4TH ANNUAL COMPETITION AND ECONOMIC REGULATION (ACER) WEEK

JOHANNESBURG, SOUTH AFRICA

Friday, 20 July 2018

PARALLEL 3B: DIGITAL ECONOMY & COMPETITION
1130–1300

Chair: Nompucuko Nontombana, Competition Commission SA
Discussant: Tapera Muzata, Multichoice

Topic:

OTT Wars in South Africa: The Privacy and Cybersecurity Regulatory Asymmetry; and How it Complicates Advancing the Digital Economy Fairly – A Theoretical Perspective

By Stanley Shanapinda[1]

[1] Stanley Shanapinda, is a Ph.D. Candidate (Computer Science), having submitted his thesis for examination in April 2018. He is with the Australian Centre for Cyber Security (ACCS), University of New South Wales (UNSW), in partnership with the Data to Decisions Cooperative Research Centre (D2D CRC) research institute, South Australia. He has a Master of Management degree in ICT Policy and Regulation (MM ICT PR) from the University of the Witwatersrand (Johannesburg, South Africa). Stanley's is researching the relationships between the powers of law enforcement and national security agencies to access and use telecommunications metadata; the role of MNO's to protect privacy and ensure cyber security; the development of communications technologies and services such as OTT digital services and the role of oversight. He was the Journal Assistant for the Information Security Journal: A Global Perspective. He is a Legal Practitioner of the High Court of Namibia. He is the inaugural CEO of the Communications Regulatory Authority of Namibia (CRAN). Prior to that he was the Head: Legal Advice at Telecom Namibia Limited. Stanley was a Research Fellow and Lecturer in Communications Technologies Regulation, with the Centre for Technology and Society (CTS) at FGV Direito Rio, Brazil from February to June 2017.

Table of Contents

Abstract

Adopting strategies to offer digital products and services, enables the mobile network operator to compete with over-the-top content and communications services. It presents opportunities to make up for declining voice and SMS revenues. Adopting a digital strategy is a tough business decision that requires balancing customer privacy, cybersecurity compliance and the eroding traditional business case. This paper investigated the regulatory nexus between privacy, security and the digital economy in the South African context. It assessed how customer data may be shared with third parties to be processed using big data analytics, in a regulatory environment that requires the prior written authorisation of the individual but that also imposes this unenforceable legal requirement uniquely on the local mobile network operator. The multinational over-the-top content and communications service provider is unregulated, thereby creating the 'RICA Written Authorisation and POPIA Consent Regulatory Asymmetry' that negatively impacts cybersecurity governance, creates ethical dilemmas and ultimately does not advance the digital economy fairly, instead complicating it. This regulatory asymmetry requires revision to create a fair and predictable environment that advances the digital economy.

Key words: digital economy, personal information, cybersecurity governance, privacy, OTT, RICA, POPIA

I. Introduction and Problem Statement: The OTT Regulation Wars

The digital economy leaps and bounds in revolutionary fashion. The rise and rise of over-the-top (OTT) content and communications service provider tech giants (OTT service providers) such as Google, Facebook, Microsoft serves as evidence. The OTT service providers manage and operate platforms that resell OTT web applications such as WhatsApp and Facebook, used for instant messaging and for Voice over the Internet (VoIP) services such as Skype. In their stride, these applications leapt to outcompete traditional landline and mobile voice telephony and SMS services.[2] The mobile network operator (MNO)[3] is claiming the OTT service provider has a direct impact on its declining revenue.[4] The MNO is particularly concerned about protecting its voice and messaging business.[5] OTT connections and use outstrip traditional voice and SMS communications offered by the MNO. OTT services contributed to the bottom line of the MNO, when they were initially introduced. Thereafter services like WhatsApp became predators and traditional telecommunications services find themselves threatened.[6]

So as not to be outdone, the MNO is seeking to diversify its service offerings with versions of OTT services. These include mobile money and offering zero rated OTT web applications developed by the tech giants or their third-party associates. To address competition, the Vodacom Group adopted the Vision 2020 strategy, to develop a deep insight of customers' needs, wants and behaviours and to provide propositions[7] by using Big Data analytics, machine learning and artificial intelligence to provide a complete 360 view of the customer and to develop personalised customer propositions.[8] Vodacom states it needs to be relevant and intends on establishing itself as a leader in the digital space.[9] A key strategy of the

---

[2] Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA), 2002 (Act 70 of 2002) s 1(1) (definition of 'electronic communication service'); Electronic Communications Act (ECT), 2005 s 1 (definition of 'electronic communication') - ''electronic communications'' means the emission, transmission or reception of
information, including without limitation, voice, sound, data, text, video, animation,
visual images, moving images and pictures, signals or a combination thereof
by means of magnetism, radio or other electromagnetic waves, optical, electro- magnetic systems or any agency of a like nature, whether with or without the aid of
tangible conduct, but does not include content service;'

[3] Mobile Network Operators.
Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (Act 70 of 2002) s 1(1) (definition of 'electronic communication service provider')

[4] Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[5] Evidence by Prof Alison Gillwald, Executive Director, Research ICT Africa, to the Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[6] Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[7] Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 24 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

[8] Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 28 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

[9] Vodacom Group, 'Vodacom puts its partners in the driving seat of digital transformation' Press release,

Vodacom Group is 'Monetising mobile data'[10] via its digital products and services.[11] The Vodacom Group aims to collaborate with its partners, in its digital transformation strategy to deliver compelling data content and other digital products, services and solutions relating to social media, music, gaming and social data sharing, supported by personalised offers.[12] One such third party partner is Microsoft and the technology is the Azure cloud platform that allows the development, testing, management and storing of mobile web apps.[13]

While attempting to compete with OTT providers, the mobile network operator MNO[14] must jump the regulatory hurdle of universal service and access, lower tariffs, taxes, privacy, data protection, cyber security (critical infrastructure protection), law enforcement and security regulation. The MNO alleges the OTT service provider is not regulated to the same extent as the MNO.[15] The OTT provider is apparently granted an unfair advantage over legacy networks and services.[16] The MNO claims the regulatory burden is 'excessive'.[17] The general claim is that this overregulation creates competitive disadvantages for the MNO, as

---

Thursday, 10 May 2018 <http://www.vodacom.com/news-article.php?articleID=4476>; Vodacom advertised the position 'Senior Specialist Information Security', on the 24th of May 2018 to ensure that information security related policies are drafted and reviewed periodically; and to ensure that Vodacom complies with local and international laws regarding information security and data privacy .<https://www.linkedin.com/jobs/view/686527109/> .

Vodacom advertised the position 'Senior Insights Manager' on the 24th of May 2018, to research the customers, to profile them and seek ways to monetise the findings:

'Leading research studies and bringing the customer segments to life. Lead 3rd party research agencies to deliver segmentation, and other research studies commissioned for the enterprise business. Use the findings to bring enterprise segments to life and deliver detailed value-driven customer profiles.'

This paper only prioritized Vodacom and MTN, as major MNO players. Future research can assess the policies and practices of all market participants. The privacy policies of other MNO's and OTT service providers can be analysed in future research. Surveys can be conducted with customers to survey whether they have given any whether 'written authorisation' and 'consent' to the collection and processing of their data.

[10] Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 24 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

[11] Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 25 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

[12] Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 24 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

[13] Microsoft, Microsoft Azure 2018 <https://azure.microsoft.com/en-us/services/app-service/>; Vodacom Group, 'Vodacom accelerates digital transformation with first-to-market launch of suite of Azure solutions' Press release, Wednesday, 18 April 2018 <http://www.vodacom.com/news-article.php?articleID=4472>; <https://www.vodacombusiness.co.za/cs/groups/public/documents/document/azure-brochure.pdf>

[14] Mobile Network Operators.

Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (Act 70 of 2002) s 1(1) (definition of 'electronic communication service provider')

[15] Evidence by Mr Graham De Vries, General Manager: Regulatory Affairs, MTN, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[16] Evidence by South African Communications Forum on Over-the-Top services in South Africa
Ms Loren Braithwaite-Kabosha, SACF CEO, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[17] Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

the MNO is increasingly replaced by OTT services, resulting in revenue losses and user numbers.[18] In other words, the OTT service provider is competing with the MNO service provider, but the MNO is overregulated, unlike the OTT service provider. The services provided by the MNO and the services provided by the OTT provider compete with each other, and therefore should be regulated in the same way. [19] The MNO is therefore asking that economic regulation be extended to the OTT domain with the regulatory aim to encourage innovation and constructive competition.[20] The MNO is calling for market protection from the OTT provider.[21] Vodacom and MTN argued for fair and consistent regulatory treatment of competing services.[22] The regulation of the OTT provider was argued as necessary because of issues about cybersecurity, privacy, taxation and consumer protection.[23] The MNO is claiming the OTT provider is selling the 'personal information of subscribers'[24] and this is how they earned part of their income, the income of which is apparently not taxed in SA.[25]

Contrary to the claims above, the OTT provider claims it does not sell customer data.[26] The OTT provider claims the MNO and the OTT provider are in a symbiotic relationship where

---

[18] BEREC, 'Report on OTT services' January 2016 <https://www.bakermckenzie.com/en/-/media/files/insight/publications/2016/08/regulating-over-the-top-services/ar_itc_ottservices_aug16.pdf>

[19] Evidence by Mr Graham De Vries, General Manager: Regulatory Affairs, MTN, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[20] Evidence by South African Communications Forum on Over-the-Top services in South Africa Ms Loren Braithwaite-Kabosha, SACF CEO, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[21] Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[22] Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[23] Evidence by Mr Graham McKinnon, Chief Legal Officer, Cell C and Dr Andrew Barendse, Vodacom Managing Executive: Regulatory Affairs, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>; Evidence by Vodacom submission on Over-the-Top services in South Africa Dr Andrew Barendse, Vodacom Managing Executive: Regulatory Affairs, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[24] Evidence by Mr Graham De Vries, General Manager: Regulatory Affairs, MTN, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[25] Evidence by Mr Graham De Vries, General Manager: Regulatory Affairs, MTN, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[26] The statement was made by Facebook. Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

the MNO drives the demand for OTT services.[27] The OTT provider suggested the '… cumbersome and outdated regulation holding back the network operators …' be removed instead.[28] The OTT provider does not want to be burdened with the same 'cumbersome'[29] overregulation the MNO currently bears.[30]

II. Methodology

This paper aimed to understand how the cyber security and privacy regulatory framework regulates the sharing of customer data by the MNO vis-à-vis the OTT service provider, for using the data in the digital economy. It therefore studied the regulatory dynamic between the OTT service provider and the MNO under RICA[31] and its theoretical competitive impact.

This study used the desk research method. Laws and records from Parliamentary hearings were collected, interpreted and analysed. Documents about the privacy policies and practices were collected from the websites of the MNO and the OTT service providers and analysed. These documents were studied vis-à-vis the issues raised by the MNO's at Parliamentary hearings and contrasted against the legal provisions. Conclusions were then reached about how existing privacy and cybersecurity regulatory issues potentially impact the digital, economy, albeit from a theoretical perspective.

III. Related Works

Christoph Stork, Steve Esselaar and Chenai argue that although OTT services present a threat to voice and SMS revenue, OTT services also present an opportunity for the MNO when embraced,[32] such as zero-ratting OTT services to gain market share.[33] By offering zero rated OTT services, the MNO has less of an incentive to research and develop, whether directly or

---

[27] The statement was made by Google. Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[28] The statement was made by Google. Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[29] The statement was made by Google. Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[30] The statement was made by Google. Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options,
Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

[31] Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (Act 70 of 2002).

[32] Pg. 611-612 [5], [5.3] Christoph Stork Steve Esselaar Chenai Chair, 'OTT - Threat or opportunity for African MNOs?' *Telecommunications Policy*, Volume 41, Issues 7–8, August 2017, Pages 600-616 <https://doi-org.wwwproxy1.library.unsw.edu.au/10.1016/j.telpol.2017.05.007>

[33] Christoph Stork Steve Esselaar Chenai Chair, 'OTT - Threat or opportunity for African MNOs?' *Telecommunications Policy*, Volume 41, Issues 7–8, August 2017, Pages 600-616 <https://doi-org.wwwproxy1.library.unsw.edu.au/10.1016/j.telpol.2017.05.007>

otherwise, any if its own OTT services, and to share customer data, to develop new business models. This paper critically assesses how the current and proposed cyber security and privacy regulatory landscapes may impact decisions of the MNO to consider various options to take advantage of the mobile ecosystem, in one fashion or another.

Swales and others discussed and described how privacy is protected, but not in the context of OTT services in the digital economy.[34] Van Niekerk studied 54 cyber incidents in South Africa and was concerned about the rising trend whereby a high number of incidents of data exposure are caused by error.[35] Van Niekerk did not analyse how the relevant cyber security

[34] Lee Swales, 'Protection of personal information : South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' SA Mercantile Law Journal, Volume 28 Number 1, Mar 2016, p. 49 - 84SA Mercantile Law Journal; Constitutional protection of the right to privacy: the contribution of Chief Justice Langa to the law of search and seizure : part III : reflections on themes in Justice Langa's judgments Author Chuks Okpaluba, Acta Juridica 2015, pp 407 - 429 (2015); Leani Marlie Van Schalkwyk, Personal electronic data protection : UN guidelines and other documents. Chapter 6, Transactions of the Centre for Business Law 2005, pp 87 - 90 (2005)

[34] Anneliese Roos, Data protection : explaining the international backdrop and evaluating the current South African position, South African Law Journal 124, pp 400 - 437 (2007); Leani Marlie Van Schalkwyk, Personal electronic data protection : UN guidelines and other documents. Chapter 6, Transactions of the Centre for Business Law 2005, pp 87 - 90 (2005); Anneliese Roos, Data protection : explaining the international backdrop and evaluating the current South African position, South African Law Journal 124, pp 400 - 437 (2007); Iain Currie, The concept of privacy in the South African constitution : reprise : aantekeninge, Tydskrif vir die Suid-Afrikaanse Reg 2008, pp 549 - 557 (2008); Pamela Stein, South Africa's EU-style Data Protection Law : human rights law, Without Prejudice 12, pp 48 - 49 (2012); A. Roos, Personal data protection in New Zealand : lessons for South Africa?, Potchefstroom Electronic Law Journal 4, pp 62 - 109 (2008); Anneliese Roos, 'Privacy in the Facebook era : a South African legal perspective', South African Law Journal 129, pp 375 - 402 (2012); Kate Allan and Iain Currie, 'Enforcing access to information and privacy rights : evaluating proposals for an information protection regulator for South Africa : current developments', South African Journal on Human Rights 23, pp 570 - 586 (2007); Anneliese Roos, 'Core principles of data protection law', Comparative and International Law Journal of Southern Africa 39, pp 103 - 130 (2006); I.M. Rautenbach, 'Privacy taxonomies : aantekeninge', Tydskrif vir die Suid-Afrikaanse Reg 2009, pp 548 - 554 (2009); Anneliese Roos, 'Data protection : explaining the international backdrop and evaluating the current South African position', South African Law Journal 124, pp 400 - 437 (2007); Tamar Gidron, 'Publication of private information : an examination of the right to privacy from a comparative perspective (part 1)', Tydskrif vir die Suid-Afrikaanse Reg 2010, pp 37 - 52 (2010); Dewaldt Van Wyk, 'A safety, privacy and security disclosure : lifestyle gadgets', Without Prejudice 16, pp 58 - 59 (2016); J. Neethling, 'The concept of privacy in South African law : notes', South African Law Journal 122, pp 18 - 28 (2005); Jesicca Rajpal, 'Privacy after death in the digital world : the law', Without Prejudice 16, pp 52 - 53 (2016); Nthupang Magolego, 'Personal data on the Internet - can POPI protect you? : feature', De Rebus 2014, pp 20 - 22 (2014); Ashlin Perumall, 'Problems in protecting personal information : constitutional law', Without Prejudice 13, pp 61 - 62 (2013); Simone Monty Mark Heyink, 'guide to the protection of personal information act', De Rebus 2015, pp 60 (2015) Without Prejudice 15, pp 86 - 87 (2015); Russel Luck, RICA - walking a fine line between crime prevention and protection of rights : itc law', De Rebus 2014, pp 30 - 31 (2014); Dewaldt Van Wyk, 'How To : Living online, PRIVATELY : lifestyle gadgets', Without Prejudice 14, pp 98 - 99 (2014); Faan Coetzee, 'The press and POPI : media law', Without Prejudice 14, pp 69 - 71 (2014); Russel Luck, 'POPI - is South Africa keeping up with international trends? : feature', De Rebus 2014, pp 44 - 46 (2014); Bernard Hamann and Sylvia Papadopoulos, 'Direct marketing and spam via electronic communications : an analysis of the regulatory framework in South Africa,' De Jure 47, pp 42 - 62 (2014); Doraval Govender and Anthony Minnaar, 'The management of security information by private security service providers,' Acta Criminologica: Southern African Journal of Criminology 2014, pp 107 - 126 (2014); Mark Heyink, 'A guide to the protection of personal information act', De Rebus 2015, pp 60 (2015); Simone Monty, 'The popping of POPI : Protection of Personal Information law', Without Prejudice 15, pp 86 - 87 (2015); Megan Vries and Nabeela Moosa, 'The laws around social media : student feature', Without Prejudice 15, pp 39 - 40 (2015); Simone Monty, 'Putting yourself on the line : consumer law', Without Prejudice 15, pp 34 - 36 (2015).

[35] Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication (AJIC), 20, 113-132.

legislative framework imposed obligations on OTT providers and the MNO when sharing data with third parties, to address these incidents and what the likely economic regulation impact. Sutherland argued cybersecurity risks are not adequately assessed in South Africa.[36] Sutherland argues the ICT White Paper borrowed US and EU ideas but was not adapted to the South African landscape.[37] This paper analyses the South African cybersecurity landscape by looking at RICA, in the context of the indirect economic regulation of OTT services versus traditional voice and SMS services, and the risks posed to advancing digital innovation.

IV. The RICA Written Authorisation and POPIA Consent Regulatory Asymmetry

RICA regulates the sharing of certain communication-related information, by 'any person'.[38] The reference to 'any person' equally includes the OTT service provider and the MNO. Communication related information is '… any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialing or signaling 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 a telecommunications service provider and, where applicable, the location of the user within the telecommunication system;'[39] The communication-related information includes the location information of the device or the identifier such as the IMSI[40] and IMEI[41] (the serial number of the mobile device).[42] The biographical details about the customer and the communication-related information may be referred to as 'RICA Data'.[43] The third-party

---

https://doi.org/10.23962/10539/23573

[36] Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. The African Journal of Information and Communication (AJIC), 20, 101 [6]. <https://doi.org/10.23962/10539/23574>

[37] Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. The African Journal of Information and Communication (AJIC), 20, 102 [6]. <https://doi.org/10.23962/10539/23574>

[38] RICA ss 6, 10.

[39] RICA s 1 (definition of 'communication-related information').

[40] International Mobile Subscriber Identity.

[41] International Mobile Equipment Identity.

[42] Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. The African Journal of Information and Communication (AJIC), 20, 102 [6]. <https://doi.org/10.23962/10539/23574>; Shanapinda, S., (2016a), "Retention and disclosure of location information and location identifiers" *Australian Journal of Telecommunications and the Digital Economy* Vol 4 No 4, pp. 251-279 <http://dx.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,* Vol. 35 No. 3, pp. 17-19.

[43] RICA ss 1 (definition of 'real-time communication-related information'), 39(1)(a), (2), 62C. Real-time communication-related information means '… communication-related information which is immediately available to a telecommunications service provider-

(a) before, during, or for a period of 90 days after, the transmission of an indirect communication; and

sharing of RICA Data is regulated by the little-known principle that may be referred to as the 'Written Authorisation Requirement'. [44] However, not all parts of RICA apply equally to both the MNO and the OTT service provider. This Section describes how the MNO is regulated by RICA but how the OTT service provider is unregulated by RICA.

A. The RICA Written Authorisation Requirement and the RICA Written Authorisation and POPIA Consent Regulatory Asymmetry'

The MNO and the OTT service provider are both required to store the data about the customer for law enforcement purposes.[45] The Written Authorisation Requirement is the principle regulating the third party sharing of customer data, at a time when POPIA,[46] the Cybercrimes and the Cybersecurity Bill[47] are not yet in operation. The Written Authorisation Requirement states: The MNO may not intentionally provide or attempt to provide any *real-time communication-related information*[48] or *archived communication-related information*[49] (RICA Data) to any person, a third party. The MNO may only provide RICA Data to the customer. [50] However, the MNO may provide RICA Data to any third person at the specification and with the prior written authorisation of the customer.

(b) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates;'; RICA s 1 (definition of 'archived communication-related information'). Archived communication-related information is defined as '… any communication-related information in the possession of a telecommunications service provider and which is being stored by that telecommunication service provider in terms of section 30 (1) (*b*) for the period determined in a directive referred to in section 30 (2) (*a*) , becoming on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;'.

[44] RICA ss 12, 14.

[45] RICA s 40 (3)(b), (4)(a), (9), (10).

[46] Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

[47] Portfolio Committee on Justice and Correctional Services, DATE: 26 February 2018 CYBERCRIMES AND CYBERSECURITY BILL <https://www.ellipsis.co.za/wp-content/uploads/2017/11/180228Clause_by_Clause_Deliberation_Bill.pdf>

[48] RICA s 1 (definition of 'real-time communication-related information'). Real-time communication-related information means '… communication-related information which is immediately available to a telecommunications service provider-

(c) before, during, or for a period of 90 days after, the transmission of an indirect communication; and
(d) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates;'

[49] RICA s 1 (definition of 'archived communication-related information'). Archived communication-related information is defined as '… any communication-related information in the possession of a telecommunications service provider and which is being stored by that telecommunication service provider in terms of section 30 (1) (*b*) for the period determined in a directive referred to in section 30 (2) (*a*) , becoming on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;'.

[50] RICA s 1 (definition of 'customer'), 12. The term customer means '… any person-

(a) to whom an electronic communication service provider provides an electronic communications service, including an employee of the electronic communications 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

B. RICA Written Authorisation and POPIA Consent Regulatory Asymmetry

The MNO and the OTT service provider are treated differently by the Written Authorisation Requirement. The Written Authorisation Requirement is the tool creating the regulatory asymmetry between the MNO and the OTT service provider. The difference in the current and future regulatory treatment of the MNO and the OTT service provider may be referred to as the 'RICA Written Authorisation and POPIA Consent Regulatory Asymmetry'. The RICA Written Authorisation and POPIA Consent Regulatory Asymmetry may be described in terms of points 1 – 3 below.

1. The regulation of the MNO

The MNO is required by RICA to obtain the written authorisation of the individual customer to share and process the communication related information related to the individual.[51] The MNO must abide to the following four elements of the Written Authorisation Requirement:

a. The written authorisation must be obtained for each sharing occasion;[52]
b. The customer must determine the conditions,[53]
c. It is subject to these conditions RICA Data may be shared with the third party;[54] and
d. The customer determines and specifies who the third party is.[55]

The written authorisation must be in writing and it must be written by the customer. According to the ECT,[56] the authorisation will be in writing if the written document or the written information is in the form of a data message[57] and the information is accessible in a manner that is usable.[58]

2. The non-regulation of the OTT service provider

Since RICA came into effect, the OTT service provider did not have to comply with the written authorisation requirement.[59] No reference is made to the phrase 'any person'[60] in

---

(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.]'

The customer is not the customer of the OTT provider. The customer is the customer of the MNO, who is the telecommunications service provider.

[51] RICA s 14.
[52] RICA s 14.
[53] RICA s 14.
[54] RICA s 14.
[55] RICA s 14.
[56] Electronic Communications and Transactions Act 25 of 2002.
[57] ECT s 1 (definition of 'data message') (ECT 2002); ECA 2002 s 1 (definition of 'data'). A *data message* is defined as '… data generated =, sent, received or stored by electronic means and includes-

(a) voice, where the voice is used in an automated transaction; and
(b) a stored record;'

Data is defined as '… electronic representations of information in any form'.
[58] ECT s 12.
[59] RICA s 14.
[60] RICA ss 6, 10.

section 12 of RICA. Instead, the reference is to 'telecommunications service provider'.[61] So, whereas the MNO is restricted from sharing the location information of the mobile device, with third parties on the mobile ecosystem by RICA, the OTT provider is not regulated,[62] and this prohibition is not placed on the OTT service provider. [63]Although the OTT provider is permitted to monitor, intercept and use RICA Data for maintenance and its legal business purposes, the transfer of RICA Data to third parties, is not regulated – instead there is a gap in RICA. Without the prior written authorisation of the customer, the MNO is not legally allowed to share RICA Data with any third party, failing which the MNO would be violating the privacy of the customer.[64] The MNO is singled out not to share RICA Data with a third party. Only the MNO's local and international transfer of RICA Data to third parties in the digital ecosystem is regulated.

3. The double-decker regulation of the MNO

POPIA aims to level the playing field. Under POPIA, the MNO and the OTT service provider will be subject to the same legal conditions – to obtain the prior written consent of the customer, based on a prescribed template, as follows:[65]

a. The consent must be *voluntary*;
b. The consent must be *specific;* and
c. The consent must be an *informed expression* of the will of the individual that gives permission to the MNO or OTT service provider to process the personal information.[66]

RICA and POPIA are complementary pieces of legislation. In the absence of POPIA, RICA is the only other piece of legislation that allows the MNO the right to collect, use and share the data about the customer. Under POPIA the MNO and the OTT service provider will be subject to the same regulatory measures. However, the MNO would still be required to comply with the Written Authorisation Requirement, in addition to the POPIA consent requirement. When POPIA is enacted, the MNO must obtain written authorisation under RICA and simultaneously obtain customer consent under POPIA.[67] The OTT service provider would only need to comply with the consent requirement under POPIA.[68] This situation may be referred to as the 'MNO RICA-POPIA Double Decker Requirement'. This would make the legal requirements more onerous on the MNO. This adds to the regulatory asymmetry.

---

[61] RICA s 12.
[62] RICA s 12.
[63] RICA ss 12, 14; POPIA ss 18(1)(*g*), 72(1).
[64] RICA ss 6, 10, 14.
[65] POPIA s 11
[66] POPIA s 1 (definition of 'consent')
[67] POPIA s 11(1) (i)(*a*)
[68] POPIA s 11(1) (i)(*a*)

4. The No-Compliance, No-Enforcement and No-Oversight Phenomenon

The prohibition imposed on the MNO not to share the RICA Data without the written authorisation of the customer is not enforced. Also, there is no oversight to ensure the Written Authorisation Requirement is complied with prior to the use of RICA Data or after it has been processed, used and shared. In future, the Information Regulator will monitor and enforce compliance equally against the MNO and the OTT service provider, but only under POPIA.[69] The MNO is not guilty of an offence if the RICA Data is shared with a third party without a written authorisation obtained from the customer, despite the prohibition not to share RICA Data without the consent and without the conditions set by the customer.[70] This situation may be referred to as the 'No-Compliance, No- Enforcement and No-Oversight Phenomenon' or 'the No-COE Phenomenon', for short.

Section V analyses the relationship between cybersecurity governance and participation in the digital economy by sharing RICA Data with third parties.

V. Cybersecurity Governance and the Digital Economy

Cybersecurity governance demands compliance to relevant laws, such as RICA and POPIA.[71] When deciding to collect and use any information about customers, the MNO and the OTT service provider, must comply with the relevant regulatory environment to the extent that it is applicable to the digital products and services and the sharing of RICA Data with third parties. Governance requires adherence to policy and regulatory objectives and aligning those to the business objectives, when collecting, using, storing and processing RICA Data.[72] Data governance is therefore more than just about data protection and regulatory compliance, it is central to how an organisation such as the MNO operates.[73] Domestic regulations such as the Written Authorisation Requirement under RICA and the consent requirement under POPIA set the governance framework the MNO should comply with and incorporate into its internal data governance framework.

In order to participate in the digital economy at the same level as the OTT service provider, the MNO may need to access and use RICA Data. The business decision to share RICA Data in the digital economy with third parties, is generally subject to privacy and cybersecurity regulation, to which the OTT service provider may not generally be subject to. To assess the practical baseline levels of cyber security resilience readiness, legal requirements is a must to follow.[74] Thus, privacy and cybersecurity are two sides of the same coin. The MNO must

---

[69] PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) (POPIA): REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017. GG 4115, GoN 709, * September 2017 <http://www.justice.gov.za/inforeg/docs/InfoRegSA-RegulationsDraft-Aug2017.pdf>

[70] RICA 2003 s 50(2).

[71] ISO/IEC, 2015, 10 [5.6].

[72] ISO/IEC, 2013, 2 [4]; ASIC, 2017.

[73] Gregory, 2011, 230-248.

[74] NIST. (2018), "Framework for Improving Critical Infrastructure Cybersecurity", available at: < https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (accessed 2 May 2018); Federal Financial Institutions Examination Council, FFIEC Cybersecurity Assessment Tool, May 2017, pg. 7 <https://www.ffiec.gov/%5C/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf>.

secure RICA Data from unauthorised access and use.[75] So, when preparing internal cybersecurity risk assessment and risk management governance and oversight models, policies and procedures; and when conducting external dependency management to oversee third-party relationships, the OTT service provider and the MNO would both have to consider and incorporate privacy and cybersecurity laws and policies.[76] The participation of the MNO and OTT service provider in the digital economy hinges on the privacy protection and the cybersecurity governance that holds the balance of power. If the written authorisation of the individual is required, the question is whether the privacy policies and standard terms and conditions of the MNO qualifies as written authorisations.[77]

A. The Analysis of the Terms and Conditions and Privacy Policies of the MNO versus the OTT Service Providers

OTT service providers such as Facebook and Google can basically be regarded as self-regulatory. They can solely update their terms and conditions at any time.[78] The customer is subject to the protection under their local laws and court systems.[79] Since the RICA Written Authorisation Requirement does not regulate OTT service providers, there is no such legal protection for the SA'n customer. Since the OTT service provider is not required to comply with the Written Authorisation Requirement, the standard terms and conditions of the OTT service provider cannot be critically assessed against this legal requirement. The privacy policies of the OTT service provider are unregulated and therefore go uncheck.

The privacy policies, the standard terms and conditions, and the privacy practices of the MNO and the OTT service provider are materially similar.[80] The key similarity is that the privacy policies all lack any reference to the Written Authorisation Requirement. The MNO may and appears to have adopt similar terms and conditions as the OTT service provider. The lack of a compliance reference to the Written Authorisation Requirement may constitute a failure in cybersecurity governance. Vodacom states that it does disclose information about the customer, but it does not state that this information is only disclosed based on the conditions set by the customer in advance, and only to the third parties specified by the customer, as is required by the Written Authorisation Requirement.[81]

---

[75] RICA s 40(4)(a).
[76] NIST. (2018), "Framework for Improving Critical Infrastructure Cybersecurity", available at: < https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (accessed 2 May 2018); Federal Financial Institutions Examination Council, FFIEC Cybersecurity Assessment Tool, May 2017, pg. 6 <https://www.ffiec.gov/%5C/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf>.
[77] RICA s 14.
[78] Facebook, Terms of Service, 19 April 2018, [4] <https://www.facebook.com/legal/terms/update>
[79] Facebook, Terms of Service, 19 April 2018, [4] <https://www.facebook.com/legal/terms/update>
[80] Vodacom, Privacy Policy <http://www.vodacom.co.za/vodacom/terms/privacy-policy>; MTN Proprietary Limited, 'Terms and Conditions' 2017 <https://www.mtn.co.za/Pages/Termsandconditions.aspx?pageID=26>; Facebook, Terms of Service, 19 April 2018 <https://www.facebook.com/legal/terms/update>; Google, GOOGLE PRIVACY POLICY May 25, 2018 <https://policies.google.com/privacy>.
[81] Vodacom, Privacy Policy <http://www.vodacom.co.za/vodacom/terms/privacy-policy>

RICA uses the term communication-related information[82] referring to the RICA Data, unlike POPI that uses the term Personal Information (PI).[83] So under POPIA the question will become whether the RICA Data is PI. The term communication-related information is broad enough to include information that may be regarded as personal and sensitive.[84] The question under POPIA will be whether RICA Data is PI for RICA Data to require the prior consent of the customer before it is shared with a third party. Under RICA, the question is not whether the RICA Data is PI for it to require the prior written authorisation of the customer before it is shared with the third party. In its terms and conditions, the MNO states that it does not disclose PI about the individual, but this is information the MNO decides in his or her own unilateral view, what they consider as personal and what they consider as not personal. The question under RICA is whether the information (RICA Data) is real-time communication-related information[85] or archived communication-related information.[86] If the information to be shared is real-time communication-related information[87] or archived communication-related information,[88] the prior written authorisation of the customer is required. The question under RICA therefore is the extent to which these written authorisations have been obtained every time the call detail records, Internet session records, IMEI, IMSI, the IP Address[89] and URL[90] has been shared with a third party, and whether the customer decided specifically whether his or her information may be shared with a Vodacom partner such as Microsoft, to process using its Big Data analytics platform called Azure. Does the customer know that

---

[82] RICA s 14.

[83] POPI s 26, 27(1)(a), 28(3)

[84] Jonathan Mayer, Patrick Mutchler and John C. Mitchell, 'Evaluating the privacy properties of telephone metadata' (2016) 113(20) *Proceedings of the National Academy of Sciences of the United States of America* 5536–5541, 5536, 5538; Vodacom, Vodacom App Store T & Cs< https://myvodacom.secure.vodacom.co.za/vodacom/terms/vodacom-app-store-terms-and-conditions>

[85] RICA s 1 (definition of 'real-time communication-related information'). Real-time communication-related information means '… communication-related information which is immediately available to a telecommunications service provider-

(e) before, during, or for a period of 90 days after, the transmission of an indirect communication; and
(f) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates;'

[86] RICA s 1 (definition of 'archived communication-related information'). Archived communication-related information is defined as '… any communication-related information in the possession of a telecommunications service provider and which is being stored by that telecommunication service provider in terms of section 30 (1) (*b*) for the period determined in a directive referred to in section 30 (2) (*a*) , becoming on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;'.

[87] RICA s 1 (definition of 'real-time communication-related information'). Real-time communication-related information means '… communication-related information which is immediately available to a telecommunications service provider-

(g) before, during, or for a period of 90 days after, the transmission of an indirect communication; and
(h) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates;'

[88] RICA s 1 (definition of 'archived communication-related information'). Archived communication-related information is defined as '… any communication-related information in the possession of a telecommunications service provider and which is being stored by that telecommunication service provider in terms of section 30 (1) (*b*) for the period determined in a directive referred to in section 30 (2) (*a*) , becoming on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;'.

[89] Internet Protocol Address.

[90] Uniform Resource Locator.

Microsoft was signed up as a partner and will store its data, or was the data shared with Microsoft based on the standard terms and conditions and the privacy policy? Did the customer determine and decide on Microsoft, or did Vodacom alone decide on Microsoft? What conditions was the customer asked to set, was the customer informed that it may set conditions, and how have those conditions been incorporated into the agreement signed with Microsoft, and did this happen at every sharing accession? This is an issue the OTT service provider would be less concerned with, because the OTT service provider is not required to obtain the written authorisation[91] of the customer.

The privacy statements of the MNO and the OTT service provider does not make mention of any of the four elements of the Written Authorisation Requirement.[92] It makes no mention of the rights of the customer that Vodacom must obtain the authorisation for each sharing occasion;[93] that the customer must determine the conditions,[94] and that it is only subject to these conditions the data may be shared with the third party;[95] and that the customer determines and specifies who the third party is that must receive the information.[96] The customer is not informed in terms of the process set out under RICA that Big Data analytics will be used to share and process RICA Data to advertise products and services to the customer, based on the personal profile of the individual. The online terms and conditions do not seem updated since the Azure platform announcement. The customer is not informed, and no reasonable means are taken, except for the media releases and annual reports, to ensure the customer knows his or her rights under the Written Authorisation Requirement. The customer is simply informed, without being consulted how RICA Data will be treated and the MNO is unilaterally setting the terms. RICA clearly anticipates a scenario where there is a dialogue, at an individual level, where the customer knows their rights, and is in an equally powerful position to dictate terms about how RICA Data may be shared. The intention of RICA is not that the MNO dictates wat it considers as PI, but the customer decides what RICA Data must be shared. In other words, the customer must give the permission as to the type, nature, volume and the frequency of the information to be shared. In doing so, the customer has the casting vote about what RICA Data is personal to share and what RICA Data is not. It is not up to the MNO to decide, on behalf of the customer and thereby disempower the customer. RICA intends that the customer asserts his or her rights and be the one that makes the first and final call. Under these circumstances, the four elements of the Written Authorisation Requirement have arguably not been met. The OTT service provider need not concern themselves with these types of legal interpretation issues, and whether failure to comply with the four Written Authorisation Requirements under RICA would attract regulatory scrutiny when deciding to fully participate in the digital economy. This is a clear indication of the regulatory asymmetry that places a heavier regulatory burden on the MNO.

---

[91] RICA s 14. In terms of Bellovin et al, a URL may be the contents of a communication under USA law. This question is worth pursuing under South African law, based on the extent to which URLs may be disclosed to third parties and law enforcement agencies.
[92] RICA s 14.
[93] RICA s 14.
[94] RICA s 14.
[95] RICA s 14.
[96] RICA s 14.

As discussed in Section I, it would appear as if an MNO like the Vodacom Group does not fully comply with the existing RICA regulatory requirement, but instead continues with deploying digital products and services using the information related to the customer concerned and sharing it with third parties, to meet its future strategies of taking advantage of the digital economy. This seems to be done with the risk of non-compliance in mind, but with little evidence that the regulatory burdens are being met and addressed, no matter how cumbersome, or that the onerous burdens are being addressed with the regulators or that any good faith effort is made to try and ensure minimal compliance or material compliance, at the least. It may be because the compliance burden is too heavy to bear, or it may be a calculated decision to deal with allegations of non-compliance when they are raised and that not moving forward under the standard terms and conditions is too prejudicial a business decision to make and the risks of non-compliance may be worth taking. Section VI analyses the relationship between economic regulation and the regulatory asymmetries under RICA and POPIA.

VI. The Relationship Between Economic Regulation and the RICA Written Authorisation and POPIA Consent Regulatory Asymmetry

RICA and POPIA outline legal requirements and limitations regarding privacy and cybersecurity about law enforcement and about the digital economy. RICA and POPIA are therefore not your traditional economic regulation instruments. RICA and POPIA are regulatory instruments that encourage participation in the digital economy, but at the same time sets out restrictions under which such participation should take place. As such, RICA and POPIA impact the digital economy and this impact is one of an economic regulatory nature – the Written Authorisation Requirement imposes privacy regulations directly on private and public entities to collect and use RICA Data and PI to create and offer digital services. This indirectly modifies the economic behaviour of these business – how they collect and share RICA Data and PI. The aim is to ensure digital services are created and delivered in a secure environment that respects privacy and allows the business to still function effectively and profitably. Privacy and cybersecurity has become a serious economic regulatory issue, acting like a gatekeeper for access to the digital economy and to fully participate therein. The Written Authorisation Requirement is a measure that indirectly influences the economic behaviour of the MNO to reach the desired public interests aim of obtaining customer approval and to prevent the misuse of customer RICA Data. This is so even if hefty legal fines and criminal offenses are not used to influence the behavior of the MNO, under the No-COE Phenomenon.

The following are the ways in which RICA potentially impacts the digital economy:

- The written authorisation under RICA allows the MNO to use RICA Data that is originally collected for law enforcement purposes, for other purposes. These other

purposes include the commercial interests of the MNO, such as sharing the RICA Data with third parties, to research and create new digital services, and to improve existing digital services;

- The non-enforceability of the Written Authorisation Requirement, under the No-COE Phenomenon can be seen as creating a fine balance between the requirement to obtain the written authorisation and to share the data about the customer with third parties, to fully participate in the digital economy, without fear of alleged misuse of RICA Data. To indirectly permit the use of RICA Data, the Written Authorisation Requirement is not enforced by means of a guilty offence clause – the MNO will not be guilty of an offence if it does not comply with the Written Authorisation Requirement.[97] Looking at the state of digital services in SA, looking at the standard terms and conditions and the privacy policies and practices of the MNO, these illustrate how the MNO has implemented the use of RICA Data with little fear for regulatory intervention. The absence of a penal element creates some sort assurance that if the MNO does not comply, there would be no legal consequences. As such, the standard terms and conditions and privacy policies do not make any reference to the written authorisation under RICA. The Written Authorisation Requirement is ignored, and no serious attempt is made to try and comply with it, as there is no real fear of regulatory intervention; and

- POPIA clearly recognises the need to participate in the digital economy and encourages the MNO and OTT service provider to fully participate. As with RICA, POPIA aims to strike a balance between economic needs, privacy and security. POPIA recognises and therefore emphasises the need for economic progress within the framework of the information society.[98] POPIA is based on the philosophy that economic progress requires the removal of unnecessary impediments to the free flow of information [99] and also to make the constitutional right of privacy, limited to justifiable limitations – accepting that privacy is not an absolute right.[100]

Section VII discusses various regulatory impact scenarios and speculates as to why the MNO may have adopted this approach, to participate more effectively in the digital economy as opposed to choosing to comply with a burdensome legal requirement lacking enforcement.

VII. Discussion and Analysis: The Likely Impact of the RICA Cybersecurity and Privacy Regulatory Asymmetry on the Digital Economy

[97] RICA 2003 s 50(2).
[98] POPIA Preamble.
[99] POPIA Preamble.
[100] POPIA Preamble.

The MNO will be legally constrained to fully participate in the digital economy to the extent it voluntarily chooses, or to the extent that it is forced to comply with the unenforceable Written Authorisation Requirement. The overall question is how this regulatory model theoretically impacts digital innovation: Are MNO's unfairly restraint to take advantage of the digital economy – to build platforms, and content services, in partnerships, using RICA Data?

A. The Written Authorisation Requirement May be too Restrictive to Comply With

The Written Authorisation Requirement is a legal requirement and must be complied with, strictly speaking. However, this legal requirement is not without its challenges. The business strategies of the MNO and the need to diversify operations, given the cannibalization of its voice and SMS services, is further exasperated by the additional requirement to obtain the written authorisation and to share RICA Data as per the conditions set by the customer. Attempting to comply with the Written Authorisation Requirement may be too burdensome financially. The MNO's digital service plans may be delayed by having to obtain the conditions and determinations of the customer individually; to negotiate with every single customer; by having to accommodate the conditions of the customer; and by running the risk of discriminating between customers with the individually tailored agreements. This may be worsened by the impact on efficiencies and the delays caused in rolling out services; the labour costs to address the demands of the customers; the costs incurred as a result of having to comply; the delays to enter into third-party partnerships; the inability to present a standardise business case; dealing with unreasonable demands of customers; the hi-jacking of the business operations and being held hostage by the customer. The impracticality of obtaining the written authorisation and to cater for the diverse conditions of millions of individual customers may probably be the reason why the OTT service provider is rightly not burdened with this additional obligation. The Written Authorisation Requirement may make it impractical and create an environment where the individual customer, or small group of demanding customers are potentially stronger and has leverage over the MNO and can strong-arm the MNO. The standard popular business plan, that is viable may be prejudiced while trying to cater to the exclusive tastes of a customer that does not fit the mold. The legal requirement may be too burdensome that no reasonable MNO can comply with it. The written authorisation may therefore be unworkable and continue to subject the MNO to potential legal risks, that any consumer association and privacy protection association may legally challenge the MNO for.

B. Potential Deliberate Non-Compliance by the MNO to Participate in the Digital Economy

The MNO will be legally constrained to fully participate in the digital economy, to the extent it voluntarily chooses, and to the extent it is forced to comply with the unenforceable Written Authorisation Requirement. The decision may be based on the extent to which the Vodacom Group's Vision 2020 strategy may be impacted. The MNO is left with the discretion whether to comply, but not face any legal consequence for not complying. The legal requirement is

clear that the Vodacom Group must obtain the written authorisation of its customers to use their RICA Data as part of its Vision 2020 strategy. In deciding how to comply with the Written Authorisation Requirement, the MNO may take the calculated decision to comply as best they reasonably can, and that may mean the standard terms and conditions and the accompanying privacy policies. The greater risks of not rolling out a digital strategy that shares RICA Data, may mean continued revenue losses to the MNO. Not acting in the face of such competition to try and retain customers, may not be wise, and so the MNO may be pushed into a corner to adopt the digital strategy, and collect to share customer data. Instead of adopting zero rated OTT service packages from the OTT service provider, the MNO may choose to disregard the Written Authorisation Requirement altogether and launch its digital innovation and third party sharing strategy.

Having no written authorisation requirement to comply with would enable the MNO to seriously consider developing its own OTT services, enter into partnerships to develop OTT services, enter into mergers and acquisitions to start-up data processing companies or commercially share RICA Data with third parties that may process RCA Data to research and develop innovative products and services. The MNO is losing out on the opportunity to diversity its business in the mobile ecosystem effectively, and to advance digital services and the digital economy, and enter into revenue sharing arrangements. It however does not seem as if the Vodacom Group attempted to comply with the Written Authorisation Requirement. Its privacy policies and standard terms and conditions make no reference to the Written Authorisation Requirement. The MNO is forced into a corner to either innovate or comply with the Written Authorisation Requirement. MNO's may rather opt not comply with the legal requirements, in an effort to advance the digital economy. This sort of action may be incentivized by the lack of enforcement of non-compliance under the No-COE Phenomenon.

C. Customer Awareness and Customer Demands

The regulatory asymmetry is an uncomfortable position for the MNO to be in. The customers may start to demand that they be consulted and that their written authorisation be obtained prior to sharing their RICA Data, as per the four elements under the Written Authorisation Requirement.

The MNO customer may become aware of their rights as per the MNO RICA-POPIA Double Decker Requirement, and object to the use and the sharing of their RICA Data to third parties they did not authorise. The customer may start to demand their rights be respected. The MNO is left to negotiate these potential risks. The MNO's innovation plans may therefore indirectly be held 'hostage' by the customer. This may negatively impact the plans of the MNO to fully partake in the digital economy.

D. The Regulatory Asymmetry Creates Ethical Dilemmas of Self-Regulation

The non-enforcement of the Written Authorisation Requirement and the theoretic nature of the RICA Written Authorisation and POPIA Consent Regulatory Asymmetry means: the

MNO and the OTT service provider may practically continue to collect and use RICA Data about its customers in the same manner as it has always done. However, as corporate citizens, that must act ethically, under the King IV Code, where companies must act ethically and establish ethics committees even when not required by law,[101] the MNO may need to act ethically and incorporate the Written Authorisation Requirement n its privacy policies, standard terms and conditions and cybersecurity risk assessment and risk management policies. Given the delayed implementation of the consent requirement under POPIA, the unenforced Written Authorisation Requirement is practically a self-regulatory system. There are no strictly enforced regulations against the MNO and there are no regulations enforced against the OTT service provider. The MNO and OTT service provider solely dictate the terms and conditions and privacy policies under which they provide their services and based on that collect and share data about the customer. It is basically an 'honor system' or a 'trust system' of cybersecurity and privacy governance. The MNO is trusted act ethically, to be bound by its honour and comply with the Written Authorisation Requirement, and not to betray the trust bestowed on it, even if no legal penalty may be enforced.

It may be paradoxical to expect the MNO to obey a law from which the MNO is expressly excused from legal liability. As such, to choose whether to obey a legal requirement for which there are no consequences, the MNO is likely to place its digital economy interests above those of the privacy and data protection interests of the customer. The MNO is trusted to do the right thing while faced with a clear conflict of interest, without any external and independent legal enforcement to ensure oversight and compliance. Ethics and governance is about doing the right thing even when there is no real enforcement and no legal penalty hanging over the head of the MNO. What complicates matters for the MNO is the tough situation the MNO faces under the OTT Wars. The regulatory asymmetries create ethical dilemmas: Should the MNO continue to innovate and ignore customer rights to protect its falling revenues and to remain relevant, or inform the customers of their rights and enforce these rights?

E. The MNO may be Subjected to Accept Zero Rated OTT Services from the MNO

Stork et al., described that the MNO may adopt the strategy of accepting zero rated products from the OTT service provider to minimise the effect of revenue losses.[102] The Vodacom Group followed the music streaming model[103] but identified the risks of not being able to effectively compete in the digital content space because of lack of access to content at reasonable rates.[104] This may have led the Vodacom Group to adopt its vision to be the leader

[101] PWC, 'Governing structures and delegation – A comparison between King IV TM and King III', April 2017, Pg. 30 <https://www.pwc.co.za/en/assets/pdf/king-iv-comparison.pdf>
[102] Christoph Stork Steve Esselaar Chenai Chair, 'OTT - Threat or opportunity for African MNOs?' *Telecommunications Policy*, Volume 41, Issues 7–8, August 2017, Pages 600-616 <https://doi-org.wwwproxy1.library.unsw.edu.au/10.1016/j.telpol.2017.05.007>
[103] Vodacom. (2016). Deezer. http://www.vodacom.co.za/vodacom/services/deezer (Accessed 11 February 2016).
[104] Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 23 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

in the digital space. The Written Authorisation Requirement may be too cumbersome to comply with and compound the MNO's response strategy to revenue losses attributed to OTT services. The Written Authorisation Requirement may therefore have the indirect effect of also subjecting the MNO to accept packages of zero rated OTT services from the OTT service provider. Under these circumstances the Written Authorisation Requirement may not be creating an enabling environment for digital innovation where the MNO may share RICA Data with third parties for digital innovation.

F. The Regulatory Asymmetry Dilemma

The RICA Written Authorisation and POPIA Consent Regulatory Asymmetry has the effect of placing the MNO and the OTT service provider in unequal theoretical positions. In an almost conflicting way, the MNO and the OTT service provider are practically placed in positions where they can participate in the digital economy with little to no fear of regulatory enforcement that may stifle innovation. On the one part the MNO can participate because it cannot be held legally accountable for any misuse or unauthorised sharing of RICA Data. This enables the MNO to innovate. However, the MNO is left with regulatory uncertainty as informed customers may rebel and lobby for regulatory action, that may have a chilling effect on the plans of the MNO. The OTT service provider has no worries of this nature and may fully innovate and participate in the digital economy as it has always done, unchecked and not being supervised by any regulatory measure. The lack of supervision allows the OTT service provider to innovate with no restriction. The poor supervision over the MNO also allows the MNO to innovate, but to be weary of potential customer demands and consequent regulatory intervention at the same time. This is a regulatory asymmetry that creates regulatory uncertainty for the MNO and non-regulatory certainty for the OTT service provider. The MNO also needs regulatory certainty, just as the OTT service provider, to fully partake in the digital economy, without fearing that any unpredictable regulatory intervention may forthcoming.[105] The Written Authorisation Requirement may remain on the law books indefinitely and will continue to exist when POPIA comes into force, complicating the regulatory pressure on the MNO, seeking to innovate and be a leader in the digital innovation space. Regulatory uncertainty has a negative impact on investments in the digital economy and must be addressed.

VIII. Conclusion and Recommendations

This paper investigated the nexus between privacy, security and competition in the digital economy between the MNO and the OTT service provider. The paper critically analysed the Written Authorisation Requirement imposed by RICA, which states third-party data sharing requires the prior written authorisation of the customer. This requirement is solely imposed on the MNO and not on the OTT service provider. This creates regulatory asymmetry, imposing an unfair regulatory burden on the MNO facing competition from the OTT service

[105] POPI s 11(1) (i)(*a*)

provider that is replacing traditional communication services. The RICA requirement is not imposed on the OTT service provider. This situation creates an environment that makes it challenging for the MNO to compete with the OTT service provider by partnering with third parties, share RICA Data and to innovate and advance the digital economy. The MNO may find it challenging to comply. The MNO may however choose not to comply as compliance may result in not being able to share RICA Data, given that the customer is allowed to set conditions for the sharing of RICA Data. Instead the MNO may disregard the Written Authorisation Requirement, especially given that the Written Authorisation Requirement is not enforced. The privacy policies of the MNO do not make any reference to the Written Authorisation Requirement. The Written Authorisation Requirement may negatively impact digital innovation, given how onerous it is to comply with. All these factors make it challenging for the MNO to fully adopt digital innovation strategies, without having to disrespect the law. The MNO is left with the ethical dilemma to either disregard the law or strife to innovate and advance the digital economy. This is not an environment that encourages innovation nor respect for the rule of law. As such, the Written Authorisation Requirement, which will continue to exist after POPIA is enacted, will continue to pose unfair compliance obligations on the MNO. The Written Authorisation Requirement needs revisiting to create a fair, predictable and enabling environment for the MNO and the digital economy. This revision may need to be based on future empirical research.

IX. References

Gregory, A., (2011), "Data governance — Protecting and unleashing the value of your customer data assets", *Journal of Direct, Data and Digital Marketing Practice,* Vol.12, No. 3, pp. 230-248 <10.1057/dddmp.2010.41>.

ASIC. (2017), "Cyber resilience good practices", available at: <https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/> (accessed 2 August 2017).

Battersby, L., "Telstra offers signal boost - at a price", The *Sydney Morning Herald* (online), 6 July 2012 available at: <http://www.smh.com.au/business/telstra-offers-signal-boost--at-a-price-20120706-21l5f.html#ixzz4CfNVD8QF> (accessed 13 April 2016).

Electronic Communications and Transactions Act 25 of 2002.

Evidence by Prof Alison Gillwald, Executive Director, Research ICT Africa, to the Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Evidence by Mr Paul Hjul (Director, Crystal Web), Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Evidence by Mr Graham De Vries, General Manager: Regulatory Affairs, MTN, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Evidence by South African Communications Forum on Over-the-Top services in South Africa Ms Loren Braithwaite-Kabosha, SACF CEO, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Evidence by Vodacom submission on Over-the-Top services in South Africa
Dr Andrew Barendse, Vodacom Managing Executive: Regulatory Affairs, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Evidence by Mr Graham McKinnon, Chief Legal Officer, Cell C and Dr Andrew Barendse, Vodacom Managing Executive: Regulatory Affairs, Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Facebook, Terms of Service, 19 April 2018 <https://www.facebook.com/legal/terms/update>

Federal Financial Institutions Examination Council (FFIEC), (May 2017), "FFIEC Cybersecurity Assessment Tool", available at: <https://www.ffiec.gov/%5C/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf> (accessed on 7 June 2018).

Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, New York Times, 'Facebook Gave Device Makers Deep Access to Data on Users and Friends', 3 June 2018 https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html

Gillwald, Alison, Presentation, 'OTT', Research ICT Africa and University of Cape Town, Parliamentary hearing on OTT services, Cape Town, 26 January 2016 < https://researchictafrica.net/presentations/Presentations/2016_Gillwald_Presentation_Parliamentary_Portfolio_Committee_Hearing_on_OTT_Services.pdf>

Google, GOOGLE PRIVACY POLICY May 25, 2018 <https://policies.google.com/privacy>

He, Y., Yu, F. R., Zhao, N., Yin, H., Yao, H., Qi, R. C. (2016), "Big Data Analytics in Mobile Cellular Networks", in *IEEE Access*, Vol. 4, pp.1985-1996.
ISO/IEC. (2013), "Information technology – Security techniques – Governance of Information Security".

Information Regulator, 'Alleged Cambridge Analytical Data Breach – Facebook', 10 APRIL 2018, MEDIA STATEMENT <http://www.justice.gov.za/inforeg/docs/ms-20180410-facebook.pdf>; Mybroadband, 'Cambridge Analytica got data of Facebook users in South Africa,' Staff Writer7 April 2018 <https://mybroadband.co.za/news/security/255103-cambridge-analytica-got-data-of-facebook-users-in-south-africa.html>

ISO/IEC. (2015), "Information technology — Governance of IT for the organization. International Standard", Second edition <https://www.saiglobal.com/online/Autologin.asp?url=/online/Script/Search.asp%3FSearchType%3Dpublisheronly%26Db=ISO>.

Mayer, J., Mutchler, P. and Mitchell, J. C., (2016), "Evaluating the privacy properties of telephone metadata", *Proceedings of the National Academy of Sciences of the United States of America* Vol 113 No 20 pp. 5536-5541.

Memorandum on The Objects of the Cybercrimes And
Cybersecurity Bill, 2017
<http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.pdf>

MTN Proprietary Limited, 'Terms and Conditions' 2017, section 7
<https://www.mtn.co.za/Pages/Termsandconditions.aspx?pageID=26>

Microsoft, Microsoft Azure 2018 <https://azure.microsoft.com/en-us/services/app-service/>

NIST. (2018), "Framework for Improving Critical Infrastructure Cybersecurity", available at: < https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (accessed 2 May 2018).

Portfolio Committee on Justice and Correctional Services, DATE: 26 February 2018 CYBERCRIMES AND CYBERSECURITY BILL <https://www.ellipsis.co.za/wp-content/uploads/2017/11/180228Clause_by_Clause_Deliberation_Bill.pdf>

Parliamentary Monitoring group, 'Over-the-Top (OTT) policy and regulatory options, Telecommunications and Postal Services, Meeting Summary' 26 January 2016 <https://pmg.org.za/committee-meeting/21942/>

Protection of Personal Information Act, 2013.

Protection of Personal Information Act, 2013 (Act No. 4 OF 2013): Regulations Relating To The Protection Of Personal Information, 2017. GG 4115, GoN 709, * September 2017 <http://www.justice.gov.za/inforeg/docs/InfoRegSA-RegulationsDraft-Aug2017.pdf>

PWC, 'Governing structures and delegation – A comparison between King IV TM and King III', April 2017, Pg. 30 <https://www.pwc.co.za/en/assets/pdf/king-iv-comparison.pdf>

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

Seixas, P. (2015). ITU-ASEAN forum on over the top Services: Business, policy and regulatory trends. In Presentation at Phnom Penh. 8–9 December 2015. <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/Dec-OTT/Presentations/Phnom%20Penh%20%20Session%205%20-%20OTT%>

Shanapinda, S., (2016a), "Retention and disclosure of location information and location identifiers" *Australian Journal of Telecommunications and the Digital Economy* Vol 4 No 4, pp. 251-279 <http://dx.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,* Vol. 35 No. 3, pp. 17-19.

Stork, Christoph; Esselaar, Steve and Chair, Chenai, 'OTT - Threat or opportunity for African MNOs?' Telecommunications Policy, Volume 41, Issues 7–8, August 2017, Pages 600-616 <https://doi-org.wwwproxy1.library.unsw.edu.au/10.1016/j.telpol.2017.05.007>

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>

Trencadis Innovación, S.L. (2018) available at: <http://www.trencadis.es/en/products/gradation/> (accessed 9 June 2018).

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication (AJIC), 20, 113-132. <https://doi.org/10.23962/10539/23573>

Vodacom, Privacy Policy <http://www.vodacom.co.za/vodacom/terms/privacy-policy>

Vodacom, Vodacom App Store Ts & Cs < https://myvodacom.secure.vodacom.co.za/vodacom/terms/vodacom-app-store-terms-and-conditions>

Vodacom. (2016). Deezer. http://www.vodacom.co.za/vodacom/services/deezer (Accessed 11 February 2016).

Vodacom Group, 'Vodacom accelerates digital transformation with first-to-market launch of suite of Azure solutions' Press release, Wednesday, 18 April 2018 <http://www.vodacom.com/news-article.php?articleID=4472>;

Vodacom, 'Best technology' <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/best-technology.php>; Vodacom Group Limited Integrated Report 2017 pg.24 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>.

Vodacom Group Limited Integrated report for the year ended 31 March 2017, Pg. 23 <http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated-hires.pdf>

von Solms, B., von Solms, R., (2018), "Cybersecurity and information security – what goes where?", *Information & Computer Security*, Vol. 26 Issue 1, p. 2-9, 6 [2.3], available at <https://doi.org/10.1108/ICS-04-2017-0025>.