributing function factors (RCFFs) in Table 1 is that function pillars will have varying effects on cybersecurity resilience. We argue that among the five functions (based on an average weighting of 20% for each), *protect* controls should be the highest priority, and thus should have a higher weighting, of 25%, because it serves as the most critical resilience factor effect. We based this weighting on the view that an organisation must put greatest emphasis on prevention. We determined that *recover* controls should be lower priority, with a marginally lower weighting of 15%, making it the least critical effect factor, as it is a result of actions taken in terms of the other four functional pillars.

Resilience measure (rm)

Based on our scrutiny of the existing frameworks outlined above, we decided that one of the foundational units of measure for all higher-level metrics in the design of the CRMM mathematical model should be the resilience measure (*rm*). This *rm* is the controlling effect that measures the actual cybersecurity practice against the baseline security controls and best practices. For this measure, we adapted the COBIT 5 *achievement* rating, to produce the *rm* formulated as a quantifiable weight, as depicted in Table 2. The COBIT 5 achievement rating is a standard derived from a rating scale defined in ISO/IEC 15504, which is mostly used in process assessment modelling. It is used here because the CRMM framework is an assessment model, and the COBIT 5 achievement rating is a known and accepted standard in process modelling.

Table 2: Weightings of resilience measure (*rm*)

	***rm* level**	**Weight**	**Note**
1	not achieved	0	no controls in place, or very poor controls
2	loosely achieved	1	few controls in place, or incoherent controls
3	partially achieved	2	some controls in place, but not consistently and structurally organised; many, and/or important, elements missing
4	largely achieved	4	controls structurally implemented, but not consistent; only a few, and/or only minor, elements missing
5	fully achieved	6	baseline security; the best practice value

The resilience measure (*rm*) is the smallest unit of analysis for which data can be collected and can be specific to any particular types of resilience being measured in our framework—for example, password strength, as discussed below in relation to Figure 4 on "password regime". We built our conceptual design of *rm* through application of the SMART (*specific*, *measurable*, *actionable*, *relevant*, *timely*) construct derived from the field of strategic management. SMART is largely used in improvement and performance schemes in order to make goals achievable (Cheng et al., 2014; MindTools, 2018). We used SMART to clarify and conceptually position *rm* in a way that is focused, strategic and significant, and in a manner that increases chances of achieving certain defined objectives, as follows:

- Specific: The *rm* control is focused on a specific unit of effect measurement, and not a by-product or result of another component.
- Measurable: The *rm* control has quantifiable effect, i.e., it is accurate and complete by itself.
- Actionable. The *rm* control can be improved upon, i.e., it is easy to understand the particular corrective action required.
- Relevant: The *rm* control has measurable resilience effect, and is important to achieve the overall cybersecurity goal.
- Timely: The *rm* control is easily accessible when required.

To show how *rm* weight could be calculated in terms of the framework, Figure 4 provides a sample proposed instrument, which could be entitled "password regime".

Figure 4: Draft sample *rm* instrument: Password regime

A. Your password contains a combination of
   i. Alpha-numeric and special characters [A-z, a-z, 0-9, &, %, @, #] ... **[6]**
   ii. Alpha-numeric characters [A-z, a-z, 0-9] ..... **[4]**
   iii. Birthday date ..... **[2]**
   iv. Plain English words ..... **[1]**
   v. Family names ..... **[0]**

B. The length of your password is usually
   i. Between 8-12 characters long ..... **[6]**
   ii. Between 6-8 characters long ..... **[4]**
   iii. 6 characters long ..... **[2]**
   iv. 4 characters ..... **[1]**
   v. Less than 4 characters ..... **[0]**

The draft instrument provided in Figure 4 would aim to test users' compliance level, and knowledge, quantitatively. In respect of statement A, a user who uses *alpha-numeric and special (or weird) characters* would have more resilience against password attacks than a user who uses *family names*. In respect of statement B, a user who has a password length of *8–12 characters* would have a higher resilience measure than a user with a password length of *4 characters*.

Drawing on the assignment of numeric values in Figure 4 and Table 2, enforcement and practice for the strongest password regime (i.e., A=6, B=6) would be quantified as *rm* level 5 (fully achieved). Thus, theoretically, it can be argued that the construction of weighted scales for the quantification of granular controls can provide adequate validity in terms of summation of baseline security controls and best practices for cybersecurity resilience.

An important note to add in this context is that a user may be aware of password best practice but still fail to comply. Users' resistance to change, or human weakness, can be a major factor in cybersecurity, and identification and quantification of such weaknesses can show an organisation more precisely what the strengths and weaknesses are, as the foundation for deciding how to address these.

Based on the foregoing, CRMM could be expressed mathematically to enable the development of a suitable data structure, algorithms, and computational logic for the various *rm* effects which, when summated, would produce a result that indicates an organisational cybersecurity resilience function index (CRFI) as a cybersecurity resilience quadrant (CRQ) indicator. The mathematical formulation would be as follows:

To sum the contributing effect of *rm* for one sub-category, it can be expressed as follows:

$$RMIF = \sum_{i=1}^{n} rm_i \quad \ldots\ldots\ldots\

Now, the cybersecurity resilience function index (CRFI) is the next level equation needed to calculate the contributing effect of all resilience functions. Noting that each function has a specific contributing weight factor (see Table 1), the cybersecurity resilience function index (CRFI) can be expressed generically as follows:

$$CRFI = \sum_{i=1}^{N} (RFF)_i \times w_i \ldots\ldots\ldots\

The underlying logic is the quantification and aggregation of the effect of five functions—identify, protect, detect, respond, and recover functions—and their subcategories. In the subcategories, the resilience measure (*rm*), which is the smallest unit quantified, helps to measure the unique effects of each particular resilience indicator. The summation of the effects in a cluster of functions, including their subcategories, is then aggregated in the computation of the CRFI, leading to the generation of the CRQs. The numerical ranges assigned to each of the four possible CRQs (i.e., the four possible maturity quadrants) ensure that the cumulative resulting effect lies between 0 and 1, therefore generating four usable quadrants.

8. The cybersecurity resilience quadrants (CRQs)

The conceptual design of the cybersecurity resilience quadrants (CRQs) aims to provide a single view of an organisation's maturity level, i.e., its degree of cybersecurity resilience. The resulting $CRFI_o$ value is a pre-defined functional performance indicator that indicates in which of the four quadrants the organisation lies with respect to cybersecurity resilience maturity.

Thus, within our proposed CRMM framework, the CRQs represents the intersections of risk and resilience, as illustrated in Figure 5 on the next page. In order to formulate the CRQs, we adapted the capability maturity model integration (CMMI) developed by the Software Engineering Institute, Carnegie Mellon University (CMMI Institute, n.d.; Nath, 2018). The CMMI, which is globally recognised as a process improvement framework, has five levels (*initial, managed, defined, quantitatively managed, optimising)*. We adapted four of the five CMMI levels to conceptualise the CRQs for our CRMM framework.

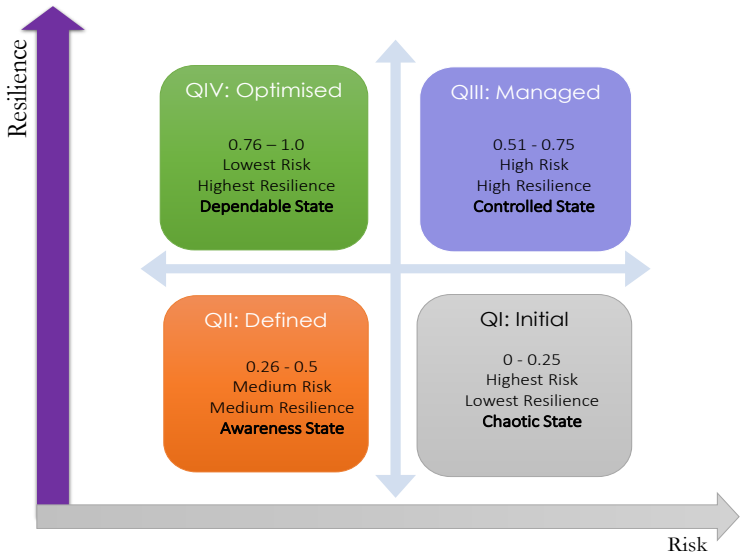
The explanations for each of the four CRQs are as follows:

- Initial: This CRQ describes a maturity level characterised by a high-risk environment with few, or ad hoc and chaotic, security controls. The organisation typically is not a stable environment, i.e., there is an absence of top management leadership and an absence of prioritisation of cyber risk as part of corporate risk management. This quadrant indicates highest risk and lowest resilience.
- Defined: This CRQ describes a maturity status that is characterised by a medium-risk environment with basic security controls in place. There is recognition of cyber risk, and the organisation is making efforts to ensure that security controls are standardised by policy, standards, procedures and governance functions. This quadrant indicates medium risk and medium resilience.
- Managed: This CRQ describes a maturity status that is well categorised and understood, and is described in standards, procedures, tools, and corporate governance practices. A critical distinction between *defined* and *managed* is the wider scope, in this quadrant, of the cybersecurity standards, policies and procedures across the organisation. Security controls are consistently planned, managed, performed, measured, and controlled. Relevant stakeholders are

aware of the cybersecurity responsibility imposed on them by virtue of their corporate responsibility. This quadrant indicates high risk but also high resilience. Risk is potentially high, but because the risk is understood and prioritised, it is managed vigorously and consistently.

- Optimised: This CRQ describes a maturity status that is effectively agile and continually improved, based on a quantitative understanding of the common cyber risk factors. There is full commitment of top management, and full understanding of organisational risk exposure. The significance of effective cybersecurity governance, and of stakeholders' roles and responsibilities, are well understood, resulting in a cycle of persistent improvement and continual revision in order to respond to changing business objectives and the changing threat environment**.** This quadrant indicates the lowest risk and highest resilience.

Figure 5: Cybersecurity resilience quadrants (CRQs)



9. Conclusion and future work

The CRMM framework we have outlined in this article conceptualises mechanisms to address cybersecurity risk management gaps. It incorporates a mathematical model designed to quantify the cybersecurity effects and variables which, if correctly addressed, can lead to improved performance of an organisation's cybersecurity. The CRMM and its CRQs provide a framework for developing, improving, and sustaining cybersecurity resilience by determining the extent to which the organisation's current actions on cybersecurity governance are working, the extent to which the organisation is improving, and the extent to which the organisation needs greater continuous improvement. Our CRMM framework offers a rigorous yardstick, a

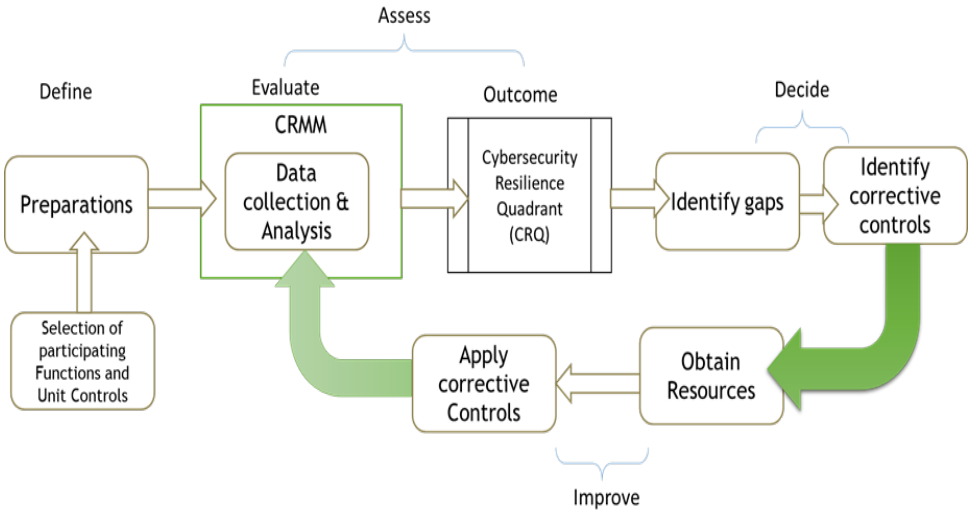
performance-rating technique, which allows comparison between an organisation's current cybersecurity performance against known best practice, and between current performance and the organisation's previous, or desired future, performance.

While there are robust cybersecurity frameworks that prescribe the essential toolkits to manage cybersecurity risk, determining the current state of cybersecurity resilience remains an imprecise practice. This gap makes it difficult for an organisation to ascertain its current status, and to identify a visible path for improvement. As an organisation advances its cybersecurity preparedness, it is expected to establish a maturity level whereby it detects areas needing enhancement, and knows how to correct negative effects by drilling down to under-performing areas. The CRMM and the CRQs are conceptualised with the aim of providing a clear single view of an organisation's cybersecurity resilience maturity, in a way that can direct the organisation to consistently and continuously better its performance. To earn an optimised CRQ rating in our framework, i.e., to achieve an optimised level of cybersecurity resilience maturity, an organisation will have to exhibit a deep understanding of, and commitment to, improving cybersecurity resilience based on statistical and quantitative methods. Conversely, an organisation found to be in one of the other three quadrants will receive an indication of the elements that the organisation requires, by way of continuous improvement, in order to advance to a higher level of cybersecurity resilience maturity, i.e., to a better CRQ.

The CRMM approach can create value for an organisation by establishing the specific gaps and priorities in its cybersecurity. Applying the CRMM framework will provide a status report on which of the four quadrants the organisation falls into, which controls are underperforming, which quadrant the organisation should move to next, and how it can move to that next quadrant, all the while building greater organisational precision in measuring resilience levels.

The conceptual design we have presented in this article is a first step towards greater precision in measuring cybersecurity resilience maturity. The next step in this research will be to move from the conceptual framework to actual testing and refinement, via pilot implementation. Pilot implementation will initially require four steps, as set out in Figure 6: (1) *define* (first, by selecting relevant functions and unit controls); (2) *assess* (evaluate the current state of pilot organisations' resilience through pilot quantitative surveys generating CRQ outcomes); (3) *decide* (decide on corrective controls); and then (4) *improve* (pilot application – apply prioritised controls to enhance resilience).

Figure 6: CRMM framework testing and refinement



We are also developing a software application to support framework testing and refinement. Using the software, organisations will be able input their relevant data and compute their CRQ and deduce appropriate remedial actions, if applicable. Our subsequent publications will, among other things, focus on the detailed computational design, algorithms, and data structures for the CRMM software tool.

References

Agile Helpline. (2011). Agile strategy manifesto. Retrieved from http://www.agilehelpline.com/2011/04/agile-strategy-manifesto.html

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3) 51–62. https://doi.org/10.5121/csit.2017.70305

Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Witte, G., & Feldman, L. (2017). *The cybersecurity framework: Implementation guidance for federal agencies*. Draft NISTIR 8170. US Department of Communication. Retrieved from https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

Center for Internet Security (CIS). (2018). CIS controls version 7. Retrieved from https://learn.cisecurity.org/20-controls-download

Cheng, Y., Deng, J., Li, J., Deloach, S. A., Singhal, A., & Ou, X. (2014). Metrics of security. In A. Kott, C. Wang, & R. F. Erbacher (Eds.), *Cyber defense and situational awareness* (pp. 263–295). Cham: Springer. https://doi.org/10.1007/978-3-319-11391-3_13

CMMI Institute. (n.d.). Introducing CMMI V2.0. Retrieved from https://cmmiinstitute.com/capability-maturity-model-integration

Dark, M., Bishop, M., Linger, R., & Goldrich, L. (2015). Realism in teaching cybersecurity research: The agile research process. In M. Bishop M., N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education across the curriculum*. Proceedings of the 9th IFIP WG 11.8 World Conference on Security Education (WISE 9), Hamburg, May. Cham: Springer. https://doi.org/10.1007/978-3-319-18500-2_1

Department for Business, Innovation and Skills (BIS). (2012). *Cyber risk management – A board level responsibility*. London: UK Government. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/12-1119-cyber-risk-management-board-responsibility.pdf

Depository Trust and Clearing House (DTCC). (2014, October). *Cyber risk – A global systemic threat: A white paper to the industry on systemic risk*. Retrieved from http://www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

Federal Republic of Nigeria. (2015). Cybercrime Act. Retrieved from http://www.nigerianlawguru.com/legislations/STATUTES/CYBERCRIME%20ACT%202015.pdf

Hartwig, R. P., & Wilkinson, C. (2014). *Cyber risks: The growing threat*. Insurance Information Institute. Retrieved from https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

Hassani, H., et al. (2011). Research methods in computer science. *Methodological Innovations Online*, *11*(1), 1–16. https://doi.org/10.13140/RG.2.2.25912.55043

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). *Cyber readiness index 2.0: A plan for cyber readiness: A baseline and an index*. Arlington, VA: Potomac Institute for Policy Studies. Retrieved from http://www.potomacinstitute.org/images/CRIndex2.0.pdf

Hewlett Packard Enterprise (HPE). (2016). *HPE cyber risk report 2016*. Retrieved from http://techbeacon.com/sites/default/files/gated_asset/hpe-cyber-risk-report-2016.pdf

Identity Theft Resource Center (ITRC). (2016). *ITRC data breach reports: 2016 end of year report*. Retrieved from https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

International Organisation for Standardisation & International Electrotechnical Commission (ISO/IEC). (n.d.). ISO/IEC 27000 family - Information security management systems. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

Information Security Forum (ISF). (2018). *The standard of good practice for information security 2018*. Retrieved from https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

Information Systems Audit and Control Association (ISACA). (2012). COBIT 5 introduction. Retrieved from https://www.isaca.org/COBIT/Documents/An-Introduction.pdf

International Telecommunication Union (ITU). (2015). Global cybersecurity index and cyberwellness profiles. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

ITU. (2017). *Global cybersecurity index 2017*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Marinos, L. (2013). *ENISA threat landscape 2013: Overview of current and emerging cyber-threats*. European Union Agency for Network and Information Security. https://doi.org/10.2788/14231

Mbanaso, U. M. (2016). Cyber warfare: African research must address emerging reality. *The African Journal of Information and Communication (AJIC), 18,* 157–164. https://doi.org/10.23962/10539/21789

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17–24. doi: 10.9790/0661-17361724

McAndrew, T. (2018, January 28). Human phish-bait: Why people are the weakest link in our cyber defence. *Washington Times*.

MindTools. (2018). SMART. Retrieved from https://www.mindtools.com/pages/article/smart-goals.htm

Minister of Justice and Correctional Services. (2018). Cybercrimes Bill. Pretoria: Government of South Africa. Retrieved from https://www.ellipsis.co.za/wp-content/uploads/2018/03/181023Clean_Cybercrimes_Bil.pdf

Nath, S. (2018). Building capability with CMMI. *ISACA Journal*. Retrieved from https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=667

National Institute of Standards and Technology (NIST). (2014). *Framework for improving critical infrastructure cybersecurity*. https://doi.org/10.1109/JPROC.2011.2165269

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. v1.1 Draft. https://doi.org/10.1109/JPROC.2011.2165269

Powers, E. W., Fancher, J. D., & Silber, J. (2016). *Beneath the surface of a cyberattack: A deeper look at business impacts*. Deloitte. https://doi.org/10.1007/978-1-4302-1115-0_14

Salhin, A., Kyiu, A., Taheri, B., Porter, C., Valantasis-Kanellos, N., & König, C. (2016). Quantitative data gathering methods and techniques. In A. Paterson et al. (Eds.), *Research methods for accounting and finance*. https://doi.org/10.23912/978-1-910158-88-3-3226

Serianu. (2017a). *Africa cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Serianu. (2017b). *Kenya cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/KenyaCyberSecurityReport2017.pdf

Serianu. (2017c). *Nigeria cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf

Serianu. (2017d). *Tanzania cybersecurity report 2017: Demystifying Africa's cybersecurity poverty line*. Retrieved from www.serianu.com/downloads/TanzaniaCyberSecurityReport2017.pdf

Serianu. (2017e). *Uganda cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from htwww.serianu.com/downloads/UgandaCyberSecurityReport2017.pdf

Sundström, M., & Holmberg, R. (2008). The weakest link human behaviour and the corruption of information security management in organisations – An analytical framework. In International Institute of Informatics and Systemics (Ed.), *IMSCI '08: 2nd International Multi-Conference on Society, Cybernetics and Informatics*, Vol. III Proceedings (pp. 94-99). Retrieved from http://portal.research.lu.se/ws/files/5974349/1543150.pdf

Van Heerden, R., Von Solms, S., & Vorster, J. (2018). Major security incidents since 2014: An African perspective. In IEEE (Ed.), *2018 IST-Africa Week Conference (IST-Africa).* Retrieved from https://ieeexplore.ieee.org/document/8417326

A Proposed "Agricultural Data Commons" in Support of Food Security

Jeremiah Baarbé
Fellow, New and Emerging Researchers Group, Open African Innovation Research (Open AIR) network, University of Ottawa
https://orcid.org/0000-0002-5360-2975

Meghan Blom
Fellow, New and Emerging Researchers Group, Open African Innovation Research (Open AIR) network, University of Ottawa
https://orcid.org/0000-0001-8858-4546

Jeremy de Beer
Professor, Faculty of Law, University of Ottawa; Senior Research Associate, Intellectual Property Unit, University of Cape Town; and Co-Founder and Director, Open African Innovation Research (Open AIR) network
https://orcid.org/0000-0001-9753-3708

Abstract
This article identifies a data governance model that could help reduce dataset access inequities currently experienced by smallholder farmers in both developed-world and developing-world settings. Agricultural data is globally recognised for its importance in addressing food insecurity, with such data generated and used by a value chain of contributors, collectors, and users. Guided by the modified institutional analysis and development (IAD) framework, our study considered the features of agricultural data as a "knowledge commons" resource. The study also looked at existing data collection modalities practiced by John Deere, Plantwise and Abalobi, and at the open data distribution modalities available under the Creative Commons and the Open Data Commons licensing frameworks. The study found that an "agricultural data commons" model could give greater agency to the smallholder farmers who contribute data. A model open data licence could be used by data collectors, supported by a certification mark and a dedicated public interest organisation. These features could engender an agricultural data commons that would be advantageous to the three key stakeholders in agricultural data: data contributors, who need engagement, privacy, control, and benefit-sharing; small and medium-sized-enterprise (SME) data collectors, who need sophisticated legal tools and an ability to brand their participation in opening data; and data users, who need open access.

Acknowledgements
This article draws on the contents of the authors' Working Paper for the Open African Innovation Research (Open AIR) network (Baarbé, Blom, & De Beer, 2017). The authors acknowledge support for this research provided by: the Social Sciences and Humanities Research Council (SSHRC) of Canada and the International Development Research Centre (IDRC), via the Open AIR network; and the Canada First Research Excellence Fund (CFREF), via the Global Institute for Food Security (GIFS). The views expressed in this work are those of the authors and do not necessarily represent those of the research funders.

Keywords
agricultural data, open data, institutional analysis and development (IAD), knowledge commons, data commons, data collection, copyright, database rights, licensing, Creative Commons, Open Data Commons, privacy, benefit-sharing, social certification, certification marks

DOI: https://doi.org/10.23962/10539/27534

Recommended citation
Baarbé, J., Blom, M., & De Beer, J. (2019). A proposed "agricultural data commons" in support of food security. *The African Journal of Information and Communication (AJIC), 23*, 1–33. https://doi.org/10.23962/10539/27534

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: https://creativecommons.org/licenses/by/4.0

1. Introduction

Agricultural data is an increasingly vital resource in the advancement and innovation of farmer organisations, food production, agricultural-sector value chain development, and provision of agricultural services (Jellema, Meijninger, & Addison, 2015). Today's farmers can potentially rely on computational and precision agriculture to inform decisions. Datasets such as weather data, market price data, and agricultural input data fuel these tools, which range from simple graphs to emerging artificial intelligence networks (GODAN, 2015). Access to, and use of, such data can play a key role, particularly in developing countries, in addressing global food insecurity by "enabling better decision making, transparency and innovation" (Open Data Charter, 2016). At the same time, however, dataset ownership rights may prevent access to and use of data—a dimension distinct from, yet as important as, farmer access to education, skills, technology, infrastructure, and finances (De Beer, 2016).

Agricultural data is collected through a range of technologies at every point in the harvesting cycle, from modern, commercial operations to smallholder, sustenance farms (see, for example, Carbonell, 2016; Jellema et al., 2015). Sensors in "smart" tractors record GPS, soil, and harvest data. Drones and satellites record land use and productivity data. Weather stations provide meteorology data. Markets generate crop yield data. In developing countries, data collection is often more labour-intensive than in developed-world settings. Intermediary data collection agencies, such as Plantwise, are often involved in reaching smallholder farmers. Projects are developing mobile apps that allow smallholder farmers and fishers to track their own data and contribute to larger data pools. Using technological platforms and applications to capture data requires investment from a variety of stakeholders, and "effective data sharing depends on a strong network of trust between data providers and consumers" (Allemang & Teegarden, 2016, p. 11).

The importance of data for agriculture underscores a growing view that data has replaced oil as the world's most valuable resource (see, for example, *The Economist*, 2017). Accordingly, in complex global markets, unequal ownership of, and unequal access to, agricultural data can exacerbate power inequalities for vulnerable groups (see, for example, Davies, 2015; Ferris & Rahman, 2016, p. 2)—entrenching these inequalities in ways that threaten sustainable development and food security. Most legal rights to data are owned by data *collectors*: entities who invest in collection of data, arrangement of databases, safeguarding of confidential information, and related activities. The lack of enforceable data rights ownership by certain communities who are data *contributors*—e.g., smallholder farmers in both the developed and developing worlds—is an important economic and ethical issue. Current models for access to open data leave many stakeholders vulnerable to the whims of collectors. Meanwhile, expansion of ownership rights to protect individual or community data contributors has the potential to cause significant complications for the collector intermediaries that practise and promote open data. Accordingly, there needs to be a shift towards encouraging the growth of innovative, sustainable, and equitable data governance platforms that allow for all stakeholders involved to receive benefits (see Frischmann et al., 2014, p. 11), including not only the data contributors and collectors, but also the data *users*.

The article seeks to identify a governance model that could help reduce dataset access inequities currently experienced by smallholder farmers. We used Ostrom's (1990) institutional analysis and development (IAD) framework, as modified by Frischmann, Madison, and Strandburg (2014) and Frischmann, Madison, and Strandburg (2017), to examine features of agricultural data as a "knowledge commons" resource. We also looked at the data collection modalities practiced by John Deere, Plantwise, and Abalobi; at the Creative Commons and the Open Data Commons frameworks for open data licensing and distribution; and at the social certification practices of Fairtrade International (n.d.). Through this study, we arrived at a model for an

"agricultural data commons" fostered by a licence that could be used by data collectors to make their datasets open. We propose that governance of this agricultural data commons would be supported by a certification mark and a dedicated public interest organisation.

Given the status of data as a key global resource, the data commons we propose could apply beyond agriculture to many other sectors. However, agriculture is a particularly fitting locus for a data commons, given agriculture's role as the birthplace of the commons and as the site of certification programmes such as the Fair Trade movement. The field of agriculture also provides illustrations of data's important geopolitical dynamics.

2. The notion of an "agricultural data commons"

The IAD model, developed by Ostrom (1990) and modified by Frischmann et al. (2014) and Strandburg et al. (2017), provides a theoretical framework that can be deployed to interrogate and understand systems of data governance in relation to their potential "knowledge commons" attributes. Knowledge commons models are ones in which knowledge and information resources are shared to produce creative and innovative products (Frischmann et al., 2014, p. 5). The knowledge commons orientation, according to Frischmann et al. (2014, p. 11), builds on the "growing realization that legal facilitation of innovation and creative production cannot be confined to a simple set of property rules to incentivize individuals to innovate".

Instead of expanding or contracting ownership rights, the commons evokes the need for mutual responsibility towards data as a shared resource. A data commons views the actors who provide, collect, clean, interpret, and use data as stakeholders. A stakeholder approach acknowledges that actors are involved in *both* inputs and outputs. In the field of agricultural data, farmers contribute; governments, large private-sector firms, large non-profit entities, and small and medium-sized-enterprise (SME) intermediaries collect; and users develop new insights. Each input is necessary to produce useable data and derive benefit from it. Legal and institutional mechanisms are needed to enable a data commons, and commons mechanisms need to recognise the contributions of all stakeholders and distribute rights in ways that reinforce participation in the commons.

The Frischmann et al. (2014) modified IAD model for understanding the dynamics of a knowledge commons calls for interrogation of five aspects:

- background of the resource;
- characteristics of the pooled resource and the technologies and skills needed to create, obtain and maintain the resource;
- members and their roles;
- governance mechanisms, such as intellectual property (IP) rights; and
- benefits and costs of participating in the knowledge commons.

In the remainder of this section 2, we explore the characteristics of a potential agricultural data commons in terms of the five IAD elements just listed. We adapt the framework for the agricultural context in a way similar to the adaptation by Strandburg et al. (2017) for the medical context, including highlighting, as Strandburg et al. (2017) do, the "social dilemmas" to which the data commons could respond.

Background of the resource

The modern story of data begins in 1989 when Berners-Lee proposed a world wide web of data. The emergence of Web 2.0 platforms in 2007 led to a market for data as companies like Facebook built business models based on user-created content (O'Reilly, 2007) and, eventually, on use of customer data to drive advertising and targeting of user preferences. Most recently, artificial intelligence and the internet of things have emerged as disruptive technologies that rely on extremely large sets of linked data (Ashton, 2009; Jordan & Mitchell, 2015).

As the market for data grows, there are increased concerns around privacy. Burners-Lee (2017) recently warned that data-for-service models are vulnerable to a loss of trust among users, who are starting to seek control over their data. While large data-driven companies seek to insulate themselves from the effects of user mistrust by ensuring their services are indispensable, SMEs stand to suffer as data-sharing norms change.

Based on recognition of the value and importance of access to data, the open data movement formed, growing out of the open access and open science movements (De Beer, 2017b). Open data is data that can be accessed, used, or shared by anyone (Open Data Handbook, n.d.). By making data publicly available and accessible, open data can foster innovation, enable more efficient decision-making, and facilitate creative use of information. In turn, such use can generate new forms of public value by improving policymaking on pressing challenges facing the global community—such as, in the context of this study, growing food insecurity. A data commons comprising accessible and usable open data can foster transparency and collaboration among stakeholders, which can, in turn, foster new discoveries to help sustainably address the problems of feeding a growing population (Carolan et al., 2015). For example, open data can be used to identify and develop solutions to problems of pest infection or drought. The benefits of open data are well understood, with McKinsey valuing the global economic potential of open data at USD3 trillion a year (McKinsey, 2013).

Characteristics of the pooled resource

The nature of data can vary. It is shaped by cultural and institutional norms,and can take many forms, including: "big data", such as real-time or census data; and more qualitative data, including satellite images, pictures, texts, or maps. Data is generally technological in nature, created through the application of techniques to capture and represent characteristics of phenomena (De Mauro et al., 2016, pp. 123–125). The

term "data" is often used to refer to both discrete information about a phenomenon and sets of information compiled in databases. As a resource, data is characterised by the intersection of depletable phenomena and renewable knowledge (Manovich, 2012). The events being captured and the methods of capturing data are tangible and limited. When the events are located on farmers' fields, the resource inputs are rival, meaning that only those farmers can collect data. But once data is captured in a digital format it becomes an intangible resource and easily copied.

Data is created by persuading contributors, including communities of contributors—e.g., for the purposes of this study, communities of smallholder farmers—to provide access to phenomena of interest (De Beer, 2016, p. 11). Organisations playing the role of collectors then invest in the collecting, selecting, and aggregating of the data. By doing so they generally create ownership rights in the datasets they aggregate. The data contributors, meanwhile, tend not to have enforceable rights to the data sets developed by the collectors, generating inequality and marginalisation (De Beer, 2016, p. 14)—as the contributors become vulnerable to the whims of the collectors who own the data. In order for the data to yield benefits for contributor groups, there must be a configuration of the data governance structure that allows for equitable appropriation of, access to, and use of, the data.

Agricultural data includes information about weather patterns, soil attributes, crop yields, the occurrence and spread of diseases and pests, and supply-chain data (see Allemang & Teegarden, 2016, p. 6). Precision agriculture offers farmers the ability to use data gathered from their fields to make informed decisions. (Stakeholders can also compile data into pooled databases for uses that include policy creation, business intelligence, supply chain management, scientific research, and the development of new applications and technologies.)

The members of the commons: Contributors, collectors, users

As stated above, we start with three key categories of stakeholders—*contributors*, *collectors*, *users*—participating in communities of data production and use. In other words, these are some of the key members in any potential data commons. Manovich (2012), writing in the context of big data as a sociological and digital humanities research tool, describes a similar taxonomy of stakeholders in data communities, writing of "those who create data (both consciously and by leaving digital footprints), those who have the means to collect it, and those who have expertise to analyze it" (2012, p. 460).

Our model proposes three categories of stakeholders: data contributors provide access to the phenomena being captured; collectors gather data and make it available; and users use data to gain insights, develop applications, and make decisions. In the context of agricultural data, the contributors are often farmers. The collectors, who can be governments, private-sector firms, large non-profits, or SMEs (including social

enterprises), are typically the legal owners of the data and are responsible for opening access through licensing (De Beer, 2016, p. 14). Through their use of technology and application of intellectual property (IP) law, collectors hold proprietary ownership rights to the data collected, including the right to appropriate value from data. Even when collectors offer open access, their ownership rights allow them to choose to publish partial datasets, meaning contributors are not able to fully share in the benefits of the data they provide.

The three categories of stakeholders we have set out may not be exhaustive. For example, those who rely on agricultural products as inputs (e.g., seeds) or outputs (e.g., food) may also impact, or be impacted by, the governance of agricultural data. Whether such stakeholders should be considered members of the commons *per se* is debatable, but spillover effects and overall social value are regardless useful to consider.

Governance mechanisms

A number of (often overlapping) legal mechanisms contribute to the bundle of property rights in data (De Beer, 2016, p. 8). Possibly the most important of these rights for access to data are the exclusive rights under copyright, which include the rights to publish, copy, and circulate. A data commons must also account for other potential rights in data, including *sui generis* database rights, personal privacy rights, and rights to protection of confidential information. Also relevant to governance of data in a commons are technological systems and social norms.

Copyright protects the original expression of ideas. Applied to data, copyright can exist in original compilations of data, such as databases. Copyright protects the structure of databases and specific combinations of data. The World Trade Organisation (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires its member countries to provide protections to works that are sufficiently original (WTO, 1994). The originality standard for granting copyright in a compilation of data varies from country to country, but most require some level of creative input. Within a data commons, copyright favors collectors as the members from which the database originates.

Although the data within a compilation, broadly described, may include copyrightable works (e.g., a database of satellite photos for determining land use), most agricultural data falls in the category of facts or ideas, which do not enjoy protection in and of themselves. The European Union and Mexico offer *sui generis* database rights in non-original databases that are not otherwise copyrightable. European "manufacturers" that make "substantial investments in either the obtaining, verification or presentation of the contents" enjoy a 15-year right to prohibit the reuse or extraction of substantial parts of the contents of the database (Directive 96/9/EC of the European Parliament, 1996). Mexican law provides a five-year protection for non-original databases. These

unique database rights have not gained the international traction hoped for by policymakers. In a 10-year review in 2005 of the 1996 EC Directive on databases, the EU noted that "the new instrument has had no proven impact on the production of databases" (Commission of the European Communities, 2005).

Privacy rights are not property rights, but they are an important governance mechanism that can provide stronger protection for contributors (see, for example, Lessig, 2002; Samuelson, 2000; Warren & Brandeis, 1890). Privacy rights give contributors some control over how their personally identifiable information is used. The principle of informed consent guides privacy law. Contributors must consent before collectors can gather and use identifying information. Consent often occurs when contributors, via user licences, provide access to their personal data in return for access to software or other services. There are no global instruments governing privacy rights, and laws vary greatly between jurisdictions. Privacy is a necessary part of a data commons, but privacy rights alone are not sufficient to provide for the needs of contributors in a data commons—because much valuable agricultural data is not the kind of personally identifiable data that privacy rights protect.

Protection of confidential information, i.e., trade secrets, offers some of the strongest control over data. Just because collectors own the rights to a dataset does not mean they are under an obligation to provide access to the data. Instead, databases within the control of collectors can be kept confidential, with legal consequences should the data be released. The TRIPS Agreement provides that "[n]atural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices" (WTO, 1994, art. 39(2)).

Data is typically made available via licensing contracts. Creative Commons and other standard open data licences are available to collectors that hold rights to data. These licences allow collectors to authorise the use of some or all of their rights, including: copyright in data; and copyright and *sui generis* rights in databases. While standard open data licences address the needs of collectors and users, these licences do not address the needs of contributors.

It is important to recognise the limitations of licensing as a governance mechanism in an agricultural data commons. While licences are very useful for transferring rights—e.g., giving someone the right to use a database—licences cannot be used to create rights (De Beer, 2016, p. 11). For example, a licence cannot create ownership rights for contributor data where copyright in the data does not exist. This confusion is sometimes seen in contracts where collectors tell contributors that the contributors "own" their data. In reality, contributors seeking to enforce ownership rights in their data would find that no ownership rights exist. However, certain clauses in a licence can be useful in an agricultural data commons, by creating enforceable norms,

between parties, that meet the needs of contributors and achieve goals similar to those of ownership.

Benefits and costs of participating

The modified IAD model draws attention to several social dilemmas, including: the potential for conflict between data collectors and contributors, coordinating the allocation of benefits from pooled data, and the need to aggregate data efficiently (Strandburg et al., 2017).

As shown above, contributors are essential to the continued existence of data as a resource. However, current data governance mechanisms risk alienating contributors by focusing data collection responsibilities and risks on contributors without sharing benefits. Discussions around agricultural data have not adequately grappled with the most contextually appropriate norms of reciprocity. For example, should an agricultural data commons operate on a give-and-take model or a pay-it-forward (i.e., users also contribute) model?

Carbonell (2016, pp. 2, 6) describes how the power divide between data contributors and collectors creates risks for farmers and results in coercive data collection tactics. As smallholder farmers come to understand these risks, they may withdraw from data collection or seek open access options that meet their needs. The relationship between contributors and collectors is typically asymmetric, and is certainly so for smallholder farmers in the Global South. This "big data divide" (Andrejevic, 2014, p. 1674) exists because collectors have the technical expertise, storage and processing facilities, and legal sophistication to obtain and use the data. A 2014 survey conducted by the American Farm Bureau Federation highlights some of the concerns farmers have with data collection:

> Fully 77.5% of farmers surveyed said they feared regulators and other government officials might gain access to their private information without their knowledge or permission. Nearly 76% of respondents said they were concerned others could use their information for commodity market speculation without their consent. (American Farm Bureau Federation, 2014)

These figures may reflect misunderstanding of the nature of privacy rights in aggregated data about unidentifiable persons. Respondents may be confusing invasions of personal privacy with control over confidential commercial information. This survey of 3,380 US farmer found that many farmers believed they owned their data—contrary to the legal reality, explained above with reference to De Beer (2016, p. 14), that collectors, not contributors, typically own agricultural data. The American Farm Bureau Federation survey reported that "more than 81 percent believe they retain ownership of their farm data", yet more than 82% were unaware of how

collectors intended to use their data. Again, the statistics may reflect misconceptions about data ownership (American Farm Bureau Federation, 2014). Nonetheless, such concerns are also felt by developing-world smallholder farmers, who are often skeptical of large multinational corporations.

Data collectors often rely on contracts of adhesion to license their activities. Contributors are required to agree to the collectors' terms, if they want to participate in the relationship or service, on a "take-it-or-leave-it" basis without room for negotiation (Goodman, 1999, p. 319; MacLean, 2017). Contracts of adhesion are common within consumer— particularly technology and software development— sectors because they create legal certainty and enable collectors to scale up their collection efforts.

Data contributors need to be engaged both in the creation of licences and in the development of data collection and management technologies. The American Farm Bureau Federation has done considerable lobbying on data privacy, including two surveys of its members (see American Farm Bureau Federation, 2014; 2016). The Federation has:

- built a consensus around Privacy and Security Principles (Basic Knowledge 101, 2014) among precision agriculture companies, including John Deere and Monsanto's Climate Corporation;
- founded the Agriculture Data Coalition (2017), a non-profit data platform "based on data owner permission"; and
- founded Ag Data Transparent (n.d.), which evaluates and certifies companies' contracts across 10 criteria of transparency, simplicity, and trust.

Although admirable, these efforts are solely focused on developed-world large-scale American industrial agriculture. There is also a need for data collectors to engage with the concerns of small-scale data contributors and smallholder farmers, in both the developed and developing worlds, who tend to be vulnerable and at great disadvantage when dealing with sophisticated firms (Ferris & Rahman, 2016, p. 9).

Privacy is widely recognised as a fundamental human right (e.g., UN Universal Declaration of Human Rights, 1948, art. 12). The rise of computational agriculture has created a number of privacy concerns that affect farmers. Because data lasts indefinitely, exposure to the risks of privacy breaches can compound over time. A majority of the large-scale industrial farmers participating in the 2014 and 2016 American Farm Bureau Federation surveys echoed these concerns. Meanwhile, smallholder farmers and indigenous communities are especially vulnerable because data breaches may reveal valuable traditional knowledge (Ferris & Rahman, 2016, p. 9).

Where personally identifiable information is concerned, the need for privacy extends beyond the need for protection of data to the ability to know and control who has access to data, to retrieve and share data, and to have data deleted on request. These control mechanisms have been widely recognised as needed by agribusinesses, a number of which have agreed to implement the mechanisms in their contracts with farmers (Basic Knowledge 101, 2014). These principles of privacy and control also form the basis of analysis used by Ag Data Transparent (n.d.).

We found, in our examination of the Abalobi experience with fishers in South Africa (see section 3 of this article), strong awareness of the need for data privacy controls. An Abalobi interviewee (personal communication, 2017) partially attributed high user satisfaction with, and retention of, Abalobi to its data privacy policies.

A healthy commons is one that motivates collective action by distributing costs and benefits across its members (Ostrom, 1990, p. 39). The American Farm Bureau Federation survey (2016) reported that "66 percent of farmers said it was extremely important or important that they share in potential financial benefits of their data" (p. 1). In the developing world, startups are building services around the need for benefit-sharing from data. US-based Farmobile (n.d.a; n.d.b) allows farmers to collect their own data for sale in a "Data Store" marketplace. The store allows farmers to sell single-use data licences to third parties. The licences' terms and conditions make compensation mechanisms and requirements clear, including the USD-per-acre compensation rate for data (Farmobile, n.d.a, p. 1). However, the Farmobile marketplace was, at the time of our research, limited to 500 corn and soybean farmers in the US, and contributors had to meet certification requirements to ensure the accuracy of their data.

Benefit-sharing is about more than just direct compensation. Potential benefits to be derived from agricultural data include: new fields of research, greater efficiencies in supply chain management, and new applications and artificial intelligence products built on the data. Many farmers and fishers already benefit from open data or shared data. Data collected by Plantwise is empowering research on the scope and spread of plant-based diseases (see Hirschfeld, 2017). Global Open Data for Agriculture and Nutrition (GODAN) reports on open data success stories in which open data is driving agricultural innovations (Compton, 2016; 2017), with examples including: SMART!, software that uses open data to help farmers across the world with fertiliser management; and eLEAF, a service that uses open satellite data to help farmers in South Africa lower water consumption and increase fruit production in orchards (Compton, 2016, pp. 8, 14). Demonstrating such benefits to potential data contributors can be a powerful motivator for data-sharing (Allemang & Teegarden, 2016, p. 7).

Although opening up access to data may appear to be in conflict with privacy, these concerns can be addressed by aggregating and anonymising data, and by showing contributors the value of opening data. Respecting principles of privacy and control, collectors who plan to open data should obtain consent via licensing, which we cover later in this article in section 4.

3. Relevant models of data collection and governance

In an agricultural data commons, the characteristics of the pooled resources would, for the reasons provided above, need to largely be determined by the decisions of the collectors of the data. Data-collecting actors are characterised by: differing business models; differing levels of legal sophistication; differing methods; differing approaches to data access; and differing relationships with their contributors and users. For our study, we examined three entities that collect and pool agricultural data and two entities that provide governance mechanisms that can be used to facilitate a data commons. We examined each entity's approach to data in terms of the five aforementioned elements of the Frischmann et al. (2014) modified IAD model: background of the resource; characteristics of the pooled resource; members and their roles; governance mechanisms, and costs and benefits of participating.

Examples of entities collecting data

The three entities engaged in collection of agricultural (or, in the case of Abalobi, fisheries) data that we looked at were:

- John Deere, a large US-based agribusiness;
- Plantwise, an NGO that works with smallholder farmers; and
- Abalobi, a social enterprise developing catch solutions for fishers in South Africa.

John Deere

John Deere collects agricultural data from farmers using its precision agriculture systems.

Background of the resource

The US-based agricultural machinery manufacturer John Deere (Deere & Company, n.d.a, n.d.b) is a pioneer and leader in the collection of agricultural data. John Deere began developing GPS-guided tractors in the mid-1990s (Liebhold, 2018; Stone et al., 2008). By 1997, it had launched its GreenStar Precision Farming System, proclaiming in a marketing brochure that "information is your new crop" (Liebhold, 2018).

Characteristics of the pooled resource

Precision agricultural data collected by John Deere is not publicly available. Instead, the data is held privately by John Deere, which collects and processes the data as a service to its customers. Customer farmers are only able to access the data gathered,

by the farm machinery and field-monitoring stations, on their farms. John Deere, meanwhile, has access to the complete pool of data from all its customer farmers. John Deere uses trade secrets and contractual mechanisms to maintain its proprietary control over this pooled data (Deere & Company, n.d.c, p. 4).

Members and their roles

Customer farmers enjoy, by contract, some control over the data generated on their farms. Depending on the services and applications they subscribe to, John Deere's customers can view their data via various tools giving them "real-time information about crop yield, moisture content, or seeding singulation and population, from the seat of their tractor" (Deere & Company, 2015, p. 11). Customers control whether third parties can access their data.

To the extent that farming communities' norms over the use and control of data differ from those of John Deere, there may be circumstances in which the differing norms affect the communities' relationship with the company. For example, on the issue of right-to-repair, John Deere has resisted the community norm of farmers repairing their own equipment—in favour of proprietary control over software and diagnostic tools (see for example Bartholomew, 2014).

John Deere's core objective in gathering this pool of data is to develop new products and services, particularly in the areas highlighted in its 2018 Annual Report: "artificial intelligence and machine learning" (Deere & Company, 2018). One of the first indications of John Deere's intentions to develop artificial intelligence was its USD305 million acquisition of Blue River, a company specialising in computer vision and machine learning (Deere & Company, 2017). John Deere's *Annual Report* for 2018 highlights the firm's expectation that artificial intelligence will reshape its industry.

Governance mechanisms

The primary governance mechanism used by John Deere for the data it collects from customers is a non-negotiable contract of adhesion. Farmers who wish to benefit from the data generated from their fields must agree to a Data Services and Subscriptions Statement (see Appendix A of this article) and contribute to John Deere's pooled data. The contract only applies to a limited number of countries, including the US, Canada, Australia, and South Africa. Contracts that apply to other countries have lower data and privacy protections (see, for example, Deere & Company, 2014).

In respect of privacy, John Deere's Data Services and Subscriptions Statement emphasises ownership and control of data, saying "YOU CONTROL YOUR DATA" (Appendix A). The Statement defines control over data as the ability to share data with others, to manage production data and some forms of machine and administrative data, to export production data, and to delete and amend data.

At the same time, the Statement is clear that John Deere is allowed to collect, and make its own use of, contributor data. It authorises John Deere to collect production data, machine data, and administrative data, and to use data to provide services, to develop and improve products, to market to consumers, and to comply with requests from government and regulatory agencies.

Costs and benefits of participating
This contract of adhesion creates the potential for a social dilemma (Strandburg et al., 2017). John Deere uses the contract to maximise their access to data as a resource. Contributors agree their data can be included in anonymised datasets, and that John Deere has proprietary ownership of this anonymised data.

Farmers, whom John Deere relies on to contribute data, are unable to access or benefit from this pooled data. This situation becomes a dilemma if farmers realise that the cost of losing access and control over their pooled data outweighs the benefits of John Deere's precision agriculture platform. Farmers in this situation, who do not wish to contribute to the pool, must stop using John Deere's data products. At scale, such a realisation would threaten John Deere's access to pooled data as resource.

Plantwise
Plantwise collects data on pests and diseases from smallholder farmers and provides them with plant health advice.

Background of the resource
Plantwise (n.d., 2017) is a global NGO founded by the Centre for Agricultural and Biosciences International (CABI), based in Oxfordshire, UK. Its stated mission is to reduce crop loss by giving plant health advice to smallholder farmers. Working in 34 countries, with a focus on the developing world, Plantwise has established 3,700 plant clinics and trained over 10,000 plant doctors to diagnose and treat crop ailments. These clinics generate data about the prevalence of pests and crop diseases.

Characteristics of the pooled resource
Plantwise collects data each time a farmer meets a plant doctor at a Plantwise clinic. When compiled, this data provides a frontline view of emerging pests and disease outbreaks. Although Plantwise's data pool is non-rivalrous—multiple people can use the data at one time—it is nationally sensitive and excludable, because information about the spread of pests and crop diseases can affect trade relations and markets and thus cannot be widely shared. Plantwise's relationship with its partner countries is based on the understanding that each country owns the data collected within their borders (Plantwise interviewee, personal communication, 2017).

Members and their roles
Farmers bring plant samples into Plantwise clinics, often located in local marketplaces. Plant doctors examine the plants and prescribe recommended treatments. During this process, the plant doctors, who are often government extension workers, collect data by filling out a diagnostic form, often completed electronically on handheld digital tablet devices (Plantwise interviewee, personal communication, 2017). After the data is recorded, it is transferred to a central processing facility where it goes through a process of harmonisation and validation to ensure accuracy, before being analysed and stored in the Plantwise Online Management System (Sluijs, Posthumus, & Katothya, 2017).

Governance mechanisms
Plantwise does not seek explicit permission from farmers to collect data, but farmers see the data collection process taking place. Plant doctors are trained to discuss issues of data privacy and ownership with farmers.

Plantwise uses institutional and technological mechanisms to govern data collection and use (Sluijs et al., 2017). Institutional mechanisms include the relationships Plantwise has developed with partner countries and the programmes it has developed to train its data collectors. Technological mechanisms include the processes Plantwise has developed to process, clean, validate, and store data as it is collected. Another technological mechanism Plantwise administers is the access controls used to permit authorised users—often local government extension agents—to access data and reports (Sluijs et al., 2017, p. 17).

Costs and benefits of participating
Government agencies use Plantwise data to develop agricultural policy and to respond to pest and disease outbreaks. Farmers see some indirect benefits from the data, as it is used to train plant doctors and fine-tune their diagnoses. The data also contributes to the publicly available Plantwise Knowledge Bank, which contains information on identifying and treating plant diseases (CABI, n.d.). Farmers using Plantwise clinics have reported improved crop yields and increased income. For example, tomato yields in Malawi were found to be 20% higher for clinic users than for non-users (Bett et al., 2018, p. 15).

However, the national security implications of the data introduce a social dilemma of resource availability: limited access may prevent users from fully exploiting the pooled data for insights and further benefits. Plantwise has explored opening the data to select partners and researchers, but to do so requires the consent of each government, which has been challenging (Plantwise interviewee, personal communication, 2017).

Abalobi

Abalobi collects data on South African small-scale fisheries while providing business management tools to fishers.

Background of the resource

Abalobi (n.d.a) is a non-profit social enterprise that provides South African fishers with a suite of applications (apps) to track, manage, and sell their catches. Abalobi's products aim to help fishers build small businesses or form fisher cooperatives. At the same time, South African science, conservation, and planning entities have expressed interest to Abalobi in the collected data on the country's small-scale fisheries (Abalobi interviewee, personal communication, 2017). The apps could provide a way to connect the scientific community with local knowledge while still respecting the rights of fishers, who tend to be skeptical of institutions (Abalobi interviewee, personal communication, 2017).

Characteristics of the pooled resource

The apps are published on an open source basis, allowing other developers to build on them. Fishers wanting to use Abalobi must first register for the service. On registering, the fishers are asked to agree to Terms of Use (see Appendix B of this article) that detail access to and use of contributor data. Once registered, the fisher receives access to the Abalobi suite of apps. These apps include the Fisher app, offering a personal logbook and weather portal that can help fishers stay safe at sea; the Monitor app, for logging catches at the landing site; the Manager and Co-op apps, providing real-time fishery data and fleet management; and the Marketplace app, connecting fishers to markets and also enabling generation of "social stories" about the products. The pooled data generated by these apps can provide the aforementioned scientific, conservation and planning entities with a range of useful data, including the size and location of catches, which might otherwise go unreported.

Members and their roles

Three groups are involved in the pooled resource. First, the fishers are the data contributors, provide fishery data while using the apps. Second, Abalobi serves as the data collector. Third, universities, research facilities, and government entities such as the South African Department of Agriculture, Forestry and Fisheries (DAFF), comprise potential users of the data.

Governance mechanisms

Abalobi asks fishers to agree to its Terms of Use before using its apps. The Terms of Use promise to treat contributor data "with the utmost of privacy" (Appendix B). While fishers must agree that Abalobi staff can access data to maintain and improve the system, fisher data is not shared with third parties without consent. At the point of sign-up, contributors are asked whether they agree to share their data with specific

third parties: the DAFF and local fisher assistants—who work for cooperatives of fishers. Contributors are able to separately choose to share their data with either of the third parties. Abalobi understands this consent to mean that its staff would have to obtain new permission to use the data for other purposes, including other forms of research (Abalobi interviewee, personal communication, 2017).

Abalobi's development was guided by its need to address a social dilemma. The organisation found that fishers generally did not trust the government to work in their interests and were skeptical of how their data might be used (Abalobi interviewee, personal communication, 2017). As a result, Abalobi designed its app to emphasise the fishers' data ownership—and securing of fishers' consent before releasing data to third parties. Fishers who use the apps can choose whether or not their data is part of the pool shared with third parties. Only Abalobi fishers who consent to data-sharing become contributors to the pooled data. Through working with the fishers in co-design of its apps, Abalobi was able to identify the need to engender trust (via transparency and informed consent) as crucial to having fishers adopt its applications and agree to share data (Abalobi interviewee, personal communication, 2017).

Costs and benefits of participating

The primary benefits of Abalobi's apps are the service and information components available to fishers. Because data-sharing is optional and fishers are understood to own their data, fishers are able to receive the benefits of using the apps regardless of whether or not they agree to share their data with third parties.

At the time of our research in 2017, Abalobi did not publish or provide open access to fisher data. According to the Terms of Use, Abalobi can publish aggregate data without seeking further permission from fishers (e.g., "total kg Snoek catch recorded in South Africa in Nov 2016"). However, Abalobi does not interpret the relevant clause in the Terms of Use as allowing it to publish open data (which it had not yet done at the time of our research) without first obtaining further permission from the fishers who use its apps.

Abalobi makes one exception to its policy of making data-sharing optional. Fishers who wish to use the Market app to sell fish must consent to sharing data with third parties, but only on the marketplace. In addition to connecting fishers to buyers, the app allows fishers to attach "social stories" to their catches by identifying where and when fish are caught (Abalobi interviewee, personal communication, 2017). Fishers are able to use these "social stories" to sell their catches at a higher price, which can help demonstrate the value of sharing data.

Examples of entities that facilitate open data governance

We also examined two entities that facilitate the governance and distribution of pooled data:

- Creative Commons; and
- Open Data Commons.

Creative Commons

Creative Commons provides a suite of licences that allow copyright owners to authorise the use of their protected works while imposing conditions on how the work is used, such as requiring attribution, limiting the distribution of derivative works, and preventing use in commercial projects (Creative Commons, n.d.a).

Background of the resource

Creative Commons offers copyright owners a way to make their works publicly available while reserving some rights (Creative Commons, n.d.a). The Creative Commons (n.d.b) organisation enables a commons by maintaining and updating six different licences that copyright owners can apply to their works (Creative Commons, n.d.c). Creative Commons is an active supporter of the open data movement and many organisations, institutions, and governments publish their works under the Creative Commons licences (Creative Commons, n.d.d).

Characteristics of the pooled resource

Copyright owners had, as of 2017, collectively published over 1.4 billion works under a Creative Commons licence (Creative Commons, 2017). Works licensed under Creative Commons are public goods in that they are both non-rivalrous and non-excludable to an extent—anyone can freely access and use the works without limiting the ability of others to use the works. The success of Creative Commons demonstrates that copyright holders receive value from sharing their works when they are able to retain rights to attribution, distribution, and commercial use (Lessig, 2004).

Members and their roles

Creative Commons depends on copyright owners choosing to make their works publicly available. In the context of agricultural data, collectors may choose to use the Creative Commons licence to make their data available to users. Many collectors, including the global private-sector agribusiness firm Syngenta (2017), use the Creative Commons licences to open their data to the public.

Governance mechanisms

Data can be licensed using version 4 of the Creative Commons licences, which have broad application, covering rights in databases and, when applicable, rights in the data itself. The version 4 licences cover rights held via both copyright and, when applicable, *sui generis* database rights. Creative Commons (n.d.e) offers six different distribution

licences, which are characterised by stackable rights. The most permissive licence, the Attribution (CC BY) licence, allows any use as long as there is attribution of the source. The least permissive licence, the Attribution-NonCommercial-NoDerivs (CC BY-NC-ND) licence, requires that the user provide attribution, not make commercial use of the work, and not make derivatives of the work. The other four licences fall in between these two licences in terms of permissiveness.

Each of the licences has its own logo composed of a set of graphical marks that visually indicate the responsibilities associated with using the content, i.e., a mark for Attribution, a mark for NonCommercial, and so on. Creative Commons licences have a "three-layer" design (n.d.e) that makes them easy to use and have contributed to their success. The licences' legal language is supported by a human-readable layer that is easy to understand, and by a machine-readable layer that lets software (e.g., Google Image Search) understand what licence has been applied. Creative Commons has developed a licence wizard that makes it easy for owners choose a licence.

Costs and benefits of participating
One of the benefits of using Creative Commons is the degree of control that copyright owners have over how their works are licensed. This layering of licences allows them to be adapted to a broad range of use cases. For example, copyright owners (i.e., data collectors, for the purposes of this study) can choose whether or not to allow the data to be used for commercial purposes.

Open Data Commons
The Open Data Commons provides three licences that allow the owners of copyrighted databases to authorise the use of their databases while still retaining and limiting certain rights.

Background of the resource
The Open Data Commons (ODC) seeks to "provide legal solutions for open data" (Open Data Commons, n.d.). The licences are hosted by an Advisory Council made up of legal and subject-matter experts who draft and manage the licences. The most recent update to the licences occurred with the publication of the ODC Attribution License (ODC-BY) in 2010 (Hatcher, 2010). An organisational email discussion list was last active in November 2018 (odc-discuss, n.d.).

Characteristics of the pooled resource
The ODC organisation does not provide statistics or usage rates for its licences, which may be attributed to the lack of a machine-readable layer in the licence's design. Like the Creative Commons licence, the ODC licences are non-rivalrous—anyone can use the licensed databases without limiting other uses. The ODC licences, however, exclude certain rights that are granted by Creative Commons. Specifically, the ODC licences only provide access to *sui generis* database rights and copyrights held in the

structure of databases (e.g., organisational fields and tables), and not to the content of the database being licensed (e.g., crop yield data).

Members and their roles
Data collectors are the primary members of the Open Data Commons. They must choose to use the ODC licence to make databases publicly available. Data users may find that ODC-licensed databases are less usable, if they are concerned about rights to the data inside licensed databases. Data contributors are not involved in ODC licensing because copyright in database structures are wholly owned by collectors.

Governance mechanisms
Open Data Commons offers three licences to data collectors wishing to make their data open: an Attribution License (ODC-BY), an Open Database License (ODbL), and a Public Domain Dedication and License (PDDL). Similar to the choices under the Creative Commons system, data collectors can choose whether they wish to put their databases in the public domain, or to limit certain rights such as: requiring attribution, requiring sharing under the same terms of use, and/or allowing adapted works. All three licences are version 1, and include both a human-readable summary as well as the legal licence but not a machine-readable version. A graphical mark is not offered; instead, the licences are applied through a textual statement.

Costs and benefits of participating
The ODC licences offer a useful tool for sharing information about data structures. Collectors may benefit from being able to exclude copyright to data—which may or may not exist—when licensing their databases. However, these exclusions may limit the usefulness of ODC-licensed databases for users of agricultural data. Another potential risk to using an Open Data Commons licence is the organisation's lack of activity since 2010. Copyright law is not static, and data collectors would be wise to ensure that the licence continues to adequately meet their needs.

4. The need for a model licence, certification mark, and organisational support
Successful creation of an agricultural data commons would, in our analysis, require a model back-to-front licence, and a certification mark, both supported by a public interest organisation and its supporting community.

Model licence
A model back-to-front licence would consist of two linked licences covering the two main relationships in the agricultural data commons. The first of the two linked licences, for data collection, would be between data collectors and data contributors. The second licence, the distribution licence that would make the data openly available, would be between data collectors and data users. (The distribution licence would fulfil the assurances of privacy, control, and openness made in the collection licence.)

A model back-to-front licence for agricultural data collection would help data-collecting SMEs to meet their legal obligations and would address the related social dilemmas of: how to avert conflict between contributors and collectors; and how to coordinate apportionment of benefits between contributors, collectors and users. Abalobi, for example, expressed a need for sophisticated legal solutions that will help them to manage their relationships with contributors and users (Abalobi interviewee, personal communication, 2017).

The findings of our study suggest that the model back-to-front licence must have several key characteristics. First, the licence should balance the needs of all stakeholders. This balancing can be achieved by, among other things, providing tools to help data collectors engage with contributors, users, and other stakeholders. These tools could include model terms of use statements, model licences, and other resources detailing best practices for engaging stakeholders.

Second, the licence should be modular. The Creative Commons and Open Data Commons licensing schemes have shown the value in providing a suite of licences that address a variety of usage scenarios. The Creative Commons licences maximise adoption by letting creators choose which licence best fits their needs. The Open Data Commons fills a gap by allowing collectors to license database structures without licensing the data they contain. Similarly, the back-to-front licence should give data collectors a variety of options to choose from in order to meet specific business models. The modular model licence would need to provide for: variances in what and how much data is made open; opportunities for other benefit-sharing measures; and varying degrees of control over data.

Finally, the model licence would need to be designed so as to maximise use. Following the successful practices developed by Creative Commons, the licence should consist of three layers, with the legal code of the licence supported by both a human-readable layer and a machine-readable layer. While the human-readable layer is important for simplicity of use, the machine-readable layer is particularly important, in order to maximise use by app developers.

The organisation supporting this back-to-front licence would need to address several potential challenges. Collectors may want more individual control over specific licence terms than are possible with a model licence. Adoption may be slow, as many collectors, which this proposed model relies on, may be hesitant to open up their data. And collectors who want to implement a data commons will still face the challenges of working with their third-party vendors to ensure conditions that respect the commitments they make in the licence.

Furthermore, because open licences are rarely if ever considered in court, the status and enforceability of the back-to-front licence will remain somewhat uncertain, with

the degree of its legal force resulting as much from social convention as from legal precedent. (However, in this respect, open copyright licensing contracts may not be much different from other contracts governed more by general principles than specific rulings.)

Certification mark

In order for a data commons to garner sufficient support, there would need to be mechanisms in place to motivate engagement. Ostrom (1990, pp. 185–187) describes how monitoring and graduated sanctions are necessary to ensure mutual participation in the commons. In the context of a knowledge commons, participants will often experience rewards and benefits that help motivate participation (Frischmann et al., 2014, p. 37). However, motivations that work in other knowledge commons may not provide sufficient benefits in this context. We suggest using a certification mark to motivate participation in the agricultural data commons.

Certification marks are trademarks that a certifying organisation issues to entities that meet qualifying standards (see Fromer, 2017, p. 127; Mogyoros, 2015). In an agricultural data commons, a certification mark would indicate to contributors, collectors, and users: (1) that the data is sourced equitably; (2) that the collector offers open data; and (3) that the collector is using the particular back-to-front licence required by the certification mark. Simply stated, the mark would be an indication of the best practices followed throughout the value chain related to the data (see De Beer, 2017a, p. 21). Use of the mark would motivate collectors to participate in the agricultural data commons—by drawing positive attention to collectors' open data collection practices and building trust in the collectors among data contributors and users.

A relevant example is the Fair Trade movement (Fairtrade International, n.d.), which uses certification marks to support marginalised producers in low-income countries, and which has its origins in agriculture production. The Fair Trade movement has been successfully used as a template in many sectors, including being adapted to the music and forestry industries (Fair Trade Music International, n.d.; Leonardi, Clement, & Defranceschi, 2012).

Organisational support

The model licence and certification mark would need to be supported, as is the case for Creative Commons and the Open Data Commons, by an organisation and community dedicated to building and managing the licence scheme. The proposed certification mark would, ideally, be governed and managed by a single organisation. This work could be done by an existing organisation, such as GODAN, Open Data Commons, or Creative Commons, or by a newly-created organisation (with attributes similar to Fairtrade International).

5. Conclusions

This study has developed the outlines of a model for an agricultural data commons that could address the inequities currently created by lack of data ownership rights for contributors of agricultural data. Supported by an independent organisation, this model licence could increase the pool of open data by providing incentives: (1) to data contributors, who need engagement, privacy, control and benefit-sharing; (2) to SME data collectors, who need sophisticated legal tools; and (3) to data users, who need access to useable data. Additionally, we have proposed that use of the model licence, and thus growth of the agricultural data commons, could be given a market-driven dimension through granting users of the model licence the ability to use a certification mark.

These governance mechanisms would increase access to agricultural data by fostering shared responsibility for the data as a common resource. This increased access to data would have the potential to address food insecurity by helping participants across food production chains make better decisions—in both developed- and developing-world contexts, but with particular relevance to the developing world and thus, in turn, with relevance to achievement of UN Sustainable Development Goal (SDG) 2 aimed at eradicating extreme hunger (UN, 2015, p. 17).

In addition to its relevance to the global effort to meet SDG 2, the field of agriculture was chosen for this study because of: (1) the recognition, in both the open data and agricultural communities, of inequitable treatment of contributors of agricultural data; (2) the presence of exemplar stakeholders, such as Plantwise and Abalobi, whose work has been amplified by organisations like GODAN and OD4D; (3) the presence of social certification examples, such as Fair Trade, that have pioneered market-driven equitable agriculture production; and (4) the origins of commons, and commons scholarship, in agriculture.

The model outlined in this article in support of enlarging the agricultural data commons could be broadly applicable to other contexts where contributors generate data and open access to data is valued. A back-to-front model licence and certification mark could be particularly useful in contexts where, as is increasingly the case, SMEs collect and use data.

References

Abalobi. (n.d.a). Website. Retrieved from http://abalobi.info

Abalobi. (n.d.b). Abalobi register [Website]. Retrieved from http://register.abalobi.org

Ag Data Transparent. (n.d.). Core principles [Website]. Retrieved from https://www.agdatatransparent.com/principles

Allemang, D., & Teegarden, B. (2016). *A global data ecosystem for agriculture and food.* Wallingford, UK: Global Open Data for Agriculture and Nutrition (GODAN). Retrieved from http://www.godan.info/documents/data-ecosystem-agriculture-and-food

American Farm Bureau Federation. (2014, October 21). American farm bureau survey shows big data use increasing, big questions remain. *AFB Newsroom*. Retrieved from https://www.fb.org/newsroom/american-farm-bureau-survey-shows-big-data-use-increasing-big-questions-rem

American Farm Bureau Federation. (2016). *Highlights of the farm bureau big data survey – May 2016*. Washington, DC. Retrieved from https://farmweeknow.com/mdfm/Fareek3/author/29/2016/5/BigDataSurveyHighlights.pdf

Andrejevic, M. (2014). The big data divide. *International Journal of Communication. 8*, 1673-1689. Retrieved from http://ijoc.org/index.php/ijoc/article/view/2161/1163

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal. 22*(7), 97-114. Retrieved from https://www.rfidjournal.com/articles/view?4986

Baarbé, J., Blom, M., & De Beer, J. (2017). *A data commons for food security*. Open AIR Working Paper 7. University of Cape Town and University of Ottawa: Open African Innovation Research (Open AIR).

Bartholomew, D. (2014). *Long comment regarding a proposed exemption under 17 U.S.C. 1201.* Moline, IL: Deere & Company. Retrieved from https://www.copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf

Basic Knowledge 101 (BK101). (2014). Privacy and security principles for farm data, November 13, 2014. Retrieved from http://www.basicknowledge101.com/pdf/PrivacyAndSecurityPrinciplesForFarmData.pdf

Bett, E., Mugwe, J., Nyalugwe, N., Haraman, E., Williams, F., Tambo, J., Wood, A., & Bundi, M. (2018). Impact of plant clinics on disease and pest management, tomato productivity and profitability in Malawi. CABI Working Paper 11, 30. Oxfordshire, UK: Centre for Agriculture and Bioscience International (CABI). Retrieved from https://site.plantwise.org/wp-content/uploads/sites/4/2019/03/WP11_plant_clinics_malawi-2.pdf

Burners-Lee, T. (2017, March 12). I invented the web. Here are three things we need to change to save it. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet

Carbonell, I. M. (2016). The ethics of big data in agriculture. *Internet Policy Review, 5*(1), 1-13. https://doi.org/10.14763/2016.1.405

Carolan, L., Smith, F., Protonotarios, V., Schaap, B., Broad, E., Hardinges, J., & Gerry, W. (2015). *How can we improve agriculture, food and nutrition with open data?* London: Open Data Institute. Retrieved from https://theodi.org/how-improve-agriculture-food-nutrition-open-data

Centre for Agricultural and Biosciences International (CABI). (n.d.). Plantwise Knowledge Bank [Website]. Retrieved from https://www.plantwise.org/knowledgebank

Christovich, M. M. (2016). Why should we care what Fitbit shares? A proposed solution to protect personal fitness information. *Hastings Communications and Entertainment Law Journal, 38*(1), 91-116. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/hascom38&div=8&id=&p age=

Commission of the European Communities. (2005). *First evaluation of Directive 96/9/EC on the legal protection of databases*. Brussels. Retrieved from http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf

Compton, S. (2016). *Success stories issue 1*. Wallingford, UK: Global Open Data for Agriculture and Nutrition (GODAN). Retrieved from http://www.godan.info/documents/godan- success-stories-issue-1

Compton, S. (2017). *Success stories issue 2*. Wallingford, UK: Global Open Data for Agriculture and Nutrition (GODAN). Retrieved from http://www.godan.info/documents/godan-success- stories-issue-2

Creative Commons (n.d.a). History [Wiki]. Retrieved from https://wiki.creativecommons.org/wiki/history

Creative Commons (n.d.b). Website. Retrieved from https://creativecommons.org

Creative Commons. (n.d.c). Program areas. Retrieved from https://creativecommons.org/about/program-areas

Creative Commons. (n.d.d). Data [Wiki]. Retrieved from https://wiki.creativecommons.org/wiki/data

Creative Commons. (n.d.e). About the licenses. Retrieved from https://creativecommons.org/licenses

Creative Commons. (2017). State of the commons. Retrieved from https://stateof.creativecommons.org

Davies, T. (2010). *Open data, democracy and public sector reform: A look at open government data use from data.gov.uk*. Master's thesis, University of Oxford. Retrieved from http://practicalparticipation.co.uk/odi/report/wp-content/uploads/2010/08/How-is-open-government-data-being-used-in-practice.pdf

Davies, T. (2015, September 2). Data, openness, community ownership and the commons [Blog post]. Tim Davies Blog. Retrieved from http://www.timdavies.org.uk/2015/09/02/openness-community-ownership-and-the- commons

De Beer, J. (2016). *Ownership of open data: Governance options for agriculture and nutrition.* Wallingford, UK: Global Open Data for Agriculture and Nutrition (GODAN). Retrieved from http://www.godan.info/documents/data-ecosystem-agriculture-and-food

De Beer, J. (2017a). Making copyright markets work for creators, consumers, and the public interest. In R. Giblin & K. Weatherall (Eds.), *What if we could reimagine copyright?* (pp. 147-175). Canberra: ANU Press. https://doi.org/10.22459/WIWCRC.01.2017.05

De Beer, J. (2017b). *Open innovation in development: Integrating theory and practice across open science, open education, and open data.* Open AIR Working Paper 3. University of Cape Town and University of Ottawa: Open African Innovation Research (Open AIR). Retrieved from https://openair.africa/2017/01/26/open-innovation-in-development-integrating-theory-and-practice-across-open-science-open-education-and-open-data/

Deere & Company. (n.d.a). Privacy summary. Retrieved from http://www.deere.com/privacy_and_data/privacy_and_data_sub_saharan_africa.page

Deere & Company. (n.d.b). Precision Ag technology. Retrieved from https://www.deere.com/en_US/products/equipment/ag_management_solutions/ag_management_solutions.page

Deere & Company. (n.d.c). John Deere Network terms & conditions of use agreement. Retrieved from https://registration.deere.com/tou/printable_en.pdf

Deere & Company. (2014). Privacy and data: Privacy summary. Retrieved from http://www.deere.com/privacy_and_data/en_CAF/privacy_and_data_sub_saharan_africa.page

Deere & Company. (2015). *Annual report*. Moline, IL. Retrieved from https://s22.q4cdn.com/253594569/files/doc_financials/annual_proxy/2015_John-Deere-Annual-Report.pdf

Deere & Company. (2017). Deere to advance machine learning capabilities in acquisition of Blue River Technology [News release]. Retrieved from https://www.deere.com/en/our-company/news-and-announcements/news-releases/2017/corporate/2017sep06-blue-river-technology

Deere & Company. (2018). *Annual report.* Moline, IL. Retrieved from https://s22.q4cdn.com/253594569/files/doc_financials/annual_proxy/2018/2018_John-Deere-Annual-Report.pdf

De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of big data based on its essential features. *Library Review, 65*(3), 122-135.

https://doi.org/10.1108/LR-06-2015-0061

Fairtrade International. (n.d.). Aims of Fairtrade standards. Retrieved from https://www.fairtrade.net/standards/aims-of-fairtrade-standards.html

Fair Trade Music International. (n.d.). About us. Retrieved from http://www.fairtrademusicinternational.org/about-fair-trade-music-international

Farmobile. (n.d.a). Legal agreements. Retrieved from https://www.farmobile.com/legal

Farmobile. (n.d.b). Data store guarantee: Terms of agreement. Retrieved from https://www.farmobile.com/static/www/docs/legal/DataStore_Agreement.pdf

Ferris, L., & Rahman, Z. (2016). *Responsible data in agriculture*. Wallingford, UK: Global Open Data for Agriculture and Nutrition (GODAN). Retrieved from http://www.godan.info/file/46934/download?token=Co5JuSLO

Frischmann, B. M., Madison, M. J., & Strandburg, K. J. (Eds.) (2014). *Governing knowledge commons*. Oxford: Oxford University Press.

Fromer, J. C. (2017). The unregulated certification mark. *Stanford Law Review, 69*, 121-200. Retrieved from https://cdn2.hubspot.net/hubfs/454850/Certification%20Mark%20Article.pdf?t=14862 98244199

Global Open Data in Agriculture and Nutrition (GODAN). (2015). Agriculture and nutrition session at Africa Open Data Conference. Retrieved from http://www.godan.info/challenges-for-global-open-data-in-agriculture-and-nutrition-the-godan-debate-at-aodc

Goodman, B. (1999). Honey, I shrink-wrapped the consumer: The shrink-wrap agreement as an adhesion contract. *Cardoso Law Review, 21*(1), 319. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/cdozo21&div=14&id=&p age=

Hatcher, J. (2010, June 24). Open Data Commons – Attribution license released [Blog post.] Open Data Commons blog. Retrieved from https://opendatacommons.org/2010/06/24/open-data-commons-attribution-license-released/index.html

Hirschfeld, M. (2017, April 16). Data from plant clinics is contributing to Trinidad and Tobago's agricultural database [Blog post.] The Plantwise Blog. Retrieved from https://blog.plantwise.org/2017/04/26/data-from-plant-clinics-is-contributing-to-trinidad-and-tobagos-agricultural-database/#more-13211

Jellema, A., Meijninger, W., & Addison, C. (2015). Open data and smallholder food and nutritional security. CTA Working Paper 15/0. Wageningen, Netherlands: Technical Centre for Agricultural and Rural Cooperation (CTA).

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives and prospects. *Science, 349*(6245), 255-260. https://doi.org/10.1126/science.aaa8415

Leonardi, A., Clement, S., & Defranceschi, P. (2012). *How to combine fair trade and forest management certification.* Freiburg, DE: Sustainable Timber Action Fund. Retrieved from http://www.sustainable-timber-action.org/fileadmin/files/STA_Toolkit/HOW_TO_COMBINE_FAIR_TRADE_AND_FOREST_MANAGEMENT_CERTIFICATION_Final.pdf

Lessig, L. (2002). Privacy as property. *Social Research, 69*(1), 247-269. Retrieved from http://www.jstor.org/stable/40971547

Lessig, L. (2004). The Creative Commons. *Montana Law Review, 65*(1), 1-14. Retrieved from https://scholarship.law.umt.edu/mlr/vol65/iss1/1

Liebhold, P. (2018). The crop of the 21st century [Blog post]. National Museum of American History blog. Retrieved from https://americanhistory.si.edu/blog/precision-farming

MacLean, C. (2017). It depends: Recasting internet clickwrap, browsewrap, "I agree," and click-through privacy clauses as waivers of adhesion. *Cleveland State Law Review, 65*(1), 43-57. Retrieved from https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=3934&context=clevstlrev

Manovich, L. (2012). Trending: The promises and the challenges of big social data. In M.K. Gold (Ed), *Debates in the digital humanities* (504-521). Minneapolis: University of Minnesota Press. https://doi.org/10.5749/minnesota/9780816677948.003.0047

Mogyoros, A. (2015). *Exploring the nature of certification marks*. BCL dissertation, University of Oxford.

odc-discuss. (n.d.). Archives [Mailing list]. Retrieved from https://lists.okfn.org/pipermail/odc-discuss

Open Data Charter. (2016, July 15). What is the vital data infrastructure for agriculture? [Blog post]. Retrieved from http://opendatacharter.net/vital-data-infrastructure-agriculture

Open Data Commons. (n.d.). About. Retrieved from https://opendatacommons.org/about/index.html

Open Data Handbook. (n.d.). What is open data? Retrieved from http://opendatahandbook.org/guide/en/what-is-open-data

O'Reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & Strategies, 65*(1), 17-37. Retrieved from https://mpra.ub.uni-muenchen.de/4578/1/mpra_paper_4578.pdf

Ostrom, E. (1990). Governing the commons: The evolution of institutions for collective action. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9780511807763

Plantwise. (n.d.). Website. Retrieved from https://www.plantwise.org

Plantwise. (2017). *Annual report 2016.* Retrieved from https://www.plantwise.org/Uploads/Plantwise/Plantwise%20Annual%20Report%20201 6.pdf

Samuelson, P. (2000). Privacy as intellectual property? *Stanford Law Review, 52*(5), 1125-1173. https://doi.org/10.2307/1229511

Sluijs, J., Posthumus, H., & Katothya, G. (2017). Plant clinic data management: An assessment of the use, management and functioning of the Kenyan Plantwise Data Management System. Oxfordshire, UK: Centre for Agriculture and Bioscience International (CABI). Retrieved from https://site.plantwise.org/wp-content/uploads/sites/4/2019/03/Sluijs-And-Posthumus-Data-Management-System-Kenya-2017.pdf

Strandburg, K. J., Frischmann, B. M., & Madison, M. J. (2017). The knowledge commons framework. In K. J. Strandburg, B. M. Frischmann, & M. J. Madison (Eds.), *Governing medical knowledge commons* (pp. 9-18). Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/9781316544587.002

Stone, M. L., Benneweis, R. K., & Van Bergeijk, J. (2008). Evolution of electronics for mobile agricultural equipment. *Transactions of the American Society of Agricultural and Biological Engineers, 51*(2), 385-390. https://doi.org/10.13031/2013.24374

Syngenta. (2017). The good growth plan progress data - productivity 2016. [Dataset.] Retrieved from https://www4.syngenta.com/~/media/Files/S/Syngenta/odi-progess/2016/pdf/SYT-GGP-c1productivity-description.pdf

The Economist (2017, May 6). The world's most valuable resource is no longer oil, but data. Retrieved from http://www.economist.com/news/leaders/21721656-data-economy-demands-new- approach-antitrust-rules-worlds-most-valuable-resource

UN. (1948). Universal Declaration of Human Rights.

UN. (2015). Transforming our world: The 2030 Agenda for Sustainable Development. A/RES/70/1. Brussels. Retrieved from https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, IV*(5), 193-220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M-J. (2017). Big data in smart farming – a review. *Agricultural Systems, 153*, 69-80. https://doi.org/10.1016/j.agsy.2017.01.023

World Trade Organisation. (WTO). (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

Appendix A: Text of John Deere's Data Services and Subscriptions Statement [1]

JOHN DEERE DATA SERVICES & SUBSCRIPTIONS STATEMENT

YOU CONTROL YOUR DATA

In an increasingly connected world, technology makes it easy for you to share your operation's data with others — if that's what you choose to do. When you entrust your data to John Deere and its subsidiaries through our Data Services and Subscriptions, we safeguard that data and honor the permissions you set for sharing it with others.

We created this statement to be clear about how we manage your data and to provide the details you need to make informed decisions about our Data Services and Subscriptions. This statement explains:

- your responsibilities for managing your data and sharing permissions, as well as your options in the event that you do not want John Deere to use or disclose your data
- the types of data we may collect from you
- how we may use or disclose that data
- our responsibilities for protecting and maintaining your data

By accessing or using any John Deere Data Services and Subscriptions, you agree that we may collect and process your personal information as described in our Privacy Policy, and you agree that we may use your data as described below and in the applicable terms of use. If you do not or cannot agree to these uses by John Deere, then you should not use John Deere Data Services and Subscriptions.

TYPES OF DATA WE COLLECT

We collect three kinds of data through the John Deere Data Services and Subscriptions, which include the John Deere Operations Center, JD Link™, and other offerings listed at www.JohnDeere.com/agreements:

Production Data is information about the work you do with your equipment and the land where you do that work. For example: • field task details • area worked • route travelled • crop harvested and yield data • agronomic inputs applied You can see and manage your Production Data in the John Deere Operations Center and mobile apps.	**Machine Data** is information that indicates machine health, efficiency, and function. Machine Data comprises: • machine health indicators, settings and readings • machine hours or life • machine location • diagnostic codes • software and firmware versions • machine attachments, implements or headers You can see some Machine Data in the John Deere Operations Center, JDLink Web and mobile apps. Some Machine Data is proprietary to John Deere.	**Administrative Data** is information that helps us support your account and activities in our system. For example: • your data sharing permissions • users linked to your account • machines, devices, and licenses linked to your account • number of acres and size of files • information about how you use your account You can see and manage some Administrative Data in the John Deere Operations Center and mobile apps.

1 Retrieved from https://www.deere.com/en/privacy-and-data/data_services/

We do not use or collect user-generated content. Some of our systems enable you to store and share information you or others create. This user-generated content includes variable rate prescriptions, notes, recordings, photographs, PDFs and other file types. We store and share this content only as you direct and to comply with court orders and legal or regulatory requirements.

YOU CONTROL WHO SEES YOUR DATA
Here are your options for controlling your account information when you use John Deere's Data Services and Subscriptions:

SHARING
You may share and disclose data in the John Deere Operations Center and other connected portals and apps. By setting permissions for your account, you control other parties' access and visibility into your data. You also control which John Deere dealers have access to data in your account. […] Please note that when you share your information with someone other than John Deere, the recipient may decide to copy, use, modify, or distribute it to others, and John Deere has no control over, or responsibility for, any such activities.

MANAGING
You may view, analyze, and manage Production Data, some Machine Data, and some Administrative Data in your account via the John Deere Operations Center and JDLink portals.

EXPORTING
You may download and export Production Data files in the John Deere Operations Center, and you may download some Machine Data from the JDLink portal.

DELETING, UPDATING, AND AMENDING
You may request that we delete, update or amend Machine Data, Production Data, and Administrative Data in your account and we will honor your request within five business days. Please note that deleting data may limit our ability to support you and, in some cases, may constitute a termination under the terms of any applicable Data Service and Subscription contracts between you and John Deere, and - subject to any applicable privacy laws - we may retain certain basic Machine or Administrative data for our record keeping purposes. Please review the terms of any such contract for details.

TO SERVE YOU
- We use your data to provide you with contracted services and offerings and to administer your account.
- We may share your data with John Deere affiliates and suppliers to provide you with contracted services and offerings and to administer your account. These affiliates and suppliers have committed to protect your data consistent with this statement and all applicable privacy and other laws. [7]
- Machine and Administrative Data only – We may share Machine Data and Administrative Data with John Deere dealers so they can support you, unless you explicitly restrict access to specific dealers.

TO LEARN FROM YOU
- We may use your data to develop and improve our products and services. For example, analyzing your data may spotlight trends that inform our product support, warranty services, and diagnostic or prognostic activities.
- We may combine your data with data from others and include your data in anonymized data sets. These anonymized data sets are proprietary to John Deere. John Deere is free to use and disclose the anonymized data, and John Deere may promote information and services derived from anonymized data. Anonymized data is never traceable back to you or your specific operations.

TO MARKET TO YOU

- We may use your data to market products and services to you, targeting offerings to match your activity, interests, and location if you provide any applicable consent. We will communicate with you only according to the preferences you set for your account.
- We may share your data with John Deere dealers so they can market products and services to you, targeting offerings to match your activity if you provide any applicable consent.

TO COMPLY WITH THE LAW

- We share your data as required by applicable laws, including data privacy and consumer protection laws. Our privacy statement is available at www.JohnDeere.com/legal.
- We may review and disclose your data to comply with court orders and legal or regulatory requirements; to prevent injury, death, losses, fraud or abuse; to protect John Deere's rights or to defend John Deere in legal proceedings; and to comply with requests from you.

We do not do anything else with your data without your separate consent. If you do not or cannot agree to the data uses described above, then you should not use John Deere Data Services and Subscriptions.

HOW WE PROTECT AND MAINTAIN YOUR DATA

SAFEGUARDING

We have implemented and will maintain standards and procedures designed to prevent misuse of information in your account:

- We maintain physical computer and network security.
- We educate our employees about the importance of data security and customer service through standard operating procedures and special training programs.
- We maintain security standards and procedures to help prevent unauthorized access to information about you, and we update and test our technology to improve the protection of your information.

STORING AND PROCESSING

We store and process data on secure servers in data centers in the United States. In the management of our systems network, we may move data across jurisdictions and may store or process your information outside your home country. . By using any John Deere Data Services and Subscriptions you agree that we may process and store your data in the United States.

DELETING

Please note that John Deere may retain data unless you delete your information as described above. After expiration of any applicable Data Service and Subscription contract, we may delete data at our discretion and subject to requirements in any applicable privacy, consumer protection, or other laws.

1. COUNTRIES

This statement applies in the United States of America, Canada, Australia, New Zealand, Argentina, Bolivia, Brazil, Colombia, Paraguay, Uruguay, and South Africa. For other countries see www.JohnDeere.com/legal.

2. JOHN DEERE DATA SERVICES AND SUBCRIPTIONS

The terms of use for the John Deere Data Services and Subscriptions are available at www.JohnDeere.com/agreements.

3. JOHN DEERE PRIVACY STATEMENT

In providing the John Deere Data Services and Subscriptions, we may receive, collect, use, manage, analyze, segment, index, transmit, transfer, store and process personal information which can include

names, contact data (telephone number, e-mail, address), and in some cases usage data (including website and mobile app use). Our Privacy Policy is available at www.JohnDeere.com/legal.

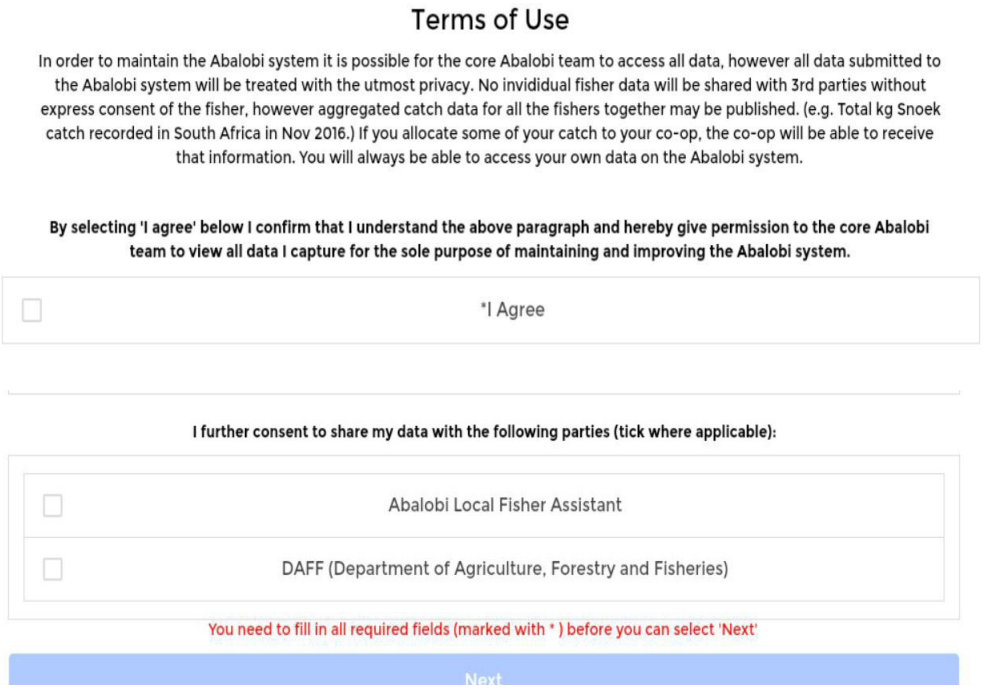
4. RESTRICTING DEALER ACCESS TO MACHINE DATA
To remove dealer access to Machine Data from machines in your account you must do both of the following: remove ServiceADVISOR Remote access for each machine from the Terminal Settings tab in the Operations Center and remove access to machine notifications and advisors from the Sharing tab on the JDLink portal.

5. DELETING, UPDATING, AMENDING MACHINE DATA, PRODUCTION DATA, AND ADMINISTRATIVE DATA
To request deletion, updates, or amendment of Machine Data, Production Data, or Administrative Data email jdlinksupport@JohnDeere.com, or call 800-251-9928. To understand how deletion may impact or terminate any John Deere Data Services or Subscriptions see www.JohnDeere.com/agreements. To understand your rights with respect to any personal information, see www.JohnDeere.com/legal.

6. MARKETING PREFERENCES Email PrivacyManager@JohnDeere.com for information about your marketing preferences or to change them.

7. ACCESS TO AFFILIATES
All references to "We" in this statement include Deere & Company and its subsidiaries. You may have granted John Deere Financial certain rights to access machine data about your equipment in your financing or lease documents, including the location, maintenance, operation and condition of your equipment. If permitted by your finance or lease agreement, John Deere Financial may continue to access machine data about your equipment during the term of the financing or lease agreement notwithstanding any election you may make. This could include reinstating machine data access if turned-off or otherwise disabled. Please review your finance or lease documents for more information.

Appendix B: Text of Abalobi data collection agreement [2]



Terms of Use

In order to maintain the Abalobi system it is possible for the core Abalobi team to access all data, however all data submitted to the Abalobi system will be treated with the utmost privacy. No invididual fisher data will be shared with 3rd parties without express consent of the fisher, however aggregated catch data for all the fishers together may be published. (e.g. Total kg Snoek catch recorded in South Africa in Nov 2016.) If you allocate some of your catch to your co-op, the co-op will be able to receive that information. You will always be able to access your own data on the Abalobi system.

By selecting 'I agree' below I confirm that I understand the above paragraph and hereby give permission to the core Abalobi team to view all data I capture for the sole purpose of maintaining and improving the Abalobi system.

☐ *I Agree

I further consent to share my data with the following parties (tick where applicable):

☐ Abalobi Local Fisher Assistant

☐ DAFF (Department of Agriculture, Forestry and Fisheries)

You need to fill in all required fields (marked with *) before you can select 'Next'

Next

2 Retrieved from a registration form linked to http://register.abalobi.org

Towards a Tiered or Differentiated Approach to Protection of Traditional Knowledge (TK) and Traditional Cultural Expressions (TCEs) in Relation to the Intellectual Property System

Chidi Oguamanam
Professor, Faculty of Law, University of Ottawa; Senior Fellow, Centre for International Governance Innovation (CIGI), Waterloo, ON, Canada; and Steering Committee Member, Open African Innovation Research (Open AIR) network
https://orcid.org/0000-0003-4301-9388

Abstract
The World Intellectual Property Organisation (WIPO) has, for nearly two decades, engaged in formulating the nature and content of a text-based legal instrument or instruments for the effective protection of genetic resources (GRs), traditional knowledge (TK), and traditional cultural expressions (TCEs, also known as folklore) within or relating to the international intellectual property (IP) system. This task has been the job of WIPO's Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore (IGC), established in 2000. In this article, I explore the context and rationales for, and evolution of, one of the IGC's evolving contributions: development of a tiered or differentiated approach to the protection of TK and TCEs. The article discusses and analyses the empirical ramifications and challenges of the tiered approach—alternatively referred to as differentiated approach—with reference to examples of forms of TK and TCE in Africa, North America and Australia. I conclude that the approach is a work in progress, still evolving, which provides a useful broad policy framework at the international level while, at the same time, its details are contingent on many considerations better addressed at national and local levels.

Keywords
Indigenous Peoples and local communities (IPLCs), genetic resources (GRs), traditional knowledge (TK), traditional cultural expressions (TCEs), tiered or differentiated approach, intellectual property (IP), World Intellectual Property Organisation (WIPO), Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore (IGC)

Acknowledgements
The author acknowledges funding support for this study provided by the Centre for International Governance Innovation (CIGI) through its International Law Research Program (ILRP). This article draws on content from the author's 2018 CIGI research paper (Oguamanam, 2018b). The author takes sole responsibility for any errors or omissions.

DOI: https://doi.org/10.23962/10539/27533

Recommended citation
Oguamanam, C. (2019). Towards a tiered or differentiated approach to protection of traditional knowledge (TK) and traditional cultural expressions (TCEs) in relation to the intellectual property system. *The African Journal of Information and Communication (AJIC), 23*, 1–24. https://doi.org/10.23962/10539/27533

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: https://creativecommons.org/licenses/by/4.0

1. Introduction

The World Intellectual Property Organisation's (WIPO's) Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge, and Traditional Cultural Expressions (hereafter the "IGC") has an extremely difficult mandate: to negotiate a text-based instrument or instruments for the effective protection of genetic resources (GRs), traditional knowledge (TK), and traditional cultural expressions (TCEs, i.e., folklore) within or relating to the intellectual property system (see WIPO, 2015).

WIPO's jurisdictional status as the host of the IGC is, in part, fallout from the World Trade Organisation's (WTO's) failure to include TK and TCEs in the text of its adjunct Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). Additionally, WIPO's jurisdiction in this area is a result of the increasing economic and trade importance of GRs, TK and TCEs. Given the longstanding involvement by UNESCO in TK and related matters including TCEs, the jurisdictional ambit of WIPO IGC is, arguably, confined to the *IP-related* ramifications of GRs, TK and TCEs, even though the protection of these subject matters inherently requires a sui generis approach. Consequently, WIPO Member States and experts are required to ensure and respect synergies between the IP-oriented and non-IP-oriented aspects of TK and TCEs as they feature in other regimes.

Enigmatic nature of TK and TCEs

The core difficulties of the IGC's task are coloured by, but not primarily a function of, the contentious nature of international IP policymaking processes, the international IP system's ubiquitous geopolitical power relations, and ideological schisms over knowledge governance (May & Sell, 2005; Oguamanam, 2012, p. 35; Raustiala, 2007). Additionally, the difficulties do not principally lie in the institutional dynamics of the WIPO's committee process or in the complex regime ecosystem in which TK and TCEs are engaged (Helfer, 2004; Oguamanam, 2007; Yu, 2007). Without question,

those factors contribute to making the IGC mandate a Herculean task.[1] But the most critical difficulties at the heart of the IGC project is the enigmatic nature of TK and, to an even greater extent, TCEs. TCEs have been, and remain, a unified or inherent component of TK. But at WIPO and other forums, attempts have been made to isolate TCEs from TK, in conceptual terms, with TCEs approached as being separate from TK. Regardless, in such contexts, both TK and TCEs are pragmatic, and thus generalised, terms of convenience and compromise—generalised, but yet not able to capture the full breadth of the complexities of (1) relationships and nuances implicated in the experiences of the custodians of TK and TCEs, and (2) the custodians' undergirding worldviews as mediated by their knowledge systems.

The interfaces between TK and innovations in the realms of pharmaceuticals, cosmetics, agriculture, chemicals and environmental conservation, which constitute the core of the "biopiracy" phenomenon, provide pivotal sites in which IP, specifically the patent regime, directly engages TK in contestation over the applications of GRs across different knowledge frameworks. Notwithstanding these examples, the interfaces between IP and TK/TCEs generally tend to be difficult to pin down. In the patent regime, "newness" of TK, analogous to an invention, is a consistently problematic issue (Mgbeoji, 2001). In the area of copyrights, fixation and publication, especially of TCEs, are perennial hurdles (Boateng, 2011; Kuruk, 1999). In respect of trademarks and designs, claims of sacredness—as a basis of exclusion of certain marks, symbols, insignias, or designs from commercial exploitation—remain a source of tension amongst stakeholders (Coombe, 1998a).

Competing interests in the IGC

For many longtime participants in the IGC, from both developed and developing countries, the lingering delay to reach agreement on anticipated text or texts, after nearly 20 years of work, is disappointing (see Oguamanam, 2017). This disillusionment is especially the case for many Global Southern countries and experts, and for Indigenous Peoples and local communities (IPLCs) from both the Global South and Global North.

However, for many Global Northern WIPO Member States, and for experts from these countries, the IGC's protracted delays are not necessarily seen as disadvantageous (Oguamanam, 2017). Most countries of the Global North, often called non-*demandeur* countries, participate in IGC negotiations with little or no vested interest in achievement of a codified international legal instrument or instruments for the protection of GRs, TK and TCEs. It was, of course, intemperate appropriation of GRs and associated TK (and even TCEs) by corporate and research entities based in

1 See the Robinson, Abdel-Latif and Roffe (2017) volume for examination of the first decade and a half of the work of the IGC.

the Global North[2] (i.e., biopiracy) (see Mgbeoji, 2006; Robinson, 2010)—facilitated largely through the international IP regime, especially the patent system—that, in part, necessitated the establishment of the IGC. Accordingly, countries of the Global North, save for a few, are reluctant participants in the IGC process;[3] for them, the status quo is desirable (Oguamanam, 2017).

Key negotiating blocs at the IGC who are invested in ensuring that the IGC results in an effective international instrument or instruments pursuant to its mandate, and who thus constitute the *demandeurs,* are the African Group, the Group of Latin American and Caribbean Countries (GRULAC), and the Asia-Pacific Group (APG). All of the aforementioned liaise, consult, and/or coalesce, as the need arises, under the auspices of the IGC's Like-Minded Countries (LMCs) group. Another key bloc in the *demandeur* category is the Indigenous Caucus, which is a coalition of accredited Indigenous Peoples' delegations to IGC who cut across geopolitical boundaries.

The study

The study on which this article is based explored development, in the IGC, of the *tiered approach*—also referred to as the *differentiated approach*—to the protection of TK and TCEs pursuant to the IGC's mandate. It is an approach which is subject to ongoing debate and continuing elaborations at the IGC.[4] (While the mandate of the IGC is to negotiate a text-based instrument or instruments for effective protection of three (often overlapping) sets of phenomena—GRs, TK, and TCEs—the tiered or differentiated approach relates to only two of the phenomena: TK and TCEs—which, it must at the same time be noted, are sites in which IPLCs often deploy GRs.)

In the study, I explored the rationale for the tiered or differentiated approach, and drew on examples from three sites of TK/TCE production—sites in Africa (Ghana), Australia, and North America (US and Canada)—in order to interrogate the approach and its potential and practical applications. The study ultimately found that the tiered or differentiated approach can potentially serve as a useful abroad policy framework operating at international level, but with the details of its operation contingent on considerations at national and local levels, including but not limited to: the specific manifestation of TK or TCE; the dynamics of IPLC customary laws and protocols

2 Often in collaboration with researchers and institutions linked to the Global South, e.g., as was the case in the failed US patent on turmeric (initially granted to WR Grace Inc.), in which US-based Indian researchers were instrumental. See Bala (2011).

3 For some of these countries, their participation takes on a vigilante tenor, which focuses on ensuring that the resulting instrument of instruments does/do not constrain or disrupt the status quo on international IP, especially the patent regime.

4 For an outline of the text of the tiered or differentiated approach to TK, see WIPO (2016b).

in regard to custody, production, and practices in relation to the manifestation of TK or TCE; and the evidentiary threshold in respect of determining the level of diffusion of a specific manifestation of TK or TCE.

2. Marginalisation of TK and TCEs from the Conventional IP system

Colonial narratives

The industrialised colonial powers showed no inclination to facilitate IPLC protection of TK and TCEs, as evidenced in narratives of colonialism deploying lenses of, among others, science, anthropology, philosophy and critical social sciences (De Sousa Santos, 2007; Oguamanam, 2015). The consensus across these renditions was that, in contrast to the "innovative cultures" of Western (or European) societies (Arewa, 2004; De Sousa Santos, 2007; Memmi, 1990; Mutua, 2011), IPLCs and non-Western societies—positioned as the West's "Other"—were lacking in meaningful innovation (see De Beer, Oguamanam, & Schonwetter, 2014; De Sousa Santos, 2007; Oguamanam, 2008). These IPLCs and non-Western civilisations were recognised as having substantial endowments of natural resources,[5] but their dealings with those resources were cast as being mundane and rudimentary, and thus incapable of transforming natural endowments from their so-called "state of nature". Accordingly, the insights, knowledge, and practices of IPLCs and non-Western societies, as applied to natural resources—in, for example, agriculture, medicine, ecology, and environmental stewardship—were adjudged to be lacking the human ingenuity and other criteria necessary for their protection under orthodox, Western-originated IP systems (Oguamanam, 2015).

"Public domain" assertions

Coupled with this denigration of the intellectual value of IPLCs' TK and TCEs—amidst compelling evidence to the contrary[6]—were, and are, assertions from rich, industrialised nations that many of the GRs and indeed broader biological resources

5 It is estimated that over 75% of global biological resources are found in the Global South and/or in traditional or ancestral habitats utilised by IPLCs. See, for example, Oguamanam (2012).

6 The first symmetric stone tools were invented in Africa. Africa is recognised as the "nest of many discoveries, inventions, creations and cultures" that have since catapulted human civilisations across the globe. In medicines, sciences, and all facets of arts and creativity, African innovations serve as the forerunner of most revolutionary inventions and ideas that have shaped the trajectory of human civilisation. Hero of Alexandria, Egypt invented the first documented steam engine in the 1st century AD. See Elahi and De Beer (2013). Yet, in the colonial worldview, "[h]istorically, Africa is not part of the world; it cannot show evidence of any movement or development. The historic movements it displays—on the Northern region of the continent—belong to the Asian and European world" (Hegel, 1970, quoted by De Sousa Santos, Nunes, and Meneses (2007, p. xxxv)). This narrative or situating of Africa "was the counterpoint of the colonial requirement of transporting civilization and wisdom to peoples who lived in the dark recess of ignorance" (De Sousa Santos et al., 2007, p. xxxv).

that constitute the pivot for the production of TK, and even TCEs, should be regarded as part of a global "public domain" or "commons". In the words of Okediji (2018):

> Armed with legal tools, such as "the common heritage of mankind" and "the public domain", scientists and international institutions facilitated the development of a global knowledge infrastructure for research and innovation, utilizing plant GRs and traditional knowledge. International regimes for science and research coalesced around the view that those resources were part of an uncharted global commons that could – indeed should – be freely and methodically exploited. (Okediji, 2018, pp. 3-4)

Such "public domain", "commons" and "common heritage" constructs, when applied to TK and TCEs, assail attempts to protect TK and TCEs within or in relation to the conventional IP paradigm.

The perspectives of IPLCs

IPLC custodians of TK and TCEs do not accept the narratives casting their knowledge and practices as lacking in human ingenuity (see Anaya, 2004: De Sousa Santos, 2007). And while TK and TCE custodians and practitioners recognise the importance of a vibrant public domain as a fundamental feature of sustainable knowledge production under the orthodox IP system, their perspective on the public domain is grounded in recognition that several centuries of delegitimation and exploitation have been the primary drivers of their TK and TCEs becoming publicly available and cast as global public goods (Oguamanam, 2018b).[7]

A central matter that has emerged at the IGC is the need to determine the context in which, and/or the degree to which, a given TK or TCE is diffused, or is publicly available such that it constitutes a part of the public domain (or an approximation of the public domain). The need to find ways to make such assessments, which will have to be done on a case-by-case basis, has led to development of the tiered or differentiated approach.

3. Emergence of the tiered or differentiated approach to TK and TCEs

27th Session of the IGC, March-April 2014

At the IGC's 27th Session in Geneva in late March and early April 2014, concerted initiatives by the LMCs group (including the African Group), led to formal documenting of the idea of a tiered or differentiated approach to TK and TCEs (Okediji, 2017). The idea had been explored before the 27th Session, in early March

7 For progressive conceptualisations of knowledge as a global public good, see Stiglitz (1999) and Maskus and Reichmann (2005).

2014, by an LMC Consultative Meeting in Bali.[8] At the Bali meeting, the Chair, Ambassador Wayne McCook of Jamaica, had leveraged "the treatment of publicly available and/or widely diffused TK and TCEs" into becoming a key cross-cutting issue for examination of TK and TCEs (McCook, 2014b). McCook then elaborated the issue further in a 51-page "Chair's Non-paper" (McCook, 2014a), helping prompt the deliberations at the IGC's 27th Session (see WIPO, 2014a). Speaking on behalf of the facilitators of the 27th Session, Nicolas Lesieur (Canada) noted that they

> [...] had sought to construct a tier-based framework that was itself based on the extent to which the TK was diffused and/or protected by beneficiaries, or not, such that there were different levels of diffusion and protection. (WIPO, 2014a, para. 95)

Accordingly, the concept was articulated in Article 3 of the Draft IGC documents on TK and TCEs that were prepared for the 27th Session (WIPO, 2014b; 2014c).

Aims and characteristics of the approach

The primary aim of the tiered or differentiated approach is to advance legal certainty and clarity on TK and TCEs in order to allay concerns raised by non-*demandeur* countries and experts, mainly of the Global North, in the IGC negotiations. The approach provides a framework for delineating different kinds of TK and TCEs based on their degrees of diffusion, or lack thereof. It then seeks to determine the extent of exclusive rights or partially exclusive rights that the TK and TCE custodians could receive, based on how much of the TK or TCE in question, or aspects thereof, is/are diffused or publicly available, as the case may be. The approach is pragmatic and malleable.

While there is not yet a consensual understanding of the approach across IGC delegates, there is wide acceptance of the idea that the approach would *not* countenance use, or continued use, of any TK or TCE without permission and accountability. Essentially, the approach recognises that some TK and TCEs are already publicly available or diffused, albeit by default through various forms of diffusion and appropriation, some legitimate some not (Oguamanam, 2018a; Okediji, 2017). As such, according to the approach, where the TK or TCE is already in the public domain or publicly available, there should not be *ex post facto* attempts, especially in regard to the former situation, to force the genie inside the bottle, i.e., to take the TK or TCE out of the public

8 For more detailed insight, see the official report of the IGC's 27th Session (WIPO, 2014a). In addition to the 2014 Bali LMCs Consultative Meeting, the history of the idea of a differentiated approach to TK is not complete without reference to the international consultative meeting of experts organised by the Government of India in New Delhi in January 2013, and India's interventions at the IGC's 27th Session.

domain and provide exclusive IP rights or related rights to its custodians.[9] (Such attempts would scare hardline, and even moderate, non-*demandeur* countries and experts, justifiably or not.) But, at the same time, the approach holds that such TK or TCEs *could* attract other residual or calibrated rights, such as various forms of attribution rights and even reparation rights, or other remedial rights, especially for TK or TCEs that were diffused through theft and other forms of misappropriation where there was no free prior and informed consent of IPLCs.

It needs to be noted that the term "public domain" is a concept and expression particular to conventional IP. Pursuant to IP, information or knowledge in the public domain is free for use by all, and not subject of protection. However, "public domain" is *not* a synonym for "publicly available". The fact that a form of knowledge or information, including TK, TCEs or uses of GRs, is publicly available does not necessarily mean that such knowledge or information has the status of being in the public domain. It is, accordingly, critical to interrogate the process or terms by which it became publicly available.

IGC stakeholder views on the approach

The African Group, India, Indonesia, and the LMCs as a whole seem to share an understanding that the tiered or differentiated approach has the potential to assist with protection of TK and TCEs—in the variegated contexts of their diffusion and in ways that will guard against use of public domain arguments to undermine protection.

The EU, the United States, Japan, South Korea and Canada are engaging the approach with apprehension. Collectively, they have expressed concern over its potential effect on a range of issues, such as the "existing freedoms and the public domain" (WIPO 2014a, para. 53 [EU]), "innovation and creativity" (para. 41, [Japan]); and "inspiration" (para. 194, [Canada]). For countries within this category, terms such as "sacred", "secret", "widely diffused", and "publicly available"—terms which are associated with the tiered or differentiated approach—are, in the words of the Canadian position, "problematic from a certainty and clarity perspective" (para. 163), or, in the view of the EU, "open to further exploration" (para. 167) and "open to interpretation" (para. 108). According to the US delegation, "publicly available and widely diffused TK and TCEs [do] not lend themselves to protection by exclusive rights" (WIPO, 2014a, para. 62). Canada's position is that "subject matter that was currently publicly available and that was not or was no longer protected

9 But consider the famous retort by Preston Hardison, a prominent member of the Indigenous Caucus at the IGC and official representative of the Tulalip Tribes of Washington State, who insists, analogously, that because Lady Gaga's music is widely diffused does not mean that she or her assigns should forgo their copyrights. Hardison rejects the genie-out-of-the-bottle argument if its objective is to facilitate appropriation of TK/TCE (see Hardison, 2016).

by an intellectual property right (IPR) should not be protected" (para. 52) under IGC instruments. South Korea's view is that publicly-available, widely-diffused TK belongs to the public, and that retroactive protection would generate an unacceptable public cost (WIPO, 2014a, para. 78).

For its part, the IGC's Indigenous Caucus has adopted a reserved (and, in my view, prudent) attitude towards the tiered or differentiated approach, insisting that irrespective of the level of diffusion, whenever TK or a TCE is erroneously placed in the public domain, or is erroneously made publicly available, Indigenous Peoples' status as rights holders, and their entitlement to compensation or other appropriate remedies, should not be compromised. For the Indigenous Caucus, recognising the sacred nature of all TK and TCEs, not the level of diffusion, should be the starting point.

4. Evolution of the tiered or differentiated approach

The tiered or differentiated approach has evolved since its introduction in 2014. Initially, the approach identified five categories of TK and TCE, namely: (1) secret; (2) sacred; (3) closely held; (4) narrowly or partially diffused; and (5) widely diffused. However, these categories defy clear delineation, particularly in respect of:

- secrecy and sacredness of TK and TCEs; and
- diffusion.

Complexities of "secrecy" and "sacredness"

While secrecy is a feature of the sacredness of TK and TCEs, sacred aspects of TK and TCEs are sometimes conveyed in contexts where they are not taken as secret; and, vice versa. Secret aspects are sometimes conveyed in contexts where they are not perceived as sacred. This is so because of the fusion of intangible and tangible elements within tangible TK/TCE manifestations—as is seen in the example of bark paintings that is presented in the next section of this article.

Complexities of the notion of "diffusion"

A closely held, or narrowly or partially diffused, manifestation of TK or a TCE will require some evidentiary threshold regarding permissible level of diffusion—to eligible or ineligible "publics"—in terms of customary laws and protocols pertaining to the particular TK/TCE form. Also, there can be instances where even though a manifestation of TK or a TCE may be secret and sacred, it is also narrowly or partially diffused, or even widely diffused.

An important consideration is the fact that the degree of "diffusion" is not always a function of "publicness"—which is to say, diffusion is not necessarily a function of exposure or accessibility of the TK or TCE to members of the public, i.e., not necessarily a function of whether or not it is "in the public domain" or "publicly

available", as per the terms used in the discussion above.[10] Diffusion incorporates other factors and considerations. As stated in Oguamanam (2016), "[b]eyond being a matter of how 'well-known' as a feature of geographical application [or dispersal] and uptake, diffusion is perhaps a referential concept to what actually is known or legitimately disclosed in a specific TK context", making it possible for there to be "a widely or partially diffused TK that remains sacred and/or secret" (2016, p. 10). This observation is also true for TCEs. Also, the notion of diffusion can be logically scaled to include the extent to which a specific form of TK/TCE interacts with, influences, and/or is influenced by, other knowledge, innovations, and practices that are not strictly recognised as TK or a TCE.[11] The concept of diffusion is not linear or presumptive. It involves articulation of the full scope of uses or applications of a TK and TCE, including the scope of its migration to, or transmission in, other knowledge contexts, as well as the range of its geographical uptakes or dispersals. This conception of diffusion, which is not reliant on publicness, is not mutually exclusive in respect of the conception grounded in publicness.

IGC deliberations seem to have not yet engaged with the full range of perspectives on the concept of diffusion—an illustration of the fact that the tiered or differentiated approach is still in its incubating stage. As the approach evolves, it can be expected that IGC stakeholders will adopt increasingly workable treatments of the realities of diffusion of TK and TCEs. One sign of increased engagement is the apparent move within the IGC towards four, and possibly even three—rather than the original conception of five—tiered categories.

Crystallisation of four tiered categories

While the IGC's tiered or differentiated approach to TK and TCEs remains a fluid concept, it currently appears to be crystallising around four overlapping (i.e., not mutually exclusive) categories,[12] as illustrated in Figure 1 below:

- secret;
- sacred;
- narrowly diffused; and
- widely diffused.

10 It is noted that not all IPs are susceptible to the public domain counterpoise. For example, trade secrets remain exclusive property of the owner in perpetuity unless it status is compromised.

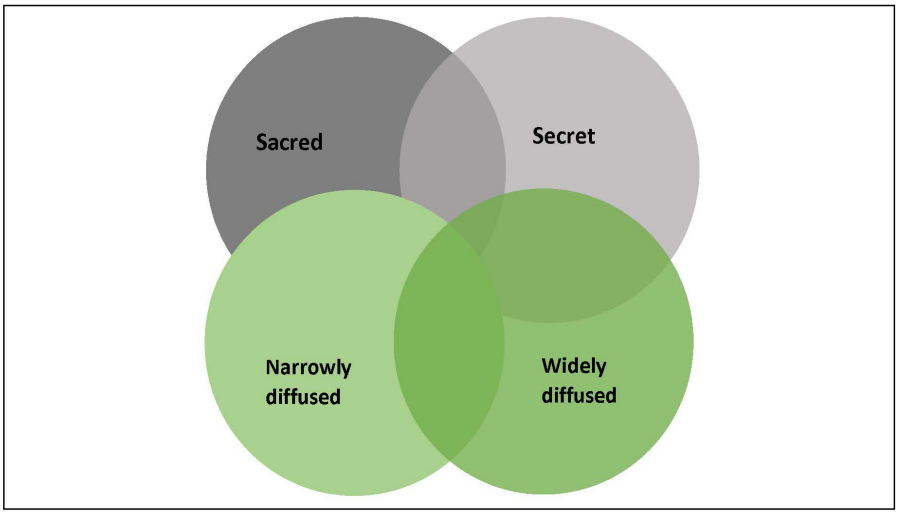
11 This is consistent with the view in anthropological circles that there is no knowledge that exists in isolation. And since knowledge is dynamic, that dynamism entails interaction across various knowledge systems as part of the process of knowledge creolisation and evolution. See Brown (1998).

12 The four-category framework dispenses with the "closely held" category, a highly vague concept. Arguably, however, the concept is captured under the "partially or narrowly diffused" category.

Central premises of this move towards four categories are that:

- strong or exclusive rights should attach to secret and sacred TK and TCEs; and
- weaker forms of rights should attach to narrowly diffused and widely diffused TK and TCEs, since they are presumably available publicly, and some could also be said to be in the public domain.[13]

Figure 1: Four-category version of tiered or differentiated approach to TK and TCEs



The four-category version of the tiered or differentiated approach, as shown in Figure 1, seeks to provide pragmatic recognition of the question of diffusion of TK and TCEs, while at the same time allowing IPLCs to make rights claims, the details of which can be customised according to the specific instance of TK or TCE and the corresponding IPLC's legal traditions and particular national context.

In the draft text on the tiered or differentiated approach, as it appeared in the Draft Articles on the protection of TK prepared for the IGC's 34th Session in 2017, the

13 There is need for a caveat here. One must not conflate the concept and ramifications of diffusion in the tiered and differentiated elaboration from other contexts. Wide diffusion is not an excuse for abandonment of rights given that the process through which a specific TK/TCE becomes widely diffused may be illegitimate as in cases of piracy or biopiracy. Therefore, to insist that wide diffusion puts TK in public domain border line with consequential weakening of rights is to reward abuses of TK through illegitimate acts of diffusion.

wording of alternative 2 ("Alt 2") under Article 5 entitled "Scope of [and Conditions of] Protection", was as follows:

> Alt 2
> Member States [should/shall] safeguard the economic and moral interests of the beneficiaries concerning traditional knowledge as defined in this instrument, as appropriate and in accordance with national law, in a reasonable and balanced manner, and in a manner consistent with Article 14, in particular:
>
> (a) Where the traditional knowledge is **secret**, whether or not it is sacred, Member States [should/shall] take legislative, administrative and/or policy measures, as appropriate, with the aim of ensuring that:
>
> i. Beneficiaries have the **exclusive and collective right** to maintain, control, use, develop, authorize or prevent access to and use/utilization of their traditional knowledge; and receive a fair and equitable share of benefits arising from its use.
>
> ii. Beneficiaries have the **moral right of attribution** and the right to the use of their traditional knowledge in a manner that respects the integrity of such traditional knowledge.
>
> (b) Where the traditional knowledge is **narrowly diffused**, whether or not it is sacred, Member States [should/shall] take legislative, administrative and/or policy measures, as appropriate, with the aim of ensuring that:
>
> i. Beneficiaries receive a **fair and equitable share of benefits** arising from its use; and
>
> ii. Beneficiaries have the **moral right** of attribution and the right to the use of their traditional knowledge in a manner that respects the integrity of such traditional knowledge.
>
> (c) Where the traditional knowledge is not protected under paragraphs (a) or (b), Member States [should/shall] use best endeavors to protect the integrity of traditional knowledge, in consultation with beneficiaries where applicable. (WIPO, 2017a, **boldfacing** of text added by author)

The IGC's 2017 Draft Articles on the protection of TCEs contained analogous (though more elaborate) provisions, appearing as alternative 3, option 1, of Article 5 entitled "Scope of [Protection]/[Safeguarding]" (WIPO, 2017b).

The renewed IGC mandate for the 2018-2019 biennium, which began in March 2018, provided opportunities for further debate on and elaboration of the tiered or differentiated approach as a work in progress. The March 2019 revisions of the Draft Articles on TK and TCEs (revisions yet to be officially adopted at the time of finalisation of this article) further reviewed the concept of the tiered or differentiated approach as a work in progress. By the time that the IGC's 2018-2019 biennium

draws to an end in June 2019, the tiered or differentiated approach will have evolved further, and, subject to the renewal of the IGC mandate by the WIPO General Assembly, exploration of the approach can be expected to morph onto the next biennium.[14]

5. Examples relevant to a tiered or differentiated approach

Kente fabrics and designs in Ghana

Ghana's kente fabrics and designs (Boateng, 2011) have over 4,000 years of history. Kente is largely linked with the pre-contact Akan people of the Asante (or Ashanti) Kingdom of West Africa, which once spread across territory that included not only parts of contemporary Ghana (Konadu, 2007) but also parts of today's countries of Côte D'Ivoire, Mali, Benin, Togo, Burkina Faso and Liberia. Originally, kente designs were associated mostly with Asante royalty, i.e., with the Asantehene (the spiritual ruler of the Asante Kingdom). Every design has a culturally rooted meaning and symbolism that depicts the Asante worldview, its rich creative imageries, its ethics of sacredness, and overall rich cultural heritage. As explained by Boateng (2011),

> [T]he motifs used in Asante kente cloth weaving have specific names; however, the cloth is usually named for the colors and design of the background, which is often striped. As with Adinkara, kente is named for historic figures and events and also for Asante values. The design kyeretwie, or leopard, or leopard catcher, for example, symbolises courage, while aberewa ben, or "wise old woman," indicates the respect accorded older women in Asante society. Another design is named Oyokoman named for the Oyoko clan. One especially rich and prestigious version of these and other designs is called adweneasa or adwenasa, a name that refers to the weaver's skills. (Boateng, 2011, p. 23)

Kente has followed plural pathways of diffusion.[15] The current reality of kente's diffusion is that it is no longer exclusive to Asante royalty. Rather, kente fabric is now available to whoever can afford it, among the Asante, in Ghana as a whole, among other Africans, and indeed, globally. Yet it is, in part, because of this global diffusion, rather than despite it, that kente remains, unquestionably, a symbol of both pre-colonial Asante identity and post-colonial Ghana's national character. Another aspect of kente's diffusion relates to transformation of its processes of production. Earlier kente fabrics were made of GRs, specifically straws from species of bamboo and raffia endemic to regions within the Asante Kingdom (Schneider, 1987). Today, kente fabrics are typically made of silk or cotton, or even industrial synthetic

14 The 40th Session of the IGC, which was held June 17–21 2019, produced the latest modified texts of the tiered or differentiated approach to TK/TCEs, which will be used for continuing negotiation over the 2021-2021 biennium.

15 They include Asante/Akan (central Ghana); Gonja (northern Ghana); and Ewe (southeastern Ghana).

materials of varying quality, including rayon. And kente designs can, today, be found in broadloom cloth,[16] in various forms of clothing and fashion accessories, and even in non-textile items such as stationary, i.e., in products falling outside kente's original and historic limitations and applications. But those uses do not extend beyond kente's characteristics as a tangible piece of creative work. To the "uninitiated", the uses do not include kente's intangible elements and symbolisms which remain exclusively relevant to the Asante.

Aboriginal bark-painting in Arnhem, Australia

Aboriginal bark paintings in Arnhem, Australia, are a fusion of the sacred, the intangible, and the tangible, in a manner that engages plural layers of diffusion. The paintings are associated with the Aboriginal peoples of the Arnhem region of Australia's Northern Territory. Case law has recognised bark paintings as creative works that are associated with sacred dreaming images and the creation stories of exclusive cultural communities (see the 1994 decision in Australia's *Milpurrurru v Indofurn Pty Ltd* case). Aboriginal bark artists operate within an exclusive cultural environment. Their work is based on and inspired by collectively-held traditional and sacred cultural heritage, the secret aspects of which are only known to a limited number of members of a specific clan.

When deploying or working with those elements of collectively-held cultural heritage, the artists effectively act as fiduciaries or cultural agents, playing intermediary roles between members of their communities and outsiders in respect of the terms of use, or access to, their scared paintings (see *Milpurrurru v Indofurn Pty Ltd* [1994]). Yet despite the deeply embedded sacred cultural symbols, rituals, and other forms of intangibility associated with bark paintings, they have gradually become quintessential, highly tangible public works of Aboriginal art, serving as integral aspects of Australia's national identity and brand. Aboriginal bark-painting images are present in Australia in ubiquitous adaptations in designs for, inter alia, postage stamps, calendars, tourist information, certified documentations in the Australian National Gallery, and the folio of Aboriginal art published by the Australian Information Service (see *Milpurrurru v Indofurn Pty Ltd* [1994], and Blakeney, 1995). Unequivocally, bark paintings are widely diffused as the proud symbol of Australia's national heritage premised on its sacred and rich Indigenous historiography and origins. Those sacred aspects associated with bark paintings as Indigenous heritage constitute aspects of their intangible essence and associated meaning-making that inalienably and residually link them to their Indigenous creators.

Cowichan weaving in North America

Cowichan weaving, practised by the Cowichan grouping of Coast Salish Indigenous Peoples in North America's Pacific Northwest (the province of British Columbia

16 For insight on the technological diffusion of kente production, see Boateng (2011, pp. 27-30).

in Canada, and Washington State in the US), is another example of TK/TCE with multiple layers of diffusion and variegated degrees of sacredness or symbolism.

According to Stopp (2012), Cowichan weaving involves the primordial skill of being able to transform plant and animal fibre materials into woven textiles products. The pre-colonial Coast Salish bred special dogs for their hair as a core GR used in weaving blankets and other functional items for protection against harsh weather conditions. Over time, following colonial encounter, other materials such as sheep wools and synthetic fibres were, and still are, used in Cowichan weaving. As well, the weaving practice has been extended and adapted in order to make sweaters, a European-origin article of clothing which, before colonial encounter, was not part of Aboriginal dress in the European form and design. Yet weaving remains a pivotal aspect of the customary laws and practices and the heritage of the Coast Salish. Similar to kente's global diffusion, the Cowichan sweater still retains its historical and cultural symbolisms even as it serves as an internationally-consumed product that provides an anchoring point for the Cowichan people's participation in the global economy (Stopp, 2012). Among other things, the symbolic aspects of Cowichan sweaters designate the intricate nature of relationships and dependencies across life forms, art and creativity as a mirror of their intangible essence in Coast Salish experience. Cowichan sweaters were prominent in Canada's showcasing during the 2010 Winter Olympics in Vancouver,[17] and are marketed globally as "warm, weatherproof, sturdy, serviceable, durable for outdoor pursuits [and] one of the world's most distinctive sweater types" (Stopp, 2012, p. 82).

6. Analysis and conclusions

Secrecy, sacredness, diffusion, and the public domain

Across the three examples outlined above, different degrees of secrecy and sacredness can be identified. Available evidence demonstrates that the Aboriginal bark paintings in Arnhem, Australia, are considered sacred, even up to the present time. Kente fabrics and designs, meanwhile, were once considered highly sacred but, over time, have had their sacredness somewhat diluted. As with bark paintings, the sacredness of kente, and the symbolisms of the designs, are sites of complex meaning-making that most easily resonate among the initiated within an exclusive cultural core.

As products and processes, the rituals and symbolisms associated with Aboriginal bark-painting and kente fabrics/designs largely designate their intangible aspects, which are outside the consciousness of the members of the public who acquire them

17 See Scassa (2015), who argues that appropriation of Indigenous cultural heritage, as exemplified by (1) a UK designer's copying of an Inuit shaman's robe and (2) Canadian retailer the Hudson's Bay Company's (HBC's) procurement of non-Cowichan-made versions of Cowichan sweaters for sale during the Vancouver Winter Olympics unravels "the disconnect between IP laws and indigenous cultural property".

only as products. The interest of non-Aboriginal or non-Indigenous patrons of bark paintings and kente lies in the products' physical (tangible) qualities.[18] In such contexts, there is little regard for the products' spiritual and other intrinsic cultural ramifications (i.e., the intangible components).[19] With regard to Cowichan weaving in North America, the intangible aspects of its culturally-rooted spirituality and symbolism rarely take prominence.

In respect of diffusion, the three examples provided above demonstrate that:

- it is possible to have sacred and/or secret forms of TK or TCE that are narrowly diffused, or—even more important for the present analysis—widely diffused; and
- diffusion is not exclusively determined by geographic dispersal or public accessibility. For example, kente designs and bark arts are now manifested in non-traditional applications, such as in stationary and/or in other sites (e.g., postage stamps, tourist ornaments, and miscellaneous accessories) where their aesthetic appeals are leveraged to create non-traditional products.

In respect of the public domain or public availability, the three examples show that:

- the less a form of TK/TCE retains its spiritual and cultural claims, the more it is likely to resonate with claims to the public domain (and consequently also resonate with weaker rights claims, or weaker claims of control, by its custodians); and
- in order to fully grapple with the notion of a tiered or differentiated approach, it is important to be conscious of the interwoven nature of the tangible and the intangible in TK and TCEs, and to be conscious of how each element changes our understanding of the public domain. For example, a form of TK or TCE may be publicly available, and may even be said to be in the public domain, while at the same time its sacred and intangible components are neither publicly available nor in the public domain.

Interfaces between GRs and TK/TCEs

Each of the three examples demonstrates that the association of GRs with TK and TCEs is not limited to the uses of GRs in the typical contexts of traditional medicine and agriculture (with corresponding associations with biodiversity and

18 The global dispersal and replication of kente on an industrialised scale via production in China demonstrates the commercial usurpation and appropriation of kente that de-links it from its cultural essence. The same has been found to be true in a number of litigations in Australia around bark paintings. Notably, in the *Milpurrurru* case, non-Aboriginal Australian businesspeople commissioned a Vietnamese company to manufacture carpets using designs from bark paintings (by eight highly regarded Aboriginal artists), with the carpets imported, distributed and marketed in Australia without regard to the sacredness of the bark paintings from which they were adapted. See *Milpurrurru v Indofurn Pty Ltd* [1994].

19 See *Milpurrurru v Indofurn Pty Ltd* [1994].

environmental conservation). Rather, the interfaces between GRs and TK and TCEs also encompass other sites of traditional creativity grounded in creative art forms,[20] as evidenced by the kente-weaving and the bark-painting, both of which depend in a primary manner on GRs.

Evidentiary threshold

Determining the status of a specific manifestation of TK or TCE in relation to each, or more than one, of the four differentiated categories listed above will be contingent upon the evidentiary threshold of the TK/TCE's diffusion or lack thereof. If the tiered or differentiated approach is to attain its objective of enhancing clarity, much will depend on deployment of the evidentiary threshold across each of the four categories of differentiation—secrecy, sacredness, narrow diffusion, wide diffusion—and across the areas of overlap among these four categories. Whether, and to what extent, a form of TK or TCE is secret, sacred, partially diffused, or widely diffused, will always be context- and subject-specific inquiries: *context-specific* with respect to the IPLC custodians or owners of the TK/TCE, and with respect to the relevant IPLC's customary laws and protocols, and *subject-specific* with respect to the type of TK/TCE at issue. It will also need to be acknowledged that context and subject can mutually interact. Moreover, in addition to documentation of the experiences of the relevant IPLC(s), documentation of the experiences of external users of the TK and TCE will be important, as an evidentiary matter, to establishing the extent of diffusion or lack thereof.

Role of IPLCs

Establishment of a credible evidentiary threshold with regard to diffusion for a particular manifestation of TK or TCE will require nuanced and sophisticated understanding of the details of the nature of the knowledge and of the layers of relationships implicated—as well as understanding of the nature and boundaries of roles assigned to stakeholders in the specific cultural context. These forms of evidence-gathering cannot be legislated at global level in a forum such as the IGC, nor even at national levels. IPLCs are the only credible custodians of their TK and TCEs, which are aspects of their self-determination and sovereignty (Coombe, 1998b; Hardison, 2016; Oguamanam, 2014).

IPLC representation at the IGC is sub-optimal and constrained.[21] And even if IPLCs were to be adequately represented at the IGC, the forum could not presume to have

20 Kente, Aboriginal bark-painting, and Cowichan weaving demonstrate the overlap of TK and TCEs with GRs and their interface with IP regimes such as copyrights, designs and trademarks—providing counterpoints to the tendency to focus GR discussions exclusively on the patent regime, i.e., the tendency to imply that efforts at patenting of innovation in life sciences (biotechnology, agriculture, chemicals, medicines, etc.) are the only sites where IP is implicated in GRs and associated TK.

21 This issue of IPLC participation in IGC deliberations has been problematic from the beginning, owing to the fact that its delegation relies on voluntary funding support from Member States. See WIPO (n.d.b).

full legitimacy in respect of detailing practical and evidentiary issues necessary to make determinations on the tiered or differentiated status of a specific manifestation of TK or TCE (see Anaya, 2016; Hardison, 2016). TK and TCEs are inherently dynamic and responsive (Posey & Dutfield, 1996), and the same is true of the undergirding customary laws, protocols, and practices of the IPLCs linked to manifestations of TK and TCEs. In formulating the details of operationalisation of the tiered or differentiated approach in national contexts, constituent IPLCs will need to provide the pathways for how their customary laws and protocols are engaged.

IGC views on roles of IPLCs as beneficiaries

The IGC's Indigenous Caucus, most non-*demandeur* members and experts, and some of the members of the LMCs group, have made it clear that they see IPLCs as the primary beneficiaries of IP protection TK and TCEs.[22] However, the African Group, and the majority of members of the LMCs group, are insisting that national governments/states are *also* legitimate beneficiaries of the protection of TK/TCEs—or, put more technically, that they are legitimate beneficiaries of any instrument(s) resulting from the IGC.

As such, Member States will need to be proactive in the IGC in formulating requisite operational details of the tiered or differentiated approach. The nature of the relationship between national governments and IPLCs is largely a factor of colonial relations (Anaya, 2004). In colonial states—for example, Canada, the US, Australia, New Zealand, and elsewhere where the settler did not withdraw—such relationships disentitle states from any claims to ownership of, or assumption of beneficiary status in relation to, TK and TCEs vis-à-vis Indigenous Peoples. The same cannot not be said with any degree of definitiveness in many postcolonial states in Africa and elsewhere in the Global South where Indigenous Peoples and various categories of IPLCs today constitute the dominant cultures and societies (Coombe, 1998b). Regardless of the nature of each national government's relation to Indigenous Peoples—and, by extension, to manifestations of TK and TCE—it is undeniable that the customary protocols and practices of IPLCs will be crucial in implementing the tiered or differentiated approach at both national and sub-national levels.

22 Article 4, alternative 1, in The Protection of Traditional Knowledge: Draft Articles, drafted for the IGC's 37th Session, provides as follows: "Beneficiaries of this instrument are indigenous [peoples] and local communities who hold [protected] traditional knowledge" (WIPO, 2018a).

References

Primary sources

Anaya, J. S. (2016). Technical Review of Key Intellectual Property-Related Issues of the WIPO Draft Instruments on Genetic Resources, Traditional Knowledge and Traditional Cultural Expressions by Professor James Anaya (December 6, 2016). WIPO/GRTKF/IC/33/INF/9. Information document submitted by the Secretariat of the United Nations Permanent Forum on Indigenous Issues. For IGC Thirty-Third Session, Geneva, February 27 to March 3, 2017. Retrieved from http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=360462

Convention on Biological Diversity (CBD). (2010). The Nagoya Protocol on Access and Benefit-Sharing. Retrieved from https://www.cbd.int/abs

CBD. (n.d.) Article 15: Access to Genetic Resources. Retrieved from https://www.cbd.int/convention/articles/default.shtml?a=cbd-15

CBD. (n.d.). *Bonn Guidelines. Retrieved from* https://www.cbd.int/doc/publications/cbd-bonn-gdls-en.pdf

CBD. (n.d.). Article 8(j): Traditional Knowledge, Innovations and Practices. Retrieved from https://www.cbd.int/traditional

Food and Agriculture Organisation of the United Nations (FAO). (2001). International Treaty on Plant Genetic Resources for Food and Agriculture. Retrieved from http://www.fao.org/plant-treaty/en/

Hardison, P. (2016). Response to WIPO Indigenous Panel on Outstanding/Pending Issues in the IGC Draft Articles on the Protection of Traditional Knowledge: Indigenous Peoples' and Local Communities' Perspectives (November 28, 2016). IGC Thirty-Second Session, Geneva, November 28 to December 2, 2016 (on file with author).

Intergovernmental Committee (IGC). (n.d.). World Intellectual Property Organisation (WIPO). Retrieved from http://www.wipo.int/tk/en/igc

McCook, W. (2014a). Traditional Knowledge and Traditional Cultural Expressions: Certain Suggested Cross-Cutting Issues – Non-Paper Prepared by the IGC Chair, His Excellency, Ambassador Wayne McCook. For IGC Twenty-Seventh Session, March 24 to April 4, 2014. Retrieved from http://www.wipo.int/export/sites/www/tk/en/igc/pdf/igc_27_issues.pdf

McCook, W. (2014b). Traditional Knowledge and Traditional Cultural Expressions: Certain Suggested Cross-Cutting Issues (March 12, 2014). WIPO/GRTKF/IC/INF/10. Document prepared by the Chair of the Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore, His Excellency, Ambassador Wayne McCook. Retrieved from http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=269068

Milpurrurru v Indofurn Pty Ltd [1994] 130 ALR 659 (Federal Court of Appeal) (Austl.).

Standing Committee on the Law of Patents. (n.d.). Website. World Intellectual Property Organisation (WIPO). Retrieved from http://www.wipo.int/policy/en/scp/

UN. (1992). Convention on Biological Diversity (CBD). Retrieved from https://www.cbd.int/convention

World Intellectual Property Organisation (WIPO). (2014a). Report (July 2, 2014). WIPO/GRTKF/IC/27/10. IGC Twenty-Seventh Session, Geneva, March 24-April 4, 2014. Retrieved from https://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_27/wipo_grtkf_ic_27_10.pdf

WIPO. (2014b). The Protection of Traditional Knowledge: Draft Articles (June 2, 2014). WIPO/GRTKF/IC/28/5. For IGC Twenty-Eighth Session, Geneva, July 7 to 9, 2014. Retrieved from https://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_28/wipo_grtkf_ic_28_5.pdf

WIPO. (2014c). The Protection of Traditional Cultural Expressions: Draft Articles (June 2, 2014). WIPO/GRTKF/IC/28/6. For the IGC Twenty-Eighth Session, Geneva, July 7 to 9, 2014, Retrieved from WIPO. (2014b). The Protection of Traditional Knowledge: Draft Articles (June 2, 2014). WIPO/GRTKF/IC/28/5. Prepared for the IGC Twenty-Eighth Session, Geneva, July 7 to 9, 2014, Retrieved from https://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_28/wipo_grtkf_ic_28_5.pdf

WIPO. (2015). Matters Concerning the Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge and Folklore. Agenda Item 17, Assemblies of Member States of WIPO Fifty-Fifth Session, October 5 to 14, 2015. Retrieved from http://www.wipo.int/export/sites/www/tk/en/igc/pdf/igc_mandate_1617.pdf

WIPO. (2016a). Report (September 23, 2016). Thirtieth Session Geneva, May 30 to June 3, 2016. WIPO/GRTKF/IC/30/10 Retrieved from http://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_31/wipo_grtkf_ic_31_ref_30_10.pdf

WIPO. (2016b). The Protection of Traditional Knowledge: Draft Articles, Rev. 2 (in Annexure) (October 3, 2016). WIPO/GRTKF/IC/32/4. For IGC Thirty-Second Session, Geneva, November 28 to December 2, 2016. Retrieved from http://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_32/wipo_grtkf_ic_32_4.pdf

WIPO. (2016c). Informal Briefing Notes: Perspectives and Experiences on Tiered Approach to the Protection of Traditional Knowledge: Scope of Protection, Exceptions and Limitations (November 3, 2016) (on file with author). WIPO. (2017a). The Protection of Traditional Knowledge: Draft Articles (March 15, 2017). WIPO/GRTKF/IC/34/5. For IGC Thirty-Fourth Session, Geneva, June 12-16, 2017. Retrieved from https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=368218

WIPO. (2017b). The Protection of Traditional Cultural Expressions: Draft Articles (June 15, 2017). WIPO/GRTKF/IC/34/8. IGC Thirty-FourthSession, Geneva, June 12-16, 2017. Retrieved from https://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_34/wipo_grtkf_ic_34_8.pdf

WIPO. (2018a). The Protection of Traditional Knowledge: Draft Articles (June 26, 2018). WIPO/GRTKF/IC/37/4. For IGC Thirty-Seventh Session, Geneva, August 27 to 31, 2018. Retrieved from https://www.wipo.int/edocs/mdocs/tk/en/wipo_grtkf_ic_37/wipo_grtkf_ic_37_4.pdf

WIPO. (2018b). The Protection of Traditional Cultural Expressions: Draft Articles (June 27, 2018). WIPO/GRTKF/IC/37/5. Drafted for IGC Thirty-Seventh Session, Geneva, August 27 to 31, 2018. Retrieved from https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=409623

WIPO. (n.d.a). Draft substantive Patent Law Treaty. Retrieved from http://www.wipo.int/patent-law/en/draft_splt.htm

WIPO. (n.d.b). Case for support: Promoting effective participation of indigenous and local communities. WIPO Voluntary Fund for Accredited Indigenous and Local Communities. Retrieved from http://www.wipo.int/export/sites/www/tk/en/igc/pdf/flyer_vol_fund.pdf

Secondary sources

Adewopo, A., Chuma-Okoro, H., & Oyewuni, A. (2014). A consideration of communal trademarks for Nigerian leather and textile products. In J. De Beer, C. Armstrong, C. Oguamanam, & T. Schonwetter (Eds.), *Innovation and intellectual property: Collaborative dynamics in Afric*a (pp. 109–131. Cape Town: UCT Press.

Akinbogun, T. L., & Ogunduyile, S. R. (2009). Crafts engagement in the economic survival of South-Western Nigerian rural women. *Journal of Enterprising Communities: People and Places in the Global Economy, 3*(2), 217–234. https://doi.org/10.1108/17506200910960897

Anaya, J. S. (2004). *Indigenous peoples in international law* (2nd ed.). Oxford: Oxford University Press.

Arewa, O. B. (2004). *Piracy, biopiracy, and borrowing: Culture, heritage, and the globalization of intellectual property*. Case Research Paper Series in Legal Studies. Working Paper No. 04-19. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=596921

Arezzo, E. (2007). Struggling around the natural divide: The protection of tangible and intangible Indigenous property. *Cardozo Arts and Entertainment Law Journal, 25*(1).

Bala, A. (2011). *Traditional knowledge and intellectual property rights: An Indian perspective*. https://doi.org/10.2139/ssrn.1954924

Battiste, M. (Ed.) (2000). *Reclaiming Indigenous voices and vision*. Vancouver: UBC Press.

Blakeney, M. (1995). Milpurrurru & Ors v Indofurn & Ors: Protecting expressions of Aboriginal folklore under copyright law. *Murdoch University Electronic Journal of Law, 2*(1).

Boateng, B. (2011). *The copyright thing doesn't work here: Adinkara and Kente cloth and intellectual property in Ghana*. Minneapolis: University of Minnesota Press. https://doi.org/10.5749/minnesota/9780816670024.001.0001

Brown, M. F. (1998). Can culture be copyrighted? *Current Anthropology, 39*(2), 193–222. https://doi.org/10.1086/204721

Brown, M. F. (2004). *Who owns native culture?* Cambridge, MA: Harvard University Press.

Coombe, R. J. (1998a). *The cultural life of intellectual properties: Authorship, appropriation and the law.* Durham, NC: Duke University Press. https://doi.org/10.1215/9780822382492

Coombe, R. J. (1998b). Intellectual property, human rights and sovereignty: New dilemmas in international law posed by the recognition of Indigenous knowledge and the conservation of biological diversity. *Indiana Journal of Global Legal Studies 6*(1), 59–115.

De Beer, J., Oguamanam, C., & Schonwetter, T. (2014). Innovation, intellectual property, and development narratives in Africa. In J. De Beer, C. Armstrong, C. Oguamanam, & T. Schonwetter (Eds.), *Innovation and intellectual property: Collaborative dynamics in Afric*a (pp. 1–31). Cape Town: UCT Press.

De Sousa Santos, B. (Ed.) (2007). *Another knowledge is possible: Beyond Northern epistemologies*. London: Verso.

De Sousa Santos, B., Nunes, J. A., & Meneses, M. P. (2007). Introduction: Opening up the canon of knowledge and recognition of difference. In B. De Sousa Santos (Ed.) (2007). *Another knowledge is possible: Beyond Northern epistemologies* (pp. xxix–lxii). London: Verso.

Elahi, S., & De Beer, J., (2013). *Knowledge and innovation in Africa: Scenarios for the future*. With D. Kawooya, C. Oguamanam, N. Rizk, and the Open AIR Network. University of Cape Town and University of Ottawa: Open African Innovation Research (Open AIR).

Helfer, L. H. (2004). Regime shifting: The TRIPS Agreement and new dynamics of international intellectual property lawmaking. *Yale Journal of International Law, 29*(1), 1–83. https://doi.org/10.2139/ssrn.459740

Jayangakula, K. (n.d.). *The protection of the expression of folklore and copyright law*. Retrieved from https://www.academia.edu/3423284/The_Protection_of_the_Expression_of_Folklore_and_Copyright_Law

Konadu, K. B. (2007). *Indigenous medicine and knowledge in African society.* London: Routledge.

Kuruk, P. (1999). Protecting folklore under modern intellectual property regimes: A reappraisal of the tensions between individual and communal rights in Africa and the United States. *American University Law Review, 48*(4), 769–849.

Maiwada, S., Dutsenwai, S. A., & Waziri, M. Y. (2012). Cultural industries and wealth creation: The case of traditional textile industry in Nigeria. *American Journal of Contemporary Research, 2*(5), 159–165.

Maskus, K. E., & Reichman, J. H. (2004). The globalization of private knowledge goods and the privatization of global public goods. *Journal of International Economic Law, 7*(2), 279–230. https://doi.org/10.1093/jiel/7.2.279

Maskus, K. E., & Reichman, J. H. (Eds.) (2005). *International public goods and transfer of technology under a globalized intellectual property regime*. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9780511494529

May, C., & Sell, S. (2005). *Intellectual property rights: A critical history*. Boulder, CO: Lynne Rienner Publishers.

Memmi, A. (1990). *The colonizer and the colonized.* London: Earthscan.

Mgbeoji, I. (2001). Patents and traditional knowledge of the uses of plants: Is a communal patent regime part of the solution to the scourge of bio piracy? *Indiana Journal of Global Legal Studies, 9*(1), 163–186.

Mgbeoji, I. (2006). *Global biopiracy: Patents, plants, and Indigenous knowledge*. Vancouver: UBC Press.

Mutua, M. (2011). Savages, victims, and saviors: The metaphor of human rights. *Harvard Law Review, 412*(1), 201–244.

Oguamanam, C. (2007). Agro-biodiversity and food security: Biotechnology and traditional agricultural practices at the periphery of international intellectual property regime complex. *Michigan State Law Review, 2007,* 215–255.

Oguamanam, C. (2008). Local knowledge as trapped knowledge: Intellectual property, culture, power and politics. *Journal of World Intellectual Property, 11*(1), 29–57. https://doi.org/10.1111/j.1747-1796.2008.00333.x

Oguamanam, C. (2012). *Intellectual property in global governance: A development question*. New York: Routledge.

Oguamanam, C. (2014). Indigenous Peoples' rights at the intersection of human rights and intellectual property rights. *Marquette Intellectual Property Law Review, 18*(2), 261–295.

Oguamanam, C. (2015). Pressuring 'suspect orthodoxy': Traditional knowledge and the patent system. In M. Rimmer (Ed.), *Indigenous intellectual property: A handbook of contemporary research* (pp. 313–333). Cheltenham, UK: Edward Elgar. https://doi.org/10.4337/9781781955901.00024

Oguamanam, C. (2016). Tiered or differentiated approach to traditional knowledge: Insights for understanding the operations of the concept and evidentiary thresholds. Presentation to WIPO-IGC Seminar on Traditional Knowledge and Intellectual Property (Nov. 24–25, 2016). Retrieved from http://www.wipo.int/edocs/mdocs/tk/en/wipo_iptk_ge_2_16/wipo_iptk_ge_2_16_presentation_7oguamanam.pdf

Oguamanam, C. (2017). Ramifications of WIPO IGC for IP and development. In D. F. Robinson, A. Abdel-Latif, & P. Roffe (Eds.), *Protecting traditional knowledge: The WIPO Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge, and Folklore* (pp. 339–346). New York: Routledge.

Oguamanam, C. (2018a). Wandering footloose: Traditional knowledge and the public domain revisited. *Journal of World Intellectual Property, 21*(5-6), 306–325. https://doi.org/10.1111/jwip.12096

Oguamanam, C. (2018b). *Tiered or differentiated approach to traditional knowledge and traditional cultural expressions: The evolution of a concept*. CIGI Papers No. 185. Waterloo, ON: Centre for International Governance Innovation (CIGI). https://doi.org/10.2139/ssrn.3265807

Okediji, R. L. (2017). Negotiating the public domain in an international framework for genetic resources, traditional knowledge and traditional cultural expressions. In D. F. Robinson, A. Abdel-Latif, & P. Roffe (Eds.), *Protecting traditional knowledge: The WIPO Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge, and Folklore* (pp. 141-172), New York: Routledge.

Okediji, R. L. (2018). *Traditional knowledge and the public domain*. CIGI Papers No. 176. Waterloo, ON: Centre for International Governance Innovation (CIGI). Retrieved from https://www.cigionline.org/sites/default/files/documents/Paper%20no.176.pdf

OseiTutu, J. J. (2011). A *sui generis* regime for traditional knowledge: The cultural divide in intellectual property law. *Marquette Intellectual Property Law Review, 15*(1), 147–215.

Posey, D. A., & Dutfield, G. (1996). *Beyond intellectual property: Toward traditional resource rights for Indigenous Peoples and local communities*. Ottawa: International Development Research Centre (IDRC). Retrieved from https://www.idrc.ca/en/book/beyond-intellectual-property-toward-traditional-resource-rights-indigenous-peoples-and-local

Raustiala, K. (2007). Density and conflict in international intellectual property law. *UC Davis Law Review, 40*(3), 1021–1038.

Reichman, J. H. (2009). Intellectual property in the twenty-first century: Will the developing countries lead or follow? *Houston Law Review, 46*(4), 1115–1185.

Robinson, D. F. (2010). *Confronting biopiracy: Challenges, cases, and international debates*. London: Routledge. https://doi.org/10.4324/9781849774710

Robinson, D. F., Abdel-Latif, A., & Roffe, P. (Eds.) (2017). *Protecting traditional knowledge: The WIPO Intergovernmental Committee on Intellectual Property and Genetic Resources, Traditional Knowledge, and Folklore*. New York: Routledge. https://doi.org/10.4324/9781315666358

Scassa, T. (2015, November 26). Copyright of Inuit robe highlights gaps in Canadian legal framework [Blog post]. Teresa Scassa Blog. Retrieved from http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=200%3

Schneider, J. (1987). The anthropology of cloth. *Annual Review of Anthropology, 16*, 409–448. https://doi.org/10.1146/annurev.an.16.100187.002205

Stiglitz, J. E. (1999). *Knowledge as a global public good.* Oxford: Oxford University Press.

Stopp, M. P. (2012). The Coast Salish knitters and the Cowichan sweater: An event of national historic significance. *Material Culture Review/ Revue de la culture matérielle, 76,* 9–29. Retrieved from https://journals.lib.unb.ca/index.php/MCR/article/view/21406/24805

Wiessner, S. (1999). Rights and status of Indigenous Peoples: A global comparative and international legal analysis. *Harvard Human Rights Journal, 12*.

Wiessner, S., & Graham, L. (2011). Indigenous sovereignty, culture, and international human rights law. *South Atlantic Quarterly, 110*(2), 403–427. https://doi.org/10.1215/00382876-1162516

Yu, P. K. (2007). International enclosure, the regime complex, and intellectual property schizophrenia. *Michigan State Law Review*, *2007(*1), 1–33.

Treatment of Kenya's Internet Service Providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017

John Walubengo
Lecturer, Multimedia University of Kenya, Nairobi
https://orcid.org/0000-0001-8278-1792

Mercy Mutemi
Advocate of the High Court of Kenya, Mutemi Sumbi Law, Nairobi
https://orcid.org/0000-0002-9983-3170

Abstract
Kenya's Copyright (Amendment) Bill, 2017, is nearing its final stage of consideration by Parliament. In this article, we provide a review of the Bill's provisions in respect of its treatment of internet intermediaries, specifically internet service providers (ISPs). We seek to establish the impact that the intermediary liability provisions in the Bill could have on ISPs' operations if the Bill is passed into law in its present form. We applaud the Bill's provision for a "safe harbours" regime, whereby ISPs would incur no liability, or limited liability, for certain specific intermediary actions. However, we also note that the framing of the Bill's notice-and-takedown provisions would require quasi-judicial skills on the part of ISPs, which may not be appropriate. We conclude by providing recommendations for how legislators could address the weaknesses in the Bill's treatment of ISPs.

Keywords
copyright, copyright infringements, internet services providers (ISPs), internet intermediaries, intermediary liability, safe harbours, notice-and-takedown, Kenya, Copyright Act, Copyright (Amendment) Bill

DOI: https://doi.org/10.23962/10539/27532

Recommended citation
Walubengo, J., & Mutemi, M. (2019). Treatment of Kenya's internet service providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017. *The African Journal of Information and Communication (AJIC), 23,* 1–11.
https://doi.org/10.23962/10539/27532

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:
https://creativecommons.org/licenses/by/4.0

1. Introduction

Copyright is a legal right granted to authors of original works allowing them to exclusively control the use, exploitation, and distribution of the works. Copyright infringement is conduct that violates any of the copyright holder's exclusive rights. Direct liability for copyright infringement is imposed on the infringers themselves. Liability may also be imposed on parties who did not take part in the infringement but either had a relationship with the direct infringer or had control over the use of copyright works by the direct infringer (see Scott, 2005, p. 104). This is known as *secondary liability,* and is the bedrock of *intermediary liability* for copyright infringement.

Internet service providers (ISPs) play a crucial role as intermediaries in the provision of services online (see Comninos, 2012). Legislators are often looking for ways to co-opt ISPs into controlling online activity, as they reckon the efficacy of ISPs would exceed that of law enforcement entities. What makes ISPs particularly attractive to legislators is their ability to grant or deny access to their services. Moreover, it is argued that ISPs materially contribute to copyright infringement because they provide the infrastructure that the infringers use, and that, for this reason, they are in a better position than copyright holders to stop copyright infringement (see Comninos, 2012; Ncube 2019; Walubengo, 2016). These conjectures may be countered by the argument that, because of the level of automation they employ, ISPs for the most part lack knowledge of the content that passes through their systems (see Walubengo, 2016). The large volume of traffic also inhibits ISPs' capacity to monitor the content moving to and from their users.

Intermediary liability for copyright infringement is a fraught area of copyright law. Prosecuting ISPs as direct or secondary infringers runs the risk of compelling ISPs to curtail investment in technological innovation—out of fear that they may incur intermediary liability based on a new form of conduct. At the same time, however, failure to prescribe certain forms of liability for copyright infringement online may discourage copyright holders from making their work available online (Scott, 2005). The applicable Kenyan law is the Copyright Act of 2001 (hereafter "the Act") (Republic of Kenya, 2001), with subsequent revisions and judicial pronouncements. The Act, in its present form, does not address the issue of intermediary liability, leaving copyright holders and ISPs to determine their own modes of interaction in the Kenyan context.

2. Relevant provisions in the Copyright (Amendment) Bill, 2017

Kenya's Copyright (Amendment) Bill, 2017 (hereafter the"Bill") (Republic of Kenya, 2017) is a project of the Kenya Copyright Board, which was established in terms of the Act to administer all aspects of copyright and related rights in Kenya. The Bill has undergone all the relevant stages in both the National Assembly and the Senate and, at time of finalisation of this article in June 2019, awaits final consideration

before the National Assembly. The Bill introduces substantial amendments to the Copyright Act. Of concern for this article are the amendments touching on intermediary liability for copyright infringement, and specifically intermediary liability as it pertains to ISPs.

Definition of ISPs

The Bill defines an ISP as "any person providing information services, systems, or [sic] access software provider that provides or enables computer access by multiple users to a computer server including connections for […] the transmission or routing of data;" (Clause 2). This definition is compound, and it does not offer sufficient clarity as to which internet players will be considered ISPs for purposes of the Bill. Clause 19 of the Bill, which would import the "safe harbours" regime into Kenyan copyright law, alludes to various forms of ISP conduct, such as ISPs providing access, caching, hosting and information location.

Broad ISP liability provisions

The Bill does not provide for an obligation on ISPs to monitor content transmitted, stored or linked. Neither is an ISP required, in terms of the Bill, to investigate suspicious activity for infringement.[1] An ISP will, however, be obliged to comply with the notice-and-takedown procedure provided for in the Bill. ISPs will also be required, pursuant to a court order, to disclose the identities of subscribers to investigative agencies if it is suspected that those subscribers are engaging in activity that amounts to copyright infringement.[2] A third obligation is for ISPs to designate an agent, and an address, to which notice-and-takedown instructions can be sent.[3]

In addition to these broad obligations, the Bill addresses intermediary liability in two more specific ways: (1) by prescribing safe harbours, and (2) by providing for a two-stage notice-and-takedown procedure. We now consider these two sets of provisions in detail.

Safe harbours

A key feature of the Bill is its aforementioned adoption of the safe harbours regime.[4] The principle underlying safe harbours is that an ISP will be guilty of contributory or vicarious infringement only if its actions fall outside the scope of certain permitted types of conduct ("safe harbours") prescribed by law. The Bill proposes four safe harbours: a conduit safe harbour, a caching safe harbour, a hosting safe harbour, and an information location safe harbour. The Bill's safe harbours provisions borrow significantly from section 512 of the US Digital Millennium Copyright Act (DMCA) of 1998 (USA, 1998).

1 See proposed section 35C(2) in the Bill's Clause 19.
2 See proposed section 35C(1)(a) in the Bill's Clause 19.
3 See proposed section 35C(1)(b) in the Bill's Clause 19.
4 See proposed sections 35A, 35B, and 35C in the Bill's Clause 19.

Conduit safe harbour

The conduit safe harbour, provided for in the Bill by proposed section 35A(1)(a), would protect an ISP from incurring liability for copyright infringement where the ISP's only role was "providing access to or transmitting content, routing or storage of content in ordinary course of business". Other conditions that would need to be met for this harbour to be applicable are that the ISP must "not initiate the transmission"; must not "select the addressee"; must provide the conduit "in an automatic, technical manner without selection" of the content; "must not modify" the content; and must "not in any promote" the content (sect. 35A(1)(a)(i)-(v)).

Where the conduit safe harbour applies, there would be no obligation on the ISP to take down or disable access to content upon the issuance of a takedown notice. We see this as a reasonable approach, since any infringing material would be on the user's computer and the ISP in such cases is purely acting as a conduit for content access (see Urban & Quilter, 2006).

Caching safe harbour

In terms of the caching safe harbour provided for in the Bill by proposed section 35A(1)(b), ISP conduct that would be exempt from copyright infringement liability would be content storage that is "automatic, intermediate and temporary" and conducted in order "to make onward transmission of the data more efficient to other recipients […]". ISPs generally use caching services to increase network performance and to reduce network congestion. When caching occurs, the material in question is stored on the ISP's system for a short period of time, so as to facilitate potential access by additional users seeking access to the same material. Caching is an integral part of the internet architecture, and hence it requires safe harbour exemption from liability.[5]

This harbour only offers protection if the ISP "does not modify" the content; "complies with rules regarding" cache-updating, in accordance with "generally accepted standards"; "complies with conditions on access to the material"; and "does not interfere with the lawful use of technology to obtain information on the use of the material" (sect. 35A(1)(b)(i)–(iv)). It is not entirely clear what the final two of these conditions relate to. Specifically, when the Bill requires that an ISP "complies with conditions on access" to the content, as stated in 35A(1)(b)(ii), it would have been useful to make reference to sample access conditions as set out by an originating site. And the phrase "lawful use of technology to obtain information on the use of material" is not clear. While it would seem to be a reference to non-interference with the technology that makes the content available for subsequent users, the provision does not offer clarity on what precisely amounts to "interference" of the kind that the ISP must refrain from if it is to remain in the caching safe harbour.

5 See *Field v. Google, Inc.* (2006).

There is one more condition an ISP must adhere to in order to be covered by the caching safe harbour. The ISP must remove or disable access "once it receives a takedown notice […] or where the original material has been deleted or access disabled on orders of a competent court or otherwise on obtaining knowledge of unlawful nature of the cached material" (sect. 35A(1)(b)(v)).

Hosting safe harbour

The hosting safe harbour, provided for in the Bill by proposed section 35A(1)(c), would protect ISPs from liability "for damages arising" from content they store "at the request of" a user. This could include content stored on behalf of web-hosting providers, video-hosting sites such as YouTube, cloud services, and other cloud storage providers such as Google Drive (see Wang, 2014). In order to be covered by this safe harbour, the ISP must "not have actual knowledge that the content or activity related to the material is infringing" copyright; the ISP must not be "aware of the facts or circumstances of the allegedly infringing activity unless the infringing nature of the material is apparent"; and the user must not be "acting under the authority or control" of the ISP (sect. 35A(1)(c)(i)-(ii)). Also, in order for this harbour to be effective, the ISP must comply with a takedown notice within 48 hours (sect. 35A(1)(c)(iii)).

Information location safe harbour

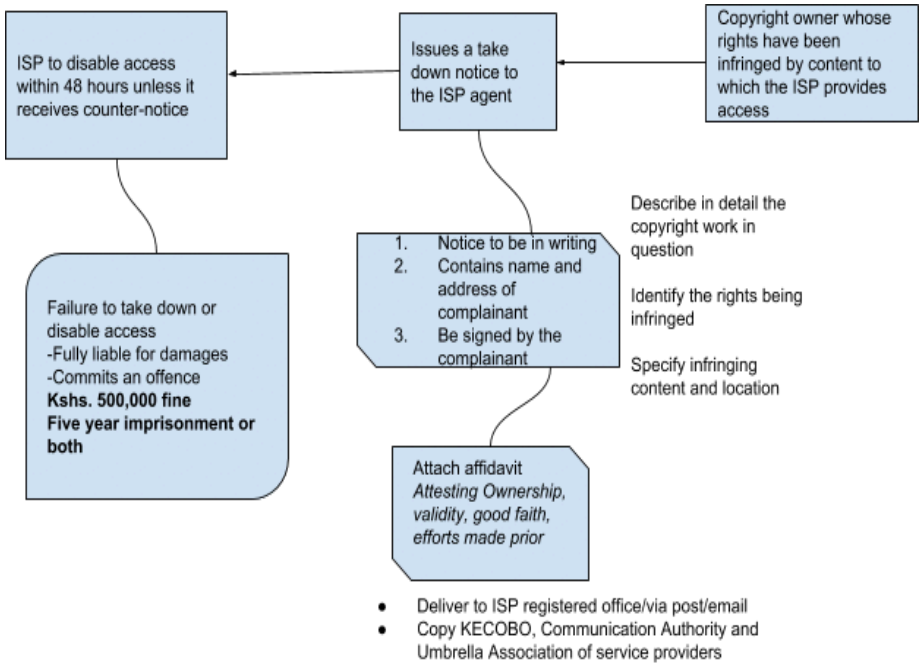
The information location safe harbour, provided for in the Bill in proposed section 35A(1)(d), protects the ISP from liability for "damages incurred by a person" if the ISP "refers or link users to a webpage containing infringing material" or if the ISP "facilitates infringing activity, by using information location tools" such as "a directory, index, reference, pointer or hyperlink". ISP facilitation of search engines such as Google, and indexing sites, is protected under this harbour. The ISP must not have had "actual knowledge" that the content is infringing, and must not have been "aware of the facts or circumstances" leading to the infringing activity (provided the infringing nature of the material was "not apparent") (sect. 35A(1)(d)(i)-(ii)). Further, the ISP is required to remove or disable access to "the reference or link to the content or the infringing activity" once it has been notified of the infringing nature of the content or activity (sect. 35A(1)(d)(iii)).

Notice-and-takedown procedure

The diagram below in Figure 1 illustrates the notice-and-takedown procedure proposed in the Bill (sect. 35(B)(1)). The notice-and-takedown procedure would e a two-step process involving (1) the complainant who claims its copyright is being infringed, and (2) the ISP who is providing access to the infringing content. The complainant must issue a takedown notice giving the details of the infringing work, its location, and the copyright being infringed. The ISP must comply with the takedown notice within 48 hours of receiving the notice, with failure to do so resulting in liability, both civil and criminal, for the ISP. In respect of the criminal liability, failure to comply with a takedown notice would attract a KES500,000 (approx. USD5,000)

fine, or a five-year imprisonment, or both. These penalties would be borne by the ISP and by every employee of the ISP who was responsible for the non-compliance with the takedown notice.[6]

Figure 1: Illustration of the notice-and takedown procedure proposed by the Bill



Source: Authors' illustration

The Bill's approach to notice-and-takedown ignores certain crucial aspects of due process and natural justice. Ignoring due process is likely to put the ISPs at odds with their users. The Bill would, if signed into law in its present form, transform the ISP from a potential contributory or vicarious infringer to an arbiter (see Mutemi, 2017). The ISP, despite being the medium through which the infringement is carried out, would become, contemporaneously, a judicial and enforcement officer. The ISP would be required to consider the affidavits sworn by the complainant, which give particulars on copyright ownership and infringement.

6 See proposed section 38(A)(1) in the Bill's Clause 22.

Needless to say, ISPs are not intellectual property experts; nor are they schooled in the justice system, specifically on matters of giving judicial relief. An affidavit containing untrue information would result in perjury proceedings if the same were presented before a court of law. Yet the ISP has no interest in verifying the veracity of the statements averred in an affidavit. Thus, the standard of proof required before a complainant is granted relief sought would be extremely low and one-sided if the Bill were to become law without amendment. The complainant would only be required to set out specific details of the copyright work and attach an affidavit of ownership, validity, and good faith.[7]

If the takedown were, more correctly, to be effected by a court process on an interlocutory basis, the complainant would be required to at least demonstrate that it (1) has a prima facie case with a possibility of success, and (2) that it would suffer irreparable damage without the orders sought. In the Kenyan legal context, before copyright infringement is confirmed, a claimant is, in terms of the precedent established by *Paul Odalo Abuor v Colourprint Ltd & Text Book Centre Ltd* (2002), required to (1) show that the content for which copyright is claimed is copyrightable, (2) that the complainant is indeed the copyright holder, and (3) that the defendant's conduct amounts to infringement that is not legally excused. An arbiter would thereafter make a ruling on what would be the suitable remedy in each case. Each of these issues troubles even the courts. The answers to these questions are not straightforward, and rather require balancing between the complainant's and defendant's claims. The Bill's provisions would bypasses these important determinations, thus privileging the claims of copyright holders.

The other due process issue raised by the Bill's approach to notice-and-takedown is the automatic granting of relief without giving the impugned content owner its right to be heard. The Bill provides for blind, strict adherence to the takedown notice, through imposing criminal liability on ISPs failing to execute takedown notices. The Bill cites a counter-notice provision in proposed section 35B(4), but only in passing and without going into detail as to what an ISP would be required to do should it receive a counter-notice. An ISP could, therefore, be expected to ignore any such counter-notice for fear of the criminal penalty to be imposed in case of non-compliance with the original takedown notice.

ISPs are offered a further incentive, in the Bill's proposed section 35B(9), to indiscriminately take down content once a notice is issued, because, in terms of this section, they will not be held liable for wrongful takedown in response to a valid notice-and-takedown procedure. It would only make sense for an ISP to err on the side of compliance, given the promise of immunity, rather than risk criminal sanction

7 See proposed section 35B(2)(g) in the Bill's Clause 19.

and legal fees (Walubengo, 2018). In the process, the ISP could supress the legitimate speech of its users (see Scott, 2005, p. 99).

Registration of copyright is not mandatory in Kenya.[8] Neither is non-registration a bar to judicial action or remedy. This means that ISPs would have no comprehensive reference point, even if they were to attempt to carry out due diligence in order to avoid customer fallout. This would open the gates for deception, i.e., false copyright claims leading to erroneous content takedowns. The Bill provides a checking mechanism, in proposed section 35B(7), to ensure that copyright holders do not abuse the notice-and-takedown procedure, but this mechanism is limited to instances of false or malicious notice-and-takedown instructions.

Exceptions and limitations

Another potential dilemma for the Bill's proposed in notice-and-takedown procedures is the uncertainty, in the Kenyan legal context, as to which conduct would amount to non-infringing use because of its coverage under the limitations and exceptions provided by Kenyan copyright law. The "fair dealing" exception, provided for in the Act and in the Bill's Second Schedule (section 26(3)(A)(1)(a)), permits use of copyright works, without obtaining the permission of the right holder, for "fair dealing for the purposes of scientific research, private use, criticism or review, or the reporting of current events; […]". In terms of this provision, and other limitations and exceptions provided for in the Act and the Bill, not all unauthorised use of copyrighted works is unlawful. At the same time, however, it is often debatable whether a use of a work is permitted by one of the limitations and exceptions. These grey areas are why governments and judiciaries have had to develop complex regulations and rules on fair dealing and other limitations and exceptions, with determinations often having to be made on a case-by-case basis (see Urban & Quilter, 2006).

In terms of the Bill, in an instance where an impugned behaviour amounted to fair dealing or a use permitted by another limitation or exception, a copyright holder would still have a right to commence a notice-and-takedown procedure (35(B)(i)). Yet ISPs cannot be expected to have the capacity to make a determination on what amounts to a permitted use in terms of the copyright limitations and exceptions, and they will be incentivised, if the provisions in the Bill become law, to comply with takedown notices. A copyright holder, even if well aware that the activity complained of amounts to fair dealing, could still be inclined to issue a takedown notice, knowing that the ISP will almost certainly honour it. This would defeat the purpose of development of the fair dealing exception and other copyright limitations and exceptions, which were developed to ensure public-interest access in support of access to knowledge and related educational and social imperatives. A likely outcome

8 See section 22(5) of the Copyright Act of 2001.

would be reversal of gains offered by the fair dealing exception. For instance, copyright holders would have a right, under the provisions proposed by the Bill, to issue takedown notices in efforts to silence critics (see Urban & Quilter, 2006).

An additional concern with Bill's proposed notice-and-takedown procedure is the apparent latitude it would provide businesses to engage the predatory practice of demanding takedown of a competitor's content (see Urban & Quilter, 2006).

3. Recommendations

Learn from the US experience

Safe harbours were first introduced into American legislation by the DMCA of 1998, and the Kenyan Bill essentially borrows the provisions of the DMCA. Numerous technological changes have taken place in the two decades ensuing since the DMCA's enactment, and, moreover, the DMCA has been tried and tested, with its weaknesses demonstrated. Kenya must learn from the failures of DMCA and improve on the DMCA model. For instance, a study carried out after the enactment of the DMCA showed that most of the takedown notices sent to ISPs related to non-copyrightable material or materials covered by "fair use" (the US variant of "fair dealing", which is more flexible than fair dealing) (Urban & Quilter, 2006).[9] This finding needs to inform the Kenyan position, i.e., it shows the need for an impartial arbiter to play a role in decisions as to whether content should be taken down.

Add clarity

Some of the problems presented by the Bill are drafting errors that can be easily fixed, as follows:

- Clause 19, introducing sections 35A(1)(a)-(d), needs to be revisited, as its present wording exempts ISPs from general liability for copyright infringement for conduct covered by the *conduit* and *caching* safe harbours (sect. 35A(1)(a)–(b)), yet the exemption from liability is only for "damages" in respect of conduct covered by the *hosting* and *information location* safe harbours (35A(1)(c)-(d)). Harmonisation would appear to be necessary across 35(A)(1).

- Section 35A(1)(b)(v) needs refinement in order to state more precisely what an ISP is to do upon receiving a takedown notice. At present, the sub-section refers, too vaguely, to "removing or disabling access".

- The Bill must pronounce itself more precisely on who can issue a takedown notice to an ISP. The Bill's proposed Section 35A(1)(d)(iii) would require that the ISP remove or disable access to links once the ISP has been informed

9 See *Online Policy Group v Diebold Inc.* (2004), a US case that demonstrates illegitimate use of notice-and-takedown procedures in violation of "fair use" doctrine provisions for permission-free use of copyright works.

of infringing content. We recommend that this requirement be made more reliable through specification that whoever is informng the ISP of infringing content must be the proven copyright holder for the material.

Improve the notice-and-takedown procedure

Due process must be written into the notice-and-takedown procedure, via the following changes:

- The Bill ought to provide for an impartial arbiter to decide on instances of copyright infringement.
- The need for immediacy of the ISP takedown is appreciated, and this can be preserved. We propose, however, that the takedown be temporary e.g., for 14 days, during which time the copyright holder would have to obtain a court order confirming the necessity of the takedown, i.e., confirming that the takedown arose out of a genuine infringement. If the copyright holder fails to obtain the court order in the given period, the ISP could restore access to the content. This would help ensure that there is only genuine use of the notice-and-takedown procedure.
- The Bill must also require ISPs to be transparent to their users on the notices received and the actions taken. This would give alleged infringers the information necessary for them to lodge counter-notices.
- The counter-notice provisions ought to be elaborated. The Bill must also prescribe the form of a counter-notice, and what the ISP ought to do if it receives a counter-notice. We propose that in the instance of a counter-notice, the ISP should not be compelled, at the same time, to take down the impugned content in terms of the original notice; rather, the ISP should be compelled to wait for a court order making a formal determination on the same.

References

Legal instruments and cases

Field v. Google, Inc., 412 F. Supp. 2d 1106 (D. Nev. 2006).

Online Policy Group v. Diebold Inc., 337 F. Supp. 2d 1195 (N.D Cal. 2004).

Paul Odalo Abuor v. Colourprint Ltd & Text Book Centre Ltd (2002) (unreported).

Republic of Kenya. (2001). Copyright Act of 2001, as amended in 2009. Retrieved from http://www.kenyalaw.org/Downloads/Acts/Copyright%20Act.pdf

Republic of Kenya. (2017). Copyright (Amendment) Bill, 2017. Retrieved from http://www.parliament.go.ke/sites/default/files/2018-09/COPYRIGHT%20%28AMENDMENT%29%20BILL.pdf

United States of America (USA). (1998). Digital Millennium Copyright Act (DMCA) of 1998. Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998). https://www.copyright.gov/legislation/pl105-304.pdf

Secondary sources

Comninos, A. (2012). *The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain*. Association for Progressive Communications (APC). Retrieved from https://www.apc.org/en/pubs/liability-internet-intermediaries-nigeria-kenya-so

Mutemi, M. (2017). ISPs to be enlisted in the fight against piracy in Kenya. [Blog post]. Centre for Intellectual Property and Information Technology (CIPIT), Strathmore University. Retrieved from http://blog.cipit.org/2017/11/06/internet-service-providers-to-be-enlisted-in-fight-against-piracy-in-kenya/

Ncube, C. (2019). Submission on the South African Copyright Amendment Bill [B13B - 2017]. Submitted to NCOP Select Committee on Trade and International Relations, Parliament of South Africa, Cape Town, on behalf of DST/NRF SARChI Research Chair: Intellectual Property, Innovation & Development, University of Cape Town. Retrieved from http://infojustice.org/wp-content/uploads/2019/03/Ncube-NCoP-Submission-February-2019.pdf

Scott, M. (2005). Safe harbours under the Digital Millennium Copyright Act. *NYU Journal of Legislation & Public Policy*, *9,* 99–166. Retrieved from http://www.nyujlpp.org/wp-content/uploads/2012/11/mike-scott-safe-harbors-under-the-digital-milennium-copyright-act.pdf

Urban, J. M., & Quilter, L. (2006). Efficient process or "chilling effects"? Takedown notices under section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer and High Technology Law Journal*, *22*(4), 621–693. Retrieved from https://scholarship.law.berkeley.edu/facpubs/501/

Walubengo, J. (2016, December 6). How the internet has made copyright protection murkier. [Blog post]. *Daily Nation.* Retrieved from https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-3477198-534u7t/index.html

Walubengo, J. (2018, February 19). Key IT concerns in copyright bill. [Blog post]. *Daily Nation.* Retrieved from https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4311138-lbnhtv/index.html

Wang, S. J. (2014). DMCA safe harbors for virtual private server providers hosting BitTorrent clients. *Duke Law & Technology Review*, *12*, 163–181. Retrieved from https://scholarship.law.duke.edu/dltr/vol12/iss1/9/

The Role of Discursive Constructions in Nigeria's ASUU-FGN Labour Conflict of 2013

Samuel Alaba Akinwotu
Senior Lecturer, Department of English Studies, Adekunle Ajasin University, Akungba-Akoko, Nigeria

https://orcid.org/0000-0002-2404-3094

Abstract

The performance of Nigeria's tertiary education sector has been undermined on numerous occasions by labour conflicts. While these labour disputes are widely reported in the media, there has been only minimal scholarly examination of the discourses that predominate in the media during these conflicts. Using the critical discourse analysis (CDA) and conceptual metaphor (CM) frameworks, this study examined the discursive features of a labour conflict in 2013 between the Academic Staff Union of Universities (ASUU) and the Federal Government of Nigeria (FGN). Statements by ASUU and FGN officials and their supporters, as published by Nigerian print and online news sources during the dispute, were purposively sampled, along with media outlets' editorial statements and readers' online comments. It was found that the labour dispute was discursively and metaphorically constructed in militaristic terms, as a conflict between two enemies engaged in a kind of battle or war. It was also found that both ASUU and the FGN engaged in propagandistic discourses in line with their militaristic discursive constructions, and that the two sides propagated disparaging discourses in respect of each other's motivations and behaviours. It was also found that certain readers reproduced elements of the prevailing discourses in their online comments on media coverage of the strike.

Keywords
Nigeria, tertiary education sector, universities, labour disputes, strikes, critical discourse analysis (CDA), conceptual metaphor (CM), sociolinguistic registers, Academic Staff Union of Universities (ASUU), Federal Government of Nigeria (FGN)

DOI: https://doi.org/10.23962/10539/27531

Recommended citation
Akinwotu, S. A. (2019). The role of discursive constructions in Nigeria's ASUU-FGN labour conflict of 2013. *The African Journal of Information and Communication (AJIC), 23,* 1–18. https://doi.org/10.23962/10539/27531

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: https://creativecommons.org/licenses/by/4.0

1. Introduction

Industrial conflict is a significant socio-political and economic problem affecting development in Nigeria. The nation witnesses frequent breakdowns in industrial relations between employees' unions and government, most of which result in strikes. Even though a strike action by employees or a lockout by management can be a useful tool in negotiations between employees and employers, these tools are generally very costly. During a strike or lockout, management (e.g., the government), the employees, and the public typically all suffer losses.

Ubeku (1983) has looked at the social and economic costs of strikes in Nigeria, including reduction of gross domestic product (GDP) and contribution to underdevelopment. Looking at Nigeria's tertiary education sector, Ofoele (2000) points out that industrial actions can sometimes be sufficiently protracted that they result in shifting of academic calendars, such that students are unable to graduate as and when due. The calendar of many public universities in Nigeria today is not in agreement with others at the international level because of incessant strikes in these institutions.

One major union in Nigerian universities that has consistently engaged government in labour disputes is the Academic Staff Union of Universities (ASUU). ASUU is the national union of all academic staff in public universities in Nigeria. It has branches in over 60 public universities across the nation. The union was formed in 1978 mainly to protect the interests of its members and as a platform to respond to the critical problems facing higher education in Nigeria (see ASUU (2008), as referenced in Odiagbe, 2012). Its formation coincided with the time when the country began to witness a decline in the oil boom and military dictatorship had become institutionalised to the extent that fundamental freedoms had been eroded. Over the years, ASUU has engaged in many industrial actions during labour disputes with the Federal Government of Nigeria (FGN). The first major challenge ASUU faced after its formation was the repressive measures taken by the President Olusegun Obasanjo military dictatorship in response to the 1978 "Ali Must Go" student protests. The union resisted the FGN's attempt to usurp the disciplinary functions of University Governing Councils and to control the universities by appointing their surrogates to Vice-Chancellor positions in contravention of established institutional procedures (Jega, 1995, p. 252).

In 1980, on the orders of President Shehu Shagari, six union members (lecturers) from the University of Lagos were dismissed for acting in opposition to FGN positions. ASUU rose against this, with a legal challenge, and the case went to the Supreme Court where, in 1986, a ruling was secured in favour of the lecturers. From the start, ASUU was a politically focussed union. As an affiliate of the Nigeria Labour Congress (NLC), ASUU brought high-profile debates on all major issues in the country into the operations of NLC.

The FGN, not comfortable with the rising profile of ASUU and its activities in NLC, disaffiliated ASUU from the NLC in 1988. This led to ASUU declaration of a strike in that year. ASUU also fought vehemently against the FGN's adoption in the mid-1980s of a structural adjustment programme (SAP) dictated by the World Bank and International Monetary Fund (IMF). The union's position was that the SAP sought to remove responsibility for education from the hands of the state and place it in the hands of the private sector. The FGN responded to ASUU's anti-SAP strike by proscribing ASUU, seizing all its properties, and banning its activities in the country. This led to a large exodus of academics, with over 1,000 leaving the country between 1988 and 1990 (Jega, 1994, p. 42).

Following its de-proscription in 1990, ASUU returned to the negotiation table with the FGN in 1991, but the negotiations—which centred on sector funding and improved working and salary conditions—broke down. In May 1992, ASUU declared another strike, but it was cut short by an order of the Industrial Arbitration Panel (IAP), which called for the suspension of the strike and ordered both sides to return to negotiations. The negotiations were successful and resulted in an agreement signed by both parties in September 1992 (see Jega, 1994; 1995; Odiagbe, 2011). In 2009, ASUU embarked on a four-month strike over government funding allocations to education and payment of academic allowances to ASUU members. This strike ended with the signing of the 2009 ASUU-FGN Memorandum of Understanding. Following what it saw as non-implementation of the provisions of the 2009 Memorandum, ASUU declared a strike—the strike that was the focus of my research—on 1 July 2013.

During the six months of this 2013 strike, both parties (ASUU and the FGN) engaged in intensive efforts to influence public opinion towards their positions. Even though strikes are widely reported in the Nigerian media, scholarly examination of the discourses deployed by competing sides in such disputes is scant—in spite of the potential usefulness of such analyses for understanding potential paths to resolution of such disputes. Accordingly, my study aimed at contributing to filling this research gap, through a critical study of some of the key discursive features, evident during the 2013 conflict, in the statements of participants, the statements of the participants' supporters, the content of media reports, the content of opinion pieces appearing in the media, and the content of reader responses to these writings.

My choice of the 2013 strike was motivated by two reasons. First, the strike was a continuation of the 2009 strike, which culminated in the signing of the landmark 2009 ASUU-FGN Memorandum of Understanding. Second, the strike discourses appearing in the media prompted many readers to post comments on news sites.

The study drew data from news articles, editorials, opinion pieces, and readers' comments that I purposively sampled from six widely-read, daily print and online

news sources (*The Punch*, *The Nation*, *Vanguard*, *This Day*, *Osun Defender* and *AIT Online*), with the data drawn from the period July to December 2013. Altogether, 17 statements present in the media, from ASUU and FGN officials and their supporters, and from media outlets' editorial-writers, were purposively selected for analysis based on their connection to the 2013 strike and their meaningfulness in discursive terms. In addition, six reader comments were purposively selected on the basis of their links to media content on the strike and on their discursive meaningfulness. The data were subjected to discourse analysis and analysis of metaphors.

2. Perspectives on industrial conflicts

Generally speaking, scholarly inquiries into industrial conflicts emerge from fields such as commerce, industrial relations, personnel management, law, political science and sociology, and are dominated by attempts to explain the prevalence of industrial conflicts in sectors and countries. There is a relative dearth of scholarly analysis of the discourses prevalent during industrial conflicts, in spite of the pragmatic relevance of such analysis to such conflicts' management and resolution.

Akhaukwa, Maru and Byaruhanga (2013) investigate the effect of sub-optimal collective bargaining processes on industrial relations environments in public universities in Kenya, and conclude that if labour and employers were fairer in their behaviour during labour negotiations, and if they were committed to implementation of agreements, collective bargaining processes could have much more positive effects on Kenya's industrial relations environment. Longe (2015) examines the impact of workplace conflict management on organisational performance in a Nigerian manufacturing firm, finding that collective bargaining strategy displays a highly significant positive correlation with organisational performance.

Odiagbe (2011) provides a historical and sociological account of industrial conflict between ASUU and the FGN. The study identifies poor teaching, poor learning and research facilities, poor remuneration, inadequate and poorly maintained accommodation facilities for students and staff, poor social amenities, and occupational stress among academics due to excessive workload, as major factors confronting higher education in Nigeria. Odiagbe concludes that ASUU-FGN conflict is made difficult to resolve by the fact that it entails both economic and political factors which have become institutionalised and embedded in the Nigerian polity.

Akinwale (2011) examines labour reform and industrial conflict management in Nigeria, and observes that efforts made towards ensuring industrial peace remain inadequate and largely mismanaged. Dahida and Adekeye (2013) have found that unstable industrial relations in public universities are to a great extent a result of government insensitivity to dispute-resolution mechanisms. Ahmed (2014) critically examines legislation on the right to strike in Nigeria, and observes that there are many stringent conditions which serve to dilute strike rights. Ekankumo and Konye (2014)

focus on the management of industrial disputes in teaching hospitals in Nigeria, identifying breaches of agreements, poor remuneration, and poor infrastructural facilities as the main causes of strikes.

In the existing research on the ASUU strike of 2013, the study by Aragbuwa (2014) employs Halliday's systemic functional grammar (SFG) framework (see Halliday, 1978) to analyse the thematic structure of statements by ASUU and FGN officials. Another study, by Ugwoma (2016), examines discourses in internet content on the strike through the lens of Van Dijk's psychologically-focused version of critical discourse analysis (CDA) (see Van Dijk (2006)), focusing on mental, context and event models in the media statements of FGN officials and FGN sympathisers. My study differed from those of Aragbuwa (2014) and Ugwoma (2016), in that (1) it examined the discourses deployed by official and supporters of *both* ASUU and the FGN; (2) is specifically examined the discourses as they appeared in print and online media reports; and (3) it also examined the discourses of readers via their online comments on media items. It is hoped that the findings offer a pragmatic resource that can inform mechanisms of conflict management and resolution in Nigeria.

3. Theoretical framework

There continues to be sustained interest, in the fields of media studies and related disciplines, in analysis of discourses that appear in the media. This is not unconnected to the important role of media in contemporary societies, coupled with the increased availability and accessibility, via online platforms, of media materials to researchers and the general public. Discourse analysis of media content can be made from a variety of theoretical perspectives. In this study, I employed both elements of both the aforementioned critical discourse analysis (CDA) frame and a compatible model focused on metaphors.

According to key CDA theorists (see Chuliaraki & Fairclough, 1999; Fairclough, 2001; Van Dijk, 1988; Wodak & Meyer, 2001), CDA studies, inter alia, the ways in which discourses are enacted, reproduced, and resisted by text and talk in social and political contexts. Van Dijk (1988) observes that CDA is concerned with the analysis of words used in discourses to reveal the sources of power, dominance, inequality, and bias, and how these sources are initiated, maintained, reproduced and transformed within specific social, economic, political and historical contexts. The theory contends that effectively accounting for a discursive event requires an adequate understanding of the situation(s), institution(s), and social structure(s) that frame it. This implies that discourse is constitutive of situations, objects of knowledge, and the social identities and relationships which exist between people and groups of people (see Wodak, 2002). CDA is political in its objectives, as it attempts to explain the connections between discourse, social practices, and social structures. It examines societal dynamics such as power, dominance, hegemony, ideology, class, gender, race, and discrimination. CDA seeks to understand how language can be used—in both

readily apparent and less readily apparent ways—as a tool to influence the thinking and actions of people and how powerful groups exercise control over public discourse.

CDA views our language as a system that encodes ideological patterns, whereby language is not just a mere means of communication but a representation of dynamic realities. CDA is often associated with Halliday's systemic functional grammar (SFG) framework in its focus on linguistic functions (see Halliday, 1985; Halliday & Hassan, 1989). SFG views language as a social process and, accordingly, Eggins (2004, p. 2) contends that the emphasis of SFG "has always been with the meanings of language in use in the textual processes of social life". This implies that there is an interrelation between form and content; between linguistic structures and the underlying ideology.

Another framework relevant to my study was the approach to the study of metaphor known as conceptual metaphor (CM). The 1980s saw a strong emergence of metaphor research, especially in the context of political discourse, following the publication of Lakoff and Johnson's seminal *Metaphors We Live By* (Lakoff & Johnson, 1980; Lakoff, 2003). According to Cserép (2014), a central thrust of the work of Lakoff and Johnson was that "[o]ur language is saturated with metaphors, rooted in recurring bodily experience, and our language is metaphorical simply because our conceptual system is metaphorical" (Cserép, 2014, p. 262*)*.

Lakoff and Johnson challenged the conventional, traditional view of metaphors as simply poetic or linguistic devices. In their analysis, metaphors are not just poetic "twists" of language; they are an integral part of how we conceptualise difficult and abstract concepts. Conceptual metaphor aligns with the view that linguistic units are symbolic structures, consisting of a pairing of phonological structure with semantic structure (see Langacker, 1987, p. 76). Cognitive linguists and CDA analysts recognise the discursive significance of metaphor in the communication and interpretation of meaning. In my study, I sought to make use of elements of both the CDA and CM approaches in my analysis of the data collected.

I also made use of the sociolinguistic concept of "register" during the course of the data analysis. Register refers to language usage variations dictated by situational context (see Halliday, McIntosh & Strevens, 1964). Register involves language use in relation to a given occupation or field of human endeavour, and it has to do with the patterned variation in language use that is peculiar to domains such as law, medicine, the military, and agriculture. Register is contextual, or situation-determined, because some socio-cultural elements exert influence on our choice of words in a given situation. Hence, context plays a significant role in the analysis of register and this, perhaps, explains why it is often deployed in CDA analysis. Halliday (1978) observes that the notion of register provides a means of investigating the linguistic foundations of everyday social interactions.

4. Findings and analysis

The findings and analysis provided in this section are divided into three sub-sections, namely: (1) discursive construction of the strike by its participants and supporters; (2) discursive representations of ASUU and the FGN; and (3) reader discourses in their online comments on elements of media items on the strike.

Participants' and supporters' discursive constructions of the strike: The strike as fight, battle, war

The main metaphorical ways in which the 2013 ASUU/FGN conflict is conceived in the statements of ASUU and FGN officials are as a fight, a battle, or a war, with the actions and decision-making of the opposing parties conceived in terms that one associates with severe conflicts. The strike is metaphorically conceptualised as contested terrain, even a battleground, where two opposing parties (ASU and the FGN) are clashing, adjusting tactics, anticipating the actions of the enemy, and reacting to the actions of the enemy.

The following statements, drawn from the sampled publications, reveal the fighting, battling and war registers present in the FGN and ASUU discourses during the labour conflict:

> **Statement 1 (FGN)**
> "We are not yet disposed to wielding the big stick, but if the government is pushed to the wall, it will invoke relevant laws to manage the situation. We are waiting for what they will do." ***– quoted by Information Nigeria (2013, November 30), in Osun Defender***

> **Statement 2 (FGN)**
> "[…] the security agencies have been directed to protect lives and property on all the campuses nationwide, especially in the universities that have reopened. […] The government will not tolerate any intimidation or harassment, and any violent union leader risks being arrested. But those who restrict themselves to the confines of the law have nothing to fear." ***– quoted by Information Nigeria (2013, November 30), in Osun Defender***

> **Statement 3 (ASUU)**
> "So, we are back to our trenches as it was the situation during the military era. We are ready for the worst now. If the situation becomes uncontrollable, we will also go underground and resort to guerilla [sic] tactics." ***– quoted by Information Nigeria (2013, November 30), in Osun Defender***

> **Statement 4 (ASUU)**
> "Our members are left with no other choice than to prosecute this strike to its logical conclusion. ASUU members nationwide are saying this strike will not be suspended until and unless the government respects the 2009 Agreement and makes concrete efforts to implement it in the best interest of the country." ***– quoted by Olugbamila (2013, August 23), in The Nation***

Statement 5 (FGN)
"[…] the strike action seems to have the backing of external forces seeking to bring his [President Goodluck Jonathan's] administration down." – ***quoted by Osun Defender, 30 November 2013***

Statement 6 (FGN: President Goodluck Jonathan)
"What ASUU is doing is no longer trade dispute but subversive action." – ***quoted by The Punch (2013, December 1)***

These statements by the opposing parties, as reproduced and disseminated in the media, reveal the participants discursively constructing the strike in fighting, battling, and even warlike, terms. A characteristic typical of situations of extreme conflict is a party or individual resorting to use of threats to intimidate an opponent. There is evidence of this in statement 2, in which the FGN speaker attempts to intimidate ASUU through threat of arrest ("any violent union leader risks being arrested") and prosecution ("will invoke relevant laws to manage the situation"*)*.

The phrases "wielding the big stick" and "we are waiting for what they will do" in statement 1, and the words "government will not tolerate any intimidation or harassment" in statement 2, are suggestive of a conflict that has, or will soon have, violent elements. President Jonathan's claim, in statement 6, that the ASUU is engaged in "subversive action", again suggests a conflict that is going to require, or already involves, a quasi-military or military dimension.

In statement 3, ASUU speaks in clearly militaristic terms, deploying multiple military/war registers: "we are back to our trenches", "we will also go underground and resort to guerilla [sic] tactics." Words such as *trenches* (dug out channel/trough), going *underground* (going into hiding), and *guerrilla tactics* (insurrectionary tactics involving going into hiding and occasionally hitting targets), are linguistic elements clearly suggestive of military engagements, battle scenes, and war. Meanwhile, the FGN suggestion, in statement 5, that ASUU's strike action has "the backing of external forces" also seems to imply that the labour dispute has elements akin to a military conflict—with ASUU's actions cast in terms usually reserved for descriptions of violent insurrections or terrorist activities prompting a state security or military response.

Also significant in statements 1-6 are several instances of the use of propaganda. Both sides appear to engage in propaganda in a manner characteristic of how this tool is used in violent conflicts, including military conflicts—as a tool aimed at gaining the support of the general public and/or turning public opinion against one's opponent. Propaganda during military conflicts heightens distrust between the opposing parties. The FGN's use of the expressions "subversive action", "backing of external forces", and "seeking to bring his [President Goodluck Jonathan's] administration down" are

propagandistic in a manner typical of military confrontations or of conflicts that may soon take on a military dimension. And ASUU is clearly aiming to sway public opinion to its side, and to demonise the government, with the warlike statement that "we are back to our trenches as it was the situation during the military era. We are ready for the worst now."

Discursive Representations of ASUU and the FGN

Representations of ASUU

Examination of statements 7-12 below, by FGN representatives and FGN supporters, reveals use of language that categorises, frames, and constructs ASUU members in an extremely negative light.

Statement 7 (A "social critic" sympathetic to the FGN)
"While the Federal Government […] continued [to] back down on all its positions, ASUU remained rigid. ASUU spurned all entreaties from […] all levels of the Federal Government." ***– opinion piece by Mohammed (2013, December 9) in Vanguard***

Statement 8 (FGN representative)
"Let them study the enabling laws to see what they have been violating." – ***quoted by Osun Defender, 30 November 2013***

Statement 9 (FGN representative)
"What they have done in the last four months amounted to economic sabotage […]. If they continue to take the law into their hands by paralysing activities in the universities, we may try them for economic sabotage." – ***quoted by Osun Defender, 30 November 2013***

Statement 10 (FGN: Finance Minister Ngozi Okonjo-Iweala)
"At present ASUU wants the government to pay N92 billion in extra allowances when resources are not there and when we are working to integrate past increases in pensions. We need to make choices in this country as we are getting to the stage where recurrent expenditures take the bulk of our resources and people get paid but can do no work […] [if ASUU's allowance demands are met and] we continue to pay them salaries and allowances we will not be able to provide infrastructure in the universities." ***– quoted by The Nation, 13 August 2013***

Statement 11 (A former student sympathetic to the FGN)
"Only a few of our academics engage in fruitful research capable of solving the needs of our society. Most of the university teachers set their target in journal publication that would help them gain promotion in their academic career even when such is far from rendering solution to our societal needs." ***– opinion piece by Festus (2013, August 29), in Osun Defender***

> **Statement 12 (A "social critic" sympathetic to the FGN)**
> "As the strike continued, some discerning Nigerians began to pick holes in the unwholesome practices of the ASUU National President, Dr Nasir Fagge and his leadership. All they did was to prolong the strike without listening to any word of reason. It was as if they were struggling to break the record on the longest lasting strike. Fagge bestrode negotiation rooms like a despot seeking who to damage." ***–opinion piece by Mohammed (2013, December 9), in Vanguard***

One can see, in statements 7-12, the FGN and its supporters deploying a wide range of condemnatory rhetoric and discourse to categorise and construct ASUU in disparaging terms. In statement 7, the FGN and ASUU are juxtaposed, with the FGN presented as accommodating ("continued [to] back down on all its positions"), and the ASUU as unyielding and rigid ("remained rigid"; "spurned all entreaties from […] all levels"). Statement 12 portrays ASUU as unyielding ("without listening to any word of reason").

Also among the discursive strategies employed by the FGN and its supporters in their portrayals of ASUU are appeals to patriotism—a characteristic of Nigerian political discourse that Okpanachi (2009) has pointed to. Appeals to patriotism are discursive, ideological devices employed to influence public perception and obtain public sympathy. Statement 9's reference to the ASUU's actions as "economic sabotage" seems clearly to suggest that ASUU is unpatriotic. And Finance Minister Okonjo-Iweala, in statement 10, also appears to cast the ASUU as disloyal to the country, when she says "We need to make choices in this country" and "[if ASUU's allowance demands are met and] we continue to pay them salaries and allowances we will not be able to provide infrastructure in the universities." The word "sabotage" also suggests illegality, implying that ASUU members are lawless, even criminals—a discourse that is also apparent in statement 8: "Let them study the enabling laws to see what they have been violating." Also suggesting a lack of allegiance to Nigeria's national interests is statement 9, with its allegation that "[o]nly a few of our academics engage in fruitful research capable of solving the needs of our society".

Statements 7-12 also contain instances where the FGN and its supporters appear to call into question the morality and integrity of ASUU members. In statement 10, the Finance Minister portrays ASUU as asking for too much ("extra allowances"), and asking to be paid for indolence ("people get paid but can do no work"). And in statement 12, the "social critic" sympathetic to the FGN, Mohammed, harshly attacks the character of the ASUU President Nasir Fagge, alleging that Fagge has engaged in "unwholesome practice" and has behaved "like a despot seeking who to damage."

At the same time, some of the FGN discourse reveals a desire to forge a sense of commonality between the government and the people of Nigeria. In contrast to the portrayals of ASUU leadership and members as being unpatriotic, the Finance Minister, in statement 10, seeks to present her government as speaking and acting on behalf of the general Nigerian public, employing linguistic elements that suggest commonality, togetherness, and solidarity. The Minister uses several phrases introduced by the plural pronoun "we", accompanied by verb forms followed by the preposition "to", suggesting forward movement, e.g.,

> […] we are working to […]
> We need to […]
> […] we are getting to […]
> […] we continue to […]
> […] we will not be able to […]

The plural pronoun "we" is a solidarity marker which serves to achieve an interpersonal function by presenting the Finance Minister as part of the general public, or at the very least someone protecting their interests. This is apparently aimed at influencing the general public towards believing her claims and giving her their support. Also, the verbs followed by "to" perform the linguistic act of seeking to convince the general public that the government is in motion, i.e., is active in working to ensure the betterment of the entire populace.

Representations of the FGN

In the media content sampled, the FGN and its officials are also subjected to negative discourses. Below are the key anti-FGN statements extracted from the data:

> **Statement 13 (ASUU: Union President Nasir Fagge)**
> "That a minister of education would pronounce a threat of mass sacking of academic staff is a tragedy of huge proportion for Nigeria and Africa." – ***quoted by AIT Online (2013, December 1)***

> **Statement 14 (ASUU: Union President Nasir Fagge)**
> "While ASUU has been struggling for conditions in which Nigerian students would benefit from a very much enhanced academic environment in teaching and research facilities, the Minister of Education is thinking of a thoughtless mass sack as a solution to the problems arising from government's non-implementation of an agreement reached with ASUU as if Nigerian rulers have made no intellectual progress since Abacha. […] we have noticed with disgust how easy it is for ministers and governments to take refuge in political blackmail." – ***quoted by AIT Online (2013, December 1)***

Statement 15 (editorial in *This Day*)
"After his recent rash pronouncement that striking members of the Academic Staff Union of Universities must return to work or get the boot, Supervising Minister of Education Nyesom Wike has had a lot of rationalisation to do in the court of public opinion. […] ASUU's request for greater validity of its agreements with the Federal Government was an opportunity for the government to prove its sincerity and preparedness to emerge from a history of untrustworthiness. If the government ever intended to honour the latest agreement with ASUU, signing a document to authenticate the agreement surely would have been the best way to demonstrate it to try get the trust of the union. [...] But the government has deliberately returned its relationship with the university teachers to a past of mistrust, a past any serious government would love to leave behind it." – ***This Day (2013, December 8)***

Statement 16 (ASUU: Union President Nasir Fagge)
"ASUU cannot believe that the [2009] agreement, the MoU and the Needs Assessment Report undertaken and endorsed by the highest public officials in the land, would be so blatantly ridiculed by the same people." ***– quoted by Olugbamila (2013, August 23) in The Nation***

Statement 17 (editorial in *The Punch*)
"For a leader who wants to leave a mark, the prolonged ASUU strike should be an opportunity for President Goodluck Jonathan to jump-start a serious discussion about the future of higher education in Nigeria. Since the government and teachers have failed to agree, an emergency has to be declared so that the problem can be solved holistically." – ***The Punch (2013, October 20)***

In statements 13 and 14 above, ASUU President Nasir Fagge portrays the FGN as negligent, framing the Minister of Education as "thoughtless" (statement 14) for considering a mass firing of teachers, which would, in Fagge's description, be "a tragedy of huge proportion" (statement 13). Fagge also calls into question the morality and integrity of the FGN—a strategy which, as seen earlier, the FGN also employs in its discourses on ASUU. Fagge makes reference to the regime of the late President Gen. Sani Abacha, a notoriously authoritarian and corrupt government in the 1990s, by suggesting "Nigerian rulers have made no intellectual progress since Abacha" and have engaged in "political blackmail" (statement 14). And in statement 16, in accusing the FGN of violating the terms of the 2009 ASUU-FGN Memorandum of Understanding, Fagge says "ASUU cannot believe" that the MoU and its accompanying texts, "endorsed by the highest public officials in the land, would be so blatantly ridiculed by the same people." This kind of discourse is clearly aimed at suggesting the FGN lacks integrity.

In a similar vein, *This Day*, in statement 15, casts the FGN as untrustworthy. *This Day*'s use of the wording "rash pronouncement" in statement 15 is an attack on the character of the Minister of Education, Nyesom Wike. And the clause, "If the government ever intended to honour the latest agreement with ASUU", accuses the FGN of deception and insincerity. Also, the *This Day* editorialist accuses the FGN of failing "to prove its sincerity and preparedness to emerge from a history of untrustworthiness", and in the process returning "its relationship with the university teachers to a past of mistrust, a past any serious government would love to leave behind it".

Statement 17, which comes from an editorial in *The Punch,* is an attack, albeit mild, on the character and office of the President. The reference to President Jonathan as someone "who wants to leave a mark", and the call for the President to declare "an emergency" to deal "holistically" with the future of higher education, appear to constructs President Jonathan as playing politics with the future of higher education in the country and failing to deal effectively with this important public policy area.

Reader discourses

The third type of discursive data analysed were reader inputs, via online "comments", in reaction to media items on the labour dispute. Below are six reader comments found to be meaningful in discursive terms. The reader responses provide indications of the degree to which the discourses discussed above—the discourses propagated by the FGN, by supporters of the FGN, by ASUU, and by media sympathetic to ASUU—are replicated in the discourses of consumers of the media items in which the discourses appear.

> **Reader comment 1**
> "I am presently a PHD student in the University of Ibadan and I must tell you that you spoke my mind. ASUU is not being sincere and considerate. The major thing they are fighting for is their earned income not infrastructural development. And it's so sad that majority of them don't merit this allowance. […] I had my MSc in UI and I can tell u dt [sic] my supervisor didn't monitor my project, as a matter of fact he did not correct anything in my study neither did he teach me anything and he is part of d [sic] lecturers requesting for earned income." ***– reader of Osun Defender, 29 August 2013.***

> **Reader comment 2**
> "It is obvious that ASUU is being used by APC [the main opposition party, the All Progressives Congress] in order to discredit and undermine the government of President Goodluck Jonathan by scoring cheap political points. Otherwise, how else can one describe ASUU's foot dragging method after having met with Mr Presdent [sic] [?]" – ***reader of Osun Defender, 30 November 2013***

Reader comment 3
"So, the President's associates think the President has done the unimaginable by sitting for 13 hours with union leaders. Did they remember the total number of days (not hours) the President sat down with the G-7 governors, most of who have now abandoned him? The truth is that we are no more in a military regime and the President cannot use high-handedness to run the country." ***– reader (Information Nigeria), in Osun Defender, 30 November 2013***

Reader comment 4
"I think the threat from the president has clearly indicated the stand of the government on this issue- they never meant all they've said in the previous meetings with ASUU leaders […] It has to go this way because their children are not studying in this country and those who do are in the private universities." ***– second reader of Osun Defender, 30 November 2013***

Reader comment 5
"What is the problem with our leaders [?] You failed to keep to the terms of an agreement you consciously entered into with ASUU since 2009, this time ASUU wants a little more commitment from you to avoid history repeating itself. Instead of doing the right thing in the interest of Nigerians, you are threatening to sack lecturers. Go ahead and see how that can solve the problem." ***– reader (Information Nigeria), in Osun Defender, 30 November 2013***

Reader comment 6
"What does it take the government to sign the agreement as being requested by ASUU if they are sincere? In fact, there would not have been any need for the strike if government had done 30% of what they have done now but they decided to allow them to go on strike before listening to them. It does not show any sign of seriousness on the part of government […]" – ***reader of This Day, 8 December 2013***

Reader comment 1 replicates, to some extent, the discourse seen earlier, in the statements of the FGN and its supporters, whereby ASUU members are framed as lacking integrity. Reader comment 1 is quite demeaning in its critique of ASUU, arguing that "[t]he major thing they are fighting for is their earned income not infrastructural development. And it's so sad that majority of them don't merit this allowance." And the reader seeks to add power to her/his critique by supporting it with reflection on personal experience, as follows: "I had my MSc in UI and I can tell u dt [sic] my supervisor didn't monitor my project, as a matter of fact he did not correct anything in my study neither did he teach me anything and he is part of d [sic] lecturers requesting for earned income."

The discourse in reader comment 2 reinforces the FGN discourse seen above, in which the ASUU is cast as being a proxy for forces hostile to the government—with the reader suggesting that ASUU is being sponsored by the APC (the opposition party) to discredit government. This reader seems to have been swayed by the content of the report she/he is responding to, in which the President is quoted as saying that the strike is "no longer trade dispute but subversive action", and by the report in which an FGN source says the strike action seems to have the backing of "external forces seeking to bring his [President Goodluck Jonathan's] administration down".

Reader comments 3 to 6 replicate discourses seen above in the statements of ASUU representatives and in the editorial comments of media outlets (*This Day, The Punch*) supportive of ASUU during the labour dispute. Comment 3 casts the President as ineffectual, mocking the FGN's applauding of the President for conducting lengthy negotiations with ASUU, and pointing to the President's much more protracted talks with "the G-7 governors, most of who have now abandoned him". Comments 4 and 5 question the morality and integrity of the FGN, which, in the words of reader 5, is not "doing the right thing in the interest of Nigerians". Comment 4 accuses the FGN of not acting in good faith, saying that "they never meant all they've said in the previous meetings with ASUU leaders". The comment goes on to cast doubt on the FGN's commitment to public tertiary education, arguing that politicians' children do not make use of public universities because they "are not studying in this country and those who do are in the private universities". Comment 6 accuses the government of lacking sincerity in its dealings with ASUU during the strike, and of not showing "any sign of seriousness" in the run-up to the labour dispute.

5. Conclusions

This study found that the 2013 labour dispute between ASUU and the FGN was discursively and metaphorically conceptualised by its participants as a conflict between two enemies engaged in a fight, a military struggle or battle, and even a war. It was also found that both the FGN and ASUU engaged in propagandistic discourses in support of their militaristic castings of the conflict, and that the FGN (and its supporters) and ASUU (and media sympathetic to it) propagated harshly disparaging discourses of each other. Finally, it was found that certain readers, in commenting on media items containing the aforementioned discourses, reproduced, and thus reinforced, elements of those discourses.

Accordingly, it can be concluded that, even though poor remuneration and poor teaching and learning facilities are basic factors motivating strike actions in Nigeria's higher education sector, the discourses at play during these labour disputes are, at the same time, likely to be significant contributors to the frequent recourse to strike action and the protracted nature of the disputes and strikes. Use of conflict-oriented, militaristic discourses, and harsh, demeaning discursive constructions of the characteristics of the opposing side, are certainly not helpful to resolution of such

labour disputes. Such discourses during the 2013 strike can only have increased the levels of animosity, bitterness and confusion.

There is, therefore, a need for realignment in the discourses of ASUU and the FGN when they are in disagreement. These two entities should seek to reduce the prevalence of conflict-oriented discourses and to seek to engender emergence of more constructive, trust-building discourses. Trust is key to the existence and success of any symbiotic relationship, and it is indispensable in resolution of conflicts. ASUU and the FGN should each seek to earn a measure of trust in the interactions with each other, so that their negotiations, while still inevitably oppositional in many respects, can, in some respects, be grounded in a shared ambition to improve the quality of Nigeria's public higher education sector.

References

Primary sources

Articles, opinion pieces, editorials

AIT Online. (2013, December 1). ASUU strike update: Nyesom Wike is ignorant - ASUU President. Retrieved from http://www.aitonline.tv/post-asuu_strike_update__nyesom_wike_is_ignorant___asuu_president

Festus, F. (2013, August 29). Questioning the sincerity of ASUU. *Osun Defender*. Retrieved from http://www.osundefender.com/strike-questioning-the-sincerity-of-asuu/

Information Nigeria. (2013, November 30). ASUU strike: Why Jonathan decided to come down hard on ASUU. *Osun Defender*. Retrieved from http://www.osundefender.com/asuu-strike-president-is-human-why-jonathan-decided-to-come-down-hard-on-asuu/

Mohammed, A. (2013, December 9). ASUU'S political game and Nigeria's university education. *Vanguard.* Retrieved from https://www.vanguardngr.com/2013/12/asuus-political-game-nigerias-university-education

Osun Defender. (2013, October 20). Breaking deadlock on ASUU strike. Retrieved from http://www.osundefender.com/breaking-deadlock-on-asuu-strike/

Osun Defender. (2013, November 30). ASUU strike no longer a trade dispute – Jonathan.

Osun Defender. (2013, December 16). ASUU strike: Lessons from Nigeria's longest strike as lecturers sheath their swords.

Orintunsin, J. (2013, August 13). FG to ASUU: We can't meet your demands. *The Nation*. Retrieved from http://thenationonlineng.net/new/fg-to-ASUU-we-cant-meet-your-demands/

Olugbamila, A. (2013, August 23). ASUU, govt talks crash. *The Nation*. Retrieved from http://thenationonlineng.net/asuu-govt-talks-crash/

This Day. (2013, December 8). ASUU Strike: As FG loses another opportunity to earn trust. Retrieved from http://allafrica.com/stories/201312091695.html

Utebor, S., & Makinde, F. (2013, December 1). ASUU strike, a rebellion – Jonathan. *The Punch*.

Readers' comments

Reader comment 1: Anonymous. (2013, August 29). *Osun Defender*. Retrieved from http://www.osundefender.com/strike-questioning-the-sincerity-of-asuu/

Reader comment 2: Clark. (2013, November 30). *Osun Defender*. Retrieved from http:/www.osundefender.org/?tag=dipreye-almieysigha

Reader comment 3: Sule. (2013, November 30). *Osun Defender*. Retrieved from http://www.osundefender.com/asuu-strike-president-is-human-why-jonathan-decided-to-come-down-hard-on-asuu/

Reader comment 4: Anonymous. (2013, November 30). *Osun Defender*. Retrieved from http://www.osundefender.com/asuu-strike-president-is-human-why-jonathan-decided-to-come-down-hard-on-asuu/

Reader comment 5: Apex. (2013, November 30). *Osun Defender*. Retrieved from http://www.osundefender.org/?tag=dipreye-almieysigha

Reader comment 6: Paulodinka Samuel O. (2013, December 8). *This Day*. Retrieved from http://allafrica.com/stories/201312091695.html

Secondary sources

Ahmed, A. B. (2014). A critical appraisal of the right to strike in Nigeria. *International Journal of Humanities and Social Science*, *4*(11(1)), 300–311.

Akhaukwa, P. J., Maru, L., & Byaruhanga, J. (2013). Effect of collective bargaining process on industrial relations environment in public universities in Kenya. *Mediterranean Journal of Social Sciences*, *4*(2) 75–286. https://dx.doi:10.5901/mjss.2013.v4n2p275

Akinwale, A. A. (2011). Labour reform and industrial conflicts mismanagement in Nigeria. Paper presented at the Sixth IIRA African Regional Congress of Industrial Relations: Emerging Trends in Employment Relations in Africa: National and International Perspectives, Lagos, 24-28 January.

Aragbuwa, A. (2014). The pragmatics of language use in industrial dispute: A study of the 2013 ASUU/FGN face-off. In R. O. Atoye (Ed.), *Papers in linguistics, volume 15* (pp. 1–21). Milton Park, UK: Taylor and Francis.

Cohen, R. (2001). Language and conflict resolution: The limits of English. *International Studies Review*, *3*(1), 25–51. https://doi.org/10.1111/1521-9488.00224

Cserép, A. (2014). Conceptual metaphor theory: In defence or on the fence*? Argumentum, 10*, 261–288.

Dahida, D. P., & Adekeye, J.A. (2013). A comparative analysis of trade disputes settlement in Nigerian public and private universities. *Journal of Law, Policy and Globalization*, *18*, 60–68.

Dunlop, J. T. (1958). *Industrial relations systems*. New York: Henry Holt and Company.

Eggins, S. (2004). *An introduction to systemic functional linguistics*. New York: Continuum.

Ekankumo, B., & Konye, I. F. (2014). Managing industrial disputes in the Nigerian teaching hospitals: An empirical analysis. *European Journal of Business and Management*, *6*(19), 152–162.

Fairclough, N. (2001). *Language and power*. New York: Longman.

Halliday, M. A. K. (1978). *Language as a social semiotic: The social interpretation of language and meaning.* London: Edward Arnold.

Halliday, M. A. K. (1985). *An introduction to functional grammar.* London: Edward Arnold.

Halliday M. A. K., & Hassan, R. (1989). *Language, context and text: Aspects of language in a social-semiotic perspective* (2nd ed.). Oxford: Oxford University Press.

Halliday, M. A. K., McIntosh, A., & Strevens, P. (1964). *The linguistic sciences and language teaching*. London: Longmans.

Jega, A. (1994). *Nigerian academics under military rule.* Department of Political Science, University of Stockholm.

Jega, A. (1995). Nigerian universities and academic staff under military rule. *Review of African Political Economy*, *22*(64), 251–256. https://doi.org/10.1080/03056249508704129

Lakoff, G. (2003, March 17). Metaphor and war, again. *Alternet*. Retrieved from https://www.alternet.org/story/15414/metaphor_and_war,_again

Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. Chicago: University of Chicago Press.

Langacker, R. W. (1987). *Foundations of cognitive grammar I: Theoretical prerequisites*. Stanford, CA: Stanford University Press.

Longe, O. (2015). Impact of workplace conflict management on organizational performance: a case of Nigerian manufacturing firm. *Journal of Management and Strategy, 6*(2), 83–92). https://doi.org/10.5430/jms.v6n2p83

Odiagbe, S. A. (2012). *Industrial conflict in Nigerian universities: A case study of the disputes between the Academic Staff Union of Universities (ASUU) and the Federal Government of Nigeria (FGN)*. PhD thesis, School of Social and Political Sciences, College of Social Sciences, University of Glasgow.

Ofoele (2000). *Management of industrial disputes*. Aba, Nigeria: Meta Printing.

Okpanachi, M. I. (2009). Discourse analysis of President Olusegun Obasanjo's national address on the Nigeria Labour Congress on 8th October, 2003. In A. Odebunmi, A. E. Arua, & S. Arimi (Eds.), *Language, gender and politics: A festschrift for Yisa Kehinde Yusuf* (pp. 312–325). Lagos: Concept Publications.

Olowe, J. H. O. (1993). *Language and ideology in Nigerian newspapers in English medium*. PhD thesis, Obafemi Awolowo University, Ile-Ife, Nigeria.

Ubeku, A. K. (1983). *Industrial relations in developing countries: The case of Nigeria*. London: Palgrave Macmillan. https://doi.org/10.1007/978-1-349-17265-8

Ugwoma, C. N. (2016). 2013 ASUU strike discourses in Nigeria: A critical discourse analysis. *Mediterranean Journal of Social Sciences*, *7*(2), 435–444. https://doi.org/10.5901/mjss.2016.v7n2p435

Van Dijk, T. A. (1988). *News as discourse*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Van Dijk, T. A (2006). Politics, ideology, and discourse. In K. Brown (ed.), *Encyclopedia of language and linguistics* (2nd ed.). https://doi.org/10.1016/B0-08-044854-2/00722-7

Wodak, R. (2002). What CDA is about: A summary of its history, important concepts and its developments. In R. Wodak, & M. Meyer (Eds.), *Methods of critical discourse analysis*. London: Sage.

PUBLICATION REVIEW

Book Review: Telecommunications Law and Regulation in Nigeria

Uchenna Jerome Orji, Telecommunications Law and Regulation in Nigeria*. Newcastle upon Tyne, UK: Cambridge Scholars Publishing, 2018, 640 pages, £80.99 (hardcover). ISBN: (10): 1-5275-0675-4; ISBN: (13): 978-1-5275-0675-6*

Reviewer: Peter Chukwuma Obutte
Senior Lecturer and Head of Department, Department of Jurisprudence and International Law, Faculty of Law, University of Ibadan, Nigeria
https://orcid.org/0000-0003-4252-6003

Keywords
telecommunications, law, regulation, policy, Nigeria

DOI: https://doi.org/10.23962/10539/27530

Recommended citation
Obutte, P. C. (2019). Book review: Telecommunications law and regulation in Nigeria. *The African Journal of Information and Communication (AJIC), 23,* 1-5. https://doi.org/10.23962/10539/27530

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: https://creativecommons.org/licenses/by/4.0

Uchenna Jerome Orji's book takes on the Herculean task of discussing and analysing the full range of laws, regulations, and policies that govern the Nigerian telecommunications industry. Developed as an expansion of his PhD thesis (Orji, 2017), the volume contains eleven chapters, an author's Preface, and a Foreword by Prof. Umar Garba Danbatta, CEO of the Nigerian Communications Commission (NCC).

Chapter 1 provides an introduction to telecommunications and its regulation. Orji traces the early history of telecommunications regulation in the United States and the United Kingdom, and the general principles that governed the early regulation of the industry in those countries. He discusses *ex ante* and *ex post* regulatory approaches, and common regulatory institutional designs, highlighting both advantages and disadvantages of various approaches and designs. This first chapter also outlines elements required to ensure a regulator's independence and discusses telecommunications as a field of law.

In Chapter 2, Orji presents an overview of the Nigerian telecommunications industry, covering both historical and contemporary elements, with this historical account is divided into four periods:

- the British colonial era, 1886-1960
- and early post-colonial years, 1960-1985
- the onset of commercialisation and liberalisation, 1985-1999
- the full liberalisation of the market, 1999-2017

A key element of this chapter is its discussion of the government's protracted process of privatising the state-owned Nigerian Telecommunications Limited (NITEL) between 2001 and 2014, before its eventual acquisition by the private-sector NATCOM Consortium in 2015. In the discussion, Orji links excessive government interference in NITEL's privatisation process to the eventual depreciation of NITEL's commercial value from over USD1 billion to its USD252 million value when acquired by NATCOM.

In Chapter 3, Orji examines legal and policy frameworks, including the legal basis for the industry's regulation under the Constitution of the Federal Republic of Nigeria (1999). He analyses several frameworks, including the Wireless Telegraphy Act (1998), the National Policy on Telecommunications (2000), the National Policy for Information Technology (2001), the National Space Policy (2001), the Nigerian Communications Act (2003), the National Information Technology Development Agency Act (2007), the draft National Information and Communication Technology Policy (2012), the Commercial Frequency Management Policy (2013), and the National Broadband Plan 2013-2018 (2013).

In this chapter, Orji also discusses the sector's key policy and regulatory institutions, including the industry regulator (the NCC), the Federal Ministry of Communication, and the National Frequency Management Council. Orji analyses the NCC's regulatory mandate and powers, and the mechanisms for holding the NCC accountable, i.e., executive supervision, legislative oversight, and judicial review. He argues that judicial review provides the best means of holding the NCC accountable. Orji also points to the need to reform the President's absolute power to remove a Commissioner of the NCC, through introduction of checks and balances to be provided by the legislature or judiciary, so as to guarantee the independence of the NCC to act in the best interests of the public and the industry. In reviewing the powers of the Minister of Communications Technology, Orji uses the 2010 case of *Mobitel Ltd v. The Minister of Information and Communication* to highlight limits of the Minister's powers over the direction of the NCC, pointing to how these limitations promote the NCC's regulatory independence in line with international best practice as mandated by the World Trade Organisation (WTO) Telecommunications Reference Paper (WTO, 1996).

In Chapter 4, Orji examines the licensing regime, under the Nigerian Communications Act (2003), which provides for individual, class, and spectrum assignment licences. The objectives of licensing, the duties of licensees and the legal effect of revoking or suspending a licence are analysed. Orji also discusses the application of the "use or lose" principle in the management of Nigeria's spectrum resources.

Chapter 5 examines the regulation of infrastructure deployment. Orji points to a general duty of care as the core legal principle that governs installation of telecommunications facilities. He links this principle with the obligations of operators to comply with environmental standards. Orji also discusses the challenges affecting deployment infrastructure in Nigeria, including the problem of multiple and conflicting layers of regulation by government authorities, e.g., the existence of conflicting environmental standards set by the NCC and the National Environmental Standards and Regulations Enforcement Agency (NESREA); overlapping regulation of telecommunications infrastructure by urban planning authorities at state and local government levels; lack of uniformity in the administration of "right of way" permits by authorities at different tiers of government; and the existence of multiple layers of taxation. Orji proposes national harmonisation of regulations on the installation of telecommunications infrastructure and the harmonisation of applicable industry taxes into a single regime.

Chapter 6 covers consumer protection. Among other things, Orji highlights the need for improved regulatory measures to protect consumers against unsolicited communications, drawing on examples from jurisdictions such as the United States and the European Union. The chapter also highlights the inadequacy of the data protection principles under the NCC's Consumer Code of Practice Regulations (2007), given that the principles do not specify the rights of consumers during the processing of their personal data.

Chapter 7 examines competition regulation in the industry, including measures to address anti-competitive practices, dominance, and the control of mergers and acquisitions. One of the key takeaways from this chapter is the apparent overlap between the merger regulation powers of the NCC and the Nigerian Securities and Exchange Commission (SEC). Orji suggest streamlining of the merger regulation mandates of the SEC and NCC, through an institutional arrangement such as a Memorandum of Understanding, in order to reduce the potential for a future regulatory conflict.

In Chapter 8, Orji looks at the regulation of interconnection and network access, including the provisions of the Nigerian Communications Act in respect of the special obligations of dominant operators. A key element in this chapter is its

discussion of the regulation of co-location and infrastructure-sharing, both of which can reduce the costs of network deployment and limit unnecessary duplication of network infrastructure.

Chapter 9 examines universal access and service, and situates these concepts within the context of the human rights to freedom of information and freedom of expression under Article 19 of the 1948 UN Universal Declaration of Human Rights, the 1966 International Convention on Civil and Political Rights, and the right to ICT access under Article 9 of the 2006 UN Convention on the Rights of Persons with Disabilities. The chapter also discusses the recognition of a human right to broadband/internet access in countries such as Costa Rica, Estonia, Finland, France, Germany, Greece, and Spain. In addition, Orji examines the challenges impeding universal access to broadband in Nigeria, including: the unharmonised administration of right-of-way permits; long delays in obtaining right-of-way permits; the high civil engineering costs incurred during network infrastructure deployment; a lack of infrastructure-sharing; and vandalisation of fibre optic infrastructure.

In Chapter 10, Orji focuses on the environmental protection and public health regime that applies in the industry, and analyses issues such as the siting and abandonment of masts and towers, and prevention of environmental pollution from telecommunication facilities. Orji illustrates the challenges of multiple and conflicting environmental regulations and charges being applied to telecommunication facilities by state environmental protection authorities. He notes that this has been a source of friction between the national environmental regulatory authority, NESREA, and state environmental protection authorities, while also increasing regulatory uncertainty and the compliance burden of operators. Orji recommends harmonisation of federal and state environmental regulations and standards, and amendment of the Constitution to grant the federal government ultimate power over the environmental regulation of telecommunications at both federal and state levels.

In Chapter 11, Orji discusses dispute resolution in the sector, and highlights the impediments to using judicial review to challenge the regulatory decisions of the NCC—due to the absence of a specified timeframe within which the NCC must provide a statement of the reasons for its decision to an aggrieved party. He proposes specification of such a timeframe for the NCC to adhere to, so as to prevent delays that could impede judicial review of an NCC decision.

This volume is a truly comprehensive compendium of Nigeria's telecommunications policies, laws and regulations, and it is current, touching on several very recent developments. Moreover, this book is written in straightforward language that makes it easy for the reader to follow the author's thoughts. The book also has a comprehensive table of contents, a rich index, and listings of all the legal cases, statutes, regulations and international instruments covered, all of which add to its

value as a reference resource. This book is recommended to students, academics, legal practitioners, regulators, and policymakers who are researching or working in the field of telecommunications law and regulation in Nigeria, or in other developing countries.

References

Mobitel Ltd v. The Minister of Information and Communication & Others [2010] (Unreported) Suit No. FHC/ABJ/M312/09.

Orji, U. J. (2017). *A critical review of the legal regime for telecommunications in Nigeria*. PhD thesis, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria.

World Trade Organisation (WTO). (1996). *Telecommunications services: Reference paper*. Retrieved from https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm

The African Journal of Information and Communication (AJIC)

Published by the LINK Centre
University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)