



Routledge
Taylor & Francis Group

UNISA

Communicatio

South African Journal for Communication Theory and Research

Routledge
Taylor & Francis Group

ISSN: (Print) (Online) Journal homepage: <https://www.tandfonline.com/loi/rcsa20>

Cyber-ethics for NGOs during Covid-19: The Eight “Ethical Variables” and a Microsocial Contract

Adelina Mbinjama

To cite this article: Adelina Mbinjama (2022) Cyber-ethics for NGOs during Covid-19: The Eight “Ethical Variables” and a Microsocial Contract, *Communicatio*, 48:1, 45-65, DOI: [10.1080/02500167.2022.2058040](https://doi.org/10.1080/02500167.2022.2058040)

To link to this article: <https://doi.org/10.1080/02500167.2022.2058040>



Published online: 30 Jun 2022.



Submit your article to this journal [↗](#)



Article views: 2



View related articles [↗](#)



View Crossmark data [↗](#)

Cyber-ethics for NGOs during Covid-19: The Eight “Ethical Variables” and a Microsocial Contract

Adelina Mbinjama

<https://orcid.org/0000-0003-2899-0707>

Cape Peninsula University of Technology, South Africa

mbinjamaa@cput.ac.za

Abstract

Jürgen Habermas’ theory of communicative action and discourse ethics as a theoretical basis merges several factors that have an impact on the use of digital media by internet users. This article provides a qualitative narrative analysis of a study of five South African-based non-governmental organisations (NGOs) on their experiences with digital media and cyber-ethics during the Covid-19 pandemic. The author interviewed employers and digital media specialists from the NGOs about their experiences with the “eight ethical variables”, namely, justice, privacy, access, accuracy, truth, human dignity, regulation, and ownership of information, during the global Covid-19 (acronym for the coronavirus disease of 2019) pandemic. The article discusses how the NGOs have been affected by the increasing use of digital media. The article argues that a need exists for a framework of cyber-ethics for self-regulation purposes, to be followed by NGOs to deal with breaches of ethical conduct. Finally, the formulation of a microsocial contract based on the proposed eight ethical variables is offered. The present study contributes to media ethics literature by proposing a framework for ethical conduct for digital media use. This is of importance to internet users and may be achievable if imbedded in employee procedural policies and public policies. It is argued that in formulating appropriate ethical guidelines, Habermas’ discourse ethics should be kept in mind for an optimal microsocial contract to be attainable.

Keywords: Covid-19; cyber-ethics; digital; non-governmental organisation; self-regulation; contract

Introduction

A media commentator recently remarked that: “Cyber attacks don’t just impact the internet, they threaten lives offline too” (Heilweil 2019). Cyber-attacks and cyber-related crimes have been increasing as the use of the internet for business and entertainment purposes has become more widespread. Heilweil (2019) reports that the Cyberpeace Institute, a Microsoft-backed non-governmental organisation (NGO) based in Geneva, Switzerland, is working with volunteers to assist civilians who are victims of cyber-attacks by investigating the attacks, and by promoting norms and international laws for responsible cyber behaviour. Digital media, including social media, are becoming increasingly popular in the NGO sector across the world (Hall, Schmitz and Dedmon 2020; Kenix and Abikanlu 2019). As digital media platforms are popular among adult internet users for both business and private applications, it is not surprising that NGOs rely on these platforms to promote their products and services (Pérez-Seijo and Berta 2020). More particularly, during the current global Covid-19 (acronym for the Coronavirus disease of 2019) pandemic, many NGOs are using digital media platforms to share content about the virus and to raise funds (Sefora and Dabija 2020). Popular media sources recently reported extensive hacking incidents on Twitter that “affected multiple major accounts” (including those of Bill Gates, Apple, Elon Musk, Barack Obama, Kanye West, Uber, Mike Bloomberg, Joe Biden and Jeff Bezos) and “shared out a Bitcoin scam to millions of users” (Ellis 2020).

NGOs are not excluded from the experience of having their emails and cell phone accounts accessed and used without their permission (Reed 2020). According to Mbinjama-Gamatham (2014, 2), these incidents are often dismissed as “cyber-related crimes”. She makes clear the importance of cyber-ethics as an area of research, especially within the NGO sector, beginning with Floridi’s (2002, 123) claim that the question, “What is the nature of right and wrong?” is one of the field questions of cyberphilosophy (Mbinjama-Gamatham 2014, 3). Such statements point to the importance of ethics as a discipline which embraces the concern with people’s desire to do good and their need to avoid morally wrong or harmful behaviours (Macer 2007). Mbinjama-Gamatham (2014, 2) also points out that often the perception is that crimes being committed online are less harmful than those which are perpetrated physically. Furthermore, these incidents are regarded as pranks (Mbinjama-Gamatham 2014, 2). She further explains that “in technical terms, such incidents could be classified as serious breaches of common ethical principles” (Mbinjama-Gamatham 2014, 2).

In the light of the above, it is clear that the increased use of digital media is accompanied by threats to the practice of cyber-ethics and by increased opportunities for cybercrime. Although there has been little academic research on cyber-ethics and the use of digital and social media in the NGO sector globally, there have been a few popular articles on websites, in newspapers and magazines that have touched on this phenomenon. Scholarly contributors in the field of cyber-ethics have written on various ethical problems encountered on the internet, such as those raised by viruses, hackers,

intellectual property and censorship (Gordon 2008; Introna 2005). However, at present there is – as far as can be ascertained – no internationally agreed-upon cyber-ethics code, although the matter has been raised by several authors, and some countries have addressed related issues by means of existing laws (Umejiaku and Anyaegbu 2016). Since Mbinjama-Gamatham's (2014) study, it is still apparent that cyber-ethics as a research area needs to be better explored, especially during periods of crisis such as the Covid-19 pandemic. Through a narrative analysis, the article focuses on contemporary issues and developments related to cyber-ethics and digital media by highlighting [mention the study] the ethical and moral problems encountered by five South African NGOs in their use of digital media communications and cyber-ethics during Covid-19. In terms of theoretical underpinnings, Jürgen Habermas' theory of communicative action and discourse ethics work in critical theory is deemed central to this kind of research as the field of ethics draws from different disciplines and is informed by different cultural perspectives.

Habermas' contributions span a wide range of subjects, including communication, justice, technology and politics (Abbott 2016; Jay 2019; Outhwaite 2013; Sharonova and Beavitt 2020; Wilkinson 2018). Mbinjama-Gamatham and Olivier (2020, 1–2) highlight that Habermas' discourse on ethics closely relates to the need for formulating ethical behavioural frameworks – in this case applicable to dealing with issues relating to cyberspace for a diverse population of internet users. Against the background of an array of recently established organisational workplace rules, the present study addressed a clear gap in media ethics literature. Except for Mbinjama-Gamatham's (2014) contribution, no previous published research has looked into a practical code of cyber-ethics that can be imbedded in either drafted or existing procedural and public policies. However, although Mbinjama-Gamatham (2014, 191–193) proposed social media ethical guidelines for NGOs, such guidelines also need to accommodate broader digital media communications, since NGOs are exposed to multimedia platforms.

My argument in the article is that there is a need for a better understanding of the possibilities to address the problem of formulating behavioural guidelines – in particular when such guidelines draw from Habermas' theory of communicative action and discourse ethics. The study from which the article has drawn thus offered a code of cyber-ethics derived from and extending Mbinjama-Gamatham's (2014) understanding of the eight ethical variables, namely, justice, privacy, access, accuracy, truth, human dignity, regulation, and ownership of information.

Theoretical Perspective and Methodology

The relevant literature (Ali 2019; Jaishankar 2020) indicates that several challenges arise from communicating on digital media. However, Mbinjama-Gamatham and Olivier (2020, 1) confirm the value of Habermas' theory of communicative action and discourse ethics to address contemporary ethical challenges. Mbinjama-Gamatham and Olivier (2020, 15) claim that better decisions about right or wrong are facilitated by

communicating, or discoursing, about such issues. They explain that in reference to Habermas, it seems valuable to address his concept of “communicative action” (Habermas 1987, 62–76). Amongst other things, communicative action includes the practice of interpersonal communication with a view to action undertaken with no hidden validity claims, as opposed to instrumental or strategic action (Habermas 1987, 47, 196, 209, 279). The latter position represents the countervailing action of (mis-)communicating disingenuously, that is, with a hidden agenda and typically with intent to wield power over unsuspecting interlocutors (Mbinjama-Gamatham and Olivier 2020, 15).

Mbinjama-Gamatham and Olivier (2020, 15) claim that

discourse ethics are important because, even if one cannot ever reach a point where the ethical, moral or non-criminal behaviour of people can be *guaranteed* – and it should be clear why it cannot; arguably every person ‘chooses’ for himself or herself what to do in every situation where they have an ethical or moral choice, whether this is on voluntaristic-cultural or partly genetically-determined grounds.

They state that one option is to provide guidance through education and/or providing, for example, an ethical code. Practically, grounds and reasons for communicative actions are needed (Mbinjama-Gamatham 2020, 15–16). In addition, information that could make a difference to the outcome of the communication between different parties is not to be intentionally withheld.

Digital media enables the networking of individuals and groups together, although such ability often has serious consequences that threaten the preservation of cyber-ethics and increase cybercrime. Mbinjama-Gamatham (2014, 15), as pointed out earlier, argues that a theoretical framework such as Habermas’ theory of communicative action and discourse ethics might better explain and operationalise terms such as “cyber-ethics” and “cybercrime”. In the cyberworld and in modern times, Habermas’ reference to strategic action is clearly relatable to cybercrimes (Mbinjama-Gamatham 2014, 15–18).

Mbinjama-Gamatham (2014) identified eight ethical variables, based on the relevant literature and, in particular, on the Habermasian perspective of communication (Habermas 1984; 1987; 1990). However, her 2014 study was limited to the communication problems experienced while on social media by 10 selected South African-based NGOs. Thus, in 2020–2021, the present study allowed a new set of 10 participants from the NGO sector to comment on and make suggestions for the formulation of a microsocial contract based on the “eight ethical variables” (also referred to as “eight ethical principles”) offered to the sector. Ten participants from five South African-based NGOs gave ethical consent to participate in the study on the ethical framework and use of digital media during Covid-19. One employer and one digital media specialist from each NGO were interviewed telephonically. A deductive method for narrative analysis was used by presenting an initial set of codes to the participants and then drawing narratives from their responses. In support of the findings, the study

analysed contemporary issues reported by South African NGOs and their experiences with cyber-ethics and digital media during Covid-19.

The relevance of drawing from Habermas' conceptual-theoretical work for consideration of cyber-ethics is supported by Finlayson (2005), who claims that Habermas and other social scientists before him were interested in the question of how social order is possible (see also Mbinjama-Gamatham and Olivier 2020, 14). Employing Habermas' paradigmatic stance of critical theory as a theoretical lens supports Feenberg (1991, 1) who points out that "critical theory of technology is concerned with the threat to human agency posed by the technocratic system that dominates modern societies". Critical theory of technology emphasises certain themes derived from the Frankfurt school of thought, often associated with Marxism, pragmatism, Heideggerian phenomenology and various theorists of rationality in modern culture (Feenberg 1991, 1–2).

Therefore, the present article drew from a qualitative narrative analysis of participant interviews and consideration of reviewed published work on cyber-ethics in digital media for NGOs in South Africa during Covid-19. A critical analysis of relevant narratives revealed categories of contemporary digital media issues pertaining to South African NGOs relating to the proposed eight ethical variables.

Conceptual Understanding of the Eight Ethical Variables for Digital Media

Pompon (2020) mentions that the World Economic Forum declared that cybersecurity matters currently more than ever before due to the Covid-19 pandemic. He explains that globally cybercriminals are taking advantage of this opportune period where people's reliance on digital tools has increased significantly. Recent popular media and academic literature on NGOs and cyber-related issues (Nchabeleng, Botha and Bisschoff 2018) indicates that the eight ethical variables proposed by Mbinjama-Gamatham (2014) are very relevant in the context of the Covid-19 pandemic, which has forced most organisations to operate remotely and increase the time spent on the internet. The article will discuss briefly the eight ethical variables (drawn from Mbinjama-Gamatham's 2014 study and more recent developments), legislation and Covid-19 measures to emphasise a number of concepts and accompanying ethical issues that confront internet users when using cyberspace. Although Pompon (2020) emphasises the need for increased cybersecurity during the pandemic, such measures cannot be faultless in and of themselves. Internet users also have to take precautionary measures while working on digital media platforms.

Justice

Mbinjama-Gamatham (2014, 4, 54) points out how “justice” refers to the way in which individuals on digital media uphold the law of the internet/social sites in order to conduct themselves uprightly and promote good behaviour and treatment towards others. This ethical principle is also contextualised to describe the way individuals are treated online (whether well or badly) and describes what happens when an individual is found guilty of committing cybercrimes. Relevant considerations include: Is the judgement and treatment towards the cybercriminal fair and reasonable? Is the judgement and treatment consistent with other states? Behaviours or actions on digital media must promote moral good and equality. “Justice” also refers to individuals’ knowledge of cyber-ethics and the law of the internet. Thus, the term includes reference to the common laws, which are, or can be, affected by digital media. This means that media and communications legal instruments fall under this category.

In order for justice to prevail, it would require collective agreement on what is considered immoral and unethical online. Currently, the justice that is required when criminal activities occur is not easily guaranteed as there are few collective agreements about what should be done to safeguard individuals from cybercrime. In response to the problem of accuracy and authentic information being shared on digital media, the then Acting Minister of Communications and Digital Technologies, Jackson Mthembu, warned South Africans that users have been arrested for spreading fake news or disinformation about Covid-19 and, should users continue to do so, they should expect it to be regarded as a punishable offence (SANEF 2020). The 10 participants from the NGOs felt that the full effect of the Protection of Personal Information Act 4 of 2013 (POPIA) (SA 2013) is a good way to get people to take responsibility for their online activities. They also indicated that issuing fines of up to R10 million or facing jail time for up to 10 years for breaking the POPIA is reasonable as NGOs also tend to be victims and perpetrators of online crime during the pandemic.

Privacy

A globalised and networked world presents many questions regarding privacy. Contextually, “privacy” refers to the privacy issues found on digital media. For example, the way in which an individual’s private information is exposed on the internet is a privacy issue. “Privacy” relates to the user’s privacy settings on digital media platforms and any problems that pertain to user confidentiality. The term can also relate to the way in which internet users practise anonymity online. According to Bizcommunity.com (2020a), Trend Micro reported that since January 2020, approximately one million spam messages have been linked to Covid-19, and the World Health Organization stated that during April 2020 there was a five-time upsurge in cyber-attacks compared to the same time in 2019, the focus being the increase in funding opportunities created by the pandemic. Amplified monetary gains made available through these funding initiatives became a drawcard for cybercriminals. Consideration

of the many ways in which individual users' data privacy is breached pinpoints potential threats to privacy for NGOs and other organisations.

The narrative analysis of the five digital media specialists revealed that they were aware that, in South Africa, the Electronic Communications and Transactions Act 25 of 2002 (SA 2002), the Consumer Protection Act 68 of 2008 (SA 2008) and the POPIA recognise and regulate contracts concluded online. Three of the five digital media specialists from the selected NGOs mentioned that, especially prior to Covid-19, sections of the legislation did not cover aspects that were specific to the cyberworld since the legislation was primarily aimed at traditional media and offline activities.

The managers of the NGOs referred to the POPIA (which came into full effect on 1 July 2021), and had a general understanding of how personal information is lawfully processed. The conditions outlined in the legislation and how personal information is regulated are equally important in addressing how the codes of conduct are issued by the Information Regulator. Other aspects to consider include procedures for dealing with complaints; provisions for regulating direct marketing by unsolicited electronic communication; and the enforcement of the POPIA (Van de Coolwijk 2020). These changes in the POPIA apply to public organisations (including NGOs), private organisations and individuals in various South African sectors.

Access

"Access" relates to the way in which internet users enter, exit, communicate with, or make use of digital media. Some examples would include issues of user-friendliness, making updates on digital media, and tools and applications to assist with access on digital media platforms. Generally, this term refers to what a user does on digital media. Personal devices, such as mobile phones and laptop computers, are being used during the Covid-19 pandemic with most employees working remotely. This presents opportunities for cybercriminals as they are aware most users are not as tech savvy as the organisations' information technology (IT) specialists that provide security measures. While the POPIA aims at protecting the personal information of internet users, it simultaneously conscientises people to behave responsibly and to be accountable for retrieving, sharing and storing data that is compromised. Tee (2021) explains that sections 110 and 114(4) of the POPIA only came into effect on 1 July 2021 as these sections relate to the modification of laws and the actual transfer of functions of the Promotion of Access to Information Act 2 of 2000 (PAIA) (SA 2000) from the South African Human Rights Commission to the Information Regulator. Tee (2021) also points out that a fine of up to R10-million and jail time of up to 10 years can be imposed, depending on the seriousness of the breach of the POPIA. The findings of the present study revealed that the digital media specialists were participating in drafting PAIA manuals to make employers aware of the intrinsic nature of the POPIA and likely repercussions of not complying with it. The contents of the PAIA manual should be prepared within the context of the organisation and should be congruent with the POPIA. This should result in an integration of ethical guidelines for companies and

organisations to adhere to, in the interest of their internal and external stakeholders. According to Tee (2021), having a PAIA manual does not mean that an organisation is POPIA compliant. Of the five NGOs that participated in the study, three had drafted their PAIA manuals and intended to publish them on their digital media platforms such as websites, social media and other technostructures found on the internet.

Accuracy

“Accuracy” refers to the extent to which the content presented on digital media is deemed correct, as well as to the way in which users are able to perform tasks on digital media with precision. The verification of content and the ability to be accurate on social and digital media platforms are relevant here. To curb fake news during Covid-19, NGOs such as the South African National Editors’ Forum (SANEF) (2020) have partnered with the government and the private sector to monitor and respond to misinformation and fake news. According to SANEF (2020), the collaboration is between the Government Communication and Information System, Media Monitoring Africa and the CovidComms volunteer communication network. SANEF (2020) reports that the initiative is in line with the work of a distinct ministerial task team established by the Department of Communications and Digital Technologies. These include the Independent Communications Authority of South Africa (ICASA), the Film and Publications Board (FPB), ZADNA, mobile phone companies, stakeholders in the IT sector, and digital media platform owners. This recent news confirms that there should be an integrated approach in dealing with cyber-ethics and, during this critical period where news is digitised for public consumption, it is important that the news is accurate. SANEF (2020) reports that if fake news is reported the Electronic Communications Services Licences, top media service providers and internet service providers are responsible for removing fake news from digital media platforms. NGOs selected for the present study expressed the view that attempts made by government and other organisations and groups to curb fake news during Covid-19 have been insufficient and that the NGO sector “feels the brunt of the misinformation” (as stated by an employer).

Truth

The ethical variable “truth” explores the way in which individuals present their organisation and themselves authentically or, putting it more directly, honestly. It also refers to trust concerns on the internet. The question arises: How often are organisations and individuals completely honest on the internet, especially when social marketing is concerned? Nchabeleng, Botha and Bisschoff’s (2018, 23) study of nine NGOs of varying sizes in Gauteng, South Africa, asked how employees manage risks associated with the new IT and social media. The authors (2018, 23) concluded that “employers should provide a standard personal responsibility” for public relations in NGOs.

In the present study, the participating NGOs revealed that important requirements in using social media are transparency, disclosure, honesty and ethics. Therefore, the variable “truth” will continue to remain an invaluable principle that needs to be

honoured when implementing rules and policies that can be supported by technology to govern online behaviour. According to an article on Bizcommunity.com (2020b), NGOs and corporate social investment programmes will be looking for ways to sustain ethical business practices, despite the claim that the unemployment rate is expected to rise to 50% due to the pandemic. The article cites Gitta Carroll, a social entrepreneur and founder of the Good Machine, who explains that for the philanthropic space to survive, “building trust between corporate donors, NGOs and recipients is essential for long-term effectiveness to overcome the challenges of poverty and inequality in South Africa” (Bizcommunity.com 2020b). Of note in this respect is that, in January 2020, an Edelman Trust Barometer survey revealed that South Africans had the lowest trust in the government of all the 28 countries surveyed, with a score of just 20%. The survey also revealed that 59% of South Africans trusted NGOs and 58% trusted business, while only 40% trusted the media. With more than 100 000 registered NGOs in South Africa, Carroll (Bizcommunity.com 2020b) asserts that trust is essential for the sustainability of NGOs and she strongly suggests that NGOs partner with each other to succeed.

Human Dignity

“Human dignity” relates to the respect shown to individuals on digital media. It also refers to the ways in which organisations are treated online, otherwise conceptualised as “corporate dignity”. A company’s corporate image and corporate identity can be manipulated on digital media, affecting the way the public views the organisation. Thus, issues concerning reputation management, disrespect, defamation and pride fall under the ethical variable “human dignity”.

BusinessTech (2020) reports that Business for South Africa (B4SA), a group that informs the country’s business community and other stakeholders of challenges faced by businesses and progress made by working groups, indicated that Covid-19 will be part of daily life in South Africa for another two years. The selected NGO sample gave examples of when individuals in their organisations, or in other NGOs, had fallen victim to online harassment and defamation. Of the five NGOs, two had drafted ethical guidelines that they shared with their publics on their digital media to protect themselves and others. To protect human and corporate dignity during the pandemic, cyber insurance is being offered to users, enabling them to have access to expert knowledge and resources to manage and recover from a cyber incident (Van de Coolwijk 2020).

Regulation

“Regulation” denotes the way digital sites are governed or monitored within an organisation. This includes the actions of line managers and gatekeepers of the social and digital media, and the requirements set by manuals, guides, employee procedural policies, and public policies. It also refers to any regulatory institutions that monitor digital media platforms. The term also refers to social contracts found on digital media, such as the “Terms of Use”. During the pandemic, there may be some unfair regulations which could be detrimental to NGOs and other internet users. Some clauses in the Terms

of Use allow the appropriation of personal information and consumer-generated content, and stakeholders, such as that a supplier, can vary the terms of a contract without the consumer agreeing to the variation. From the narrative analysis, it is clear that the Terms of Use on digital media do not explicitly discuss any jurisdiction clauses for the adjudication of disputes that may arise from breach of contract. There are also no clauses on affiliated laws to determine how to resolve disputes arising from disagreements.

It is clear from the present study which involved five selected South African-based NGOs that the Covid-19 pandemic has led to the imposition of new government regulations and thereby forced many lifestyle changes. The digital media specialists interviewed engaged with Mbinjama-Gamatham's proposed social media ethical guidelines and suggested some changes (which will be presented later in the article). Of the participants that were interested, 80% indicated that the revised ethical guidelines for digital media should be added contextually into relevant guides, manuals and policies.

Some countries have passed legislation to govern internet users' behaviour. In South Africa, the Select Committee on Security and Justice adopted the Cybercrimes and Cybersecurity Bill (B6-2017) (SA 2017). According to SAnews.gov.za (2020), the Bill

aims to create offences that have a bearing on cybercrime; criminalise the distribution of harmful data messages and to provide for interim protection orders; further regulate jurisdiction in respect of cybercrimes; further regulate the powers to investigate cybercrimes, and also further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime.

The Bill seeks to create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which incite damage to property or violence or which are harmful or intimate and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime. The Bill was then passed as the Cybercrimes Act 19 of 2020 (SA 2020).

Mbinjama (2012) predicted that the provisions of regulations related to cyber-ethics would conflict with aspects of the South African Bill of Rights (SA 1996, Chap. 2). The Cybercrimes Act 19 of 2020 might present some challenges in relations to other bills and laws, especially in respect of transnational activities that occur in the digital space. How to track who owns the digital information that caused cybercrime and where it was sourced are just a few of the questions that arise when considering regulating the online space.

Ownership of Information

“Ownership of information” refers to the owner of the content posted on the digital sites. This would pertain to the individual user or the organisation. Ownership also includes third party distribution of information on digital media platforms. Issues of intellectual property rights, data use policies on these platforms and endorsement or sharing of information falls under this category. Furthermore, allocation of responsibility for content that is being circulated to cause harm or disruption to the user is categorised here. Currently, commercial social networking companies are having to consider protection of users while they are online, such as when using Facebook, Instagram, or Snapchat. In 2018, Facebook was exposed for giving technology companies, such as Microsoft, Netflix and Spotify, special access to users’ data without their knowledge (Blumenthal 2018). The same allegations are currently being made with regard to TikTok and Chinese spy actions in the United States.

Social networking companies and legislation play a role in the levels of unethical activities that occur on digital media platforms. Facebook releasing users’ data to third parties suggests that online users can have access to other people’s information or data, which can encourage criminal activities. The Facebook-Cambridge Analytica data scandal, which involves the collection of personally identifiable information of up to 87 million Facebook users that began in 2014, exemplifies the essential need to regulate the content of online contracts found on digital media in order to protect consumer rights, including the ownership of information.

The participants from the NGOs were aware of the ways in which information can be misused and thus felt that the POPIA would help safeguard them from potential harm and make internet users more conscious of what they do with information. An NGO employer stated:

I am glad the POPI Act is in full effect. At least now people can stop and think before clicking and sharing what does not belong to them. A lot of people are desperate these days and clickbait is becoming too much during Covid-19.

According to Scott (2021), clickbait refers to a type of web content advertisement that is designed to entice its readers into clicking on an accompanying link, which may result in hacking.

Overlapping Ethical Issues

Clearly there are overlapping issues in the eight ethical variables, which is to be expected as these variables exemplify the complex nature of the digital space. This reality rings especially true during Covid-19, when organisations and individuals have been forced to operate digitally in order to avoid spreading the virus through physical interaction. To return to the Habermasian discussion on communicative action, even when there are stipulated guidelines or contracts – such as the Terms of Use – it should be clear that it is not easy to consistently practise communicative action. Naturally,

people are inclined to promote their own interests most of the time, and therefore it is likely that they would practise strategic action without being explicitly aware that they were doing so.

Concerning the theme of the article, the important distinction made by Habermas between the two modes of communication is useful. It enables the contrast to be made between the kind of communication behaviour in cyberspace that requires ethical or possibly legal intervention on the one hand, and the kind that does not, on the other. This is especially true when human life, dignity and privacy are threatened. While the eight ethical variables, as elaborated on, emerged from Mbinjama-Gamatham's (2014) study, they provide the basis for a brief narrative perspective from a new set of participants from the NGO sector during the pandemic and their experience with cyber-ethics. The eight ethical variables allowed the participants to comment on ethical guidelines and each participant was able to suggest changes to it.

From the extant literature of which measures have been taken so far to safeguard South African internet users from cybercriminals and other online offenders, it is evident that there is an integrated approach from various stakeholders in the country to address cyber-ethics. Various stakeholders have partnered and collaborated in developing Coronavirus tracing applications such as Covi-ID and COVIDConnect. However, the development of these applications has raised concerns regarding access, accuracy, privacy, trust and human dignity (Schepers and Novazi 2020; Voigt 2020). It is encouraging to note that during the pandemic, the government and application developers have been concerned about contributing to social order in cyberspace. Vulnerable groups in society, such as children, the disabled, the poor, and the elderly, are often represented by NGOs. Most of the applications do not seem to take into account the privacy, data rights and ownership of information of those who are unable to represent themselves fully on tracking applications.

Particularly during the pandemic, therefore, it is essential that internet users, organisations, government, technology experts and NGOs should seek to curb the virus and safeguard each other from misconduct while using digital media platforms. Ast (2019, 207) claims that the Integrative Social Contracts Theory (ISCT) is a popular framework to justify and identify substantive hypernorms and fundamental moral principles that are valid across cultures. Levine (2019, 393–407) argues that, for this to be possible, trust and cooperation should be part of the foundation of digital commerce by expanding the reach of Donaldson and Dunfee's (1999) Social Contracts Approach. Further, Levine (2019) argues that if trust and cooperation form the basic framework of the ISCT, then the microsocial norms can apply to the digital business community in the same way that they function in the offline business world. She also claims that if users accept such norms trust and cooperation carry moral responsibility. Thus, the ISCT is complementary to Habermas' theory of communicative action and discourse ethics, based on its reliance on universal principles and authentic local values.

Universalisability through a Microsocial Contract

Habermas' original work explains that two principles – the discourse principle and the moral (or universalisability) principle – can be applied to address conflicts that occur when people disagree about norms or validity claims (Finlayson 2005, 78). In terms of Habermas' theory of communicative action and discourse ethics, the discourse principle seems applicable during the current period of Covid-19 and for future studies on social contracts, in that all relevant stakeholders need to participate in communication and agree on the validity claims (norms) in an open and rational manner (Finlayson 2005, 79). However, the universalisability principle also has a role to play, as will be shown below. For internal regulation of digital media use within an organisation, digital media strategists, along with all those (within the organisation) affected by digital platforms, should agree on what needs to be contained in procedural policies for employees and/or public policies. The ISCT, which includes the microsocial and macrosocial contract norms (Dunfee, Smith and Ross 1999, 18), may thus play an important role in arriving at ethical and moral guidelines for digital media.

Microsocial contracts are more community-based (Dunfee, Smith and Ross 1999, 18) than macrosocial contracts, and thus allow for organisations to arrive at their own guidelines, based upon their own corporate culture, mission, values, business principles and needs. For the effectiveness of the internal regulation process of using guidelines for digital media, it seems important that the digital media specialists, along with employers or managers, consider selecting the appropriate language spoken by most stakeholders to draft the guidelines, even if English is the universal language. Digital media teams thus have to be cautious regarding the way in which the guidelines are written. They also need to consult with a wide range of stakeholders and reach consensus about the course of action in order for the universalisability principle to have the best chance of taking effect from an internal regulation perspective. Arguably, the more stakeholders from the NGO sector are involved, the more universalisable the guidelines could become. Thus, drafting the PAIA manual, alongside the POPIA and the proposed digital media ethical guidelines for NGOs, is an example of an integrated social contract as it involves guidelines for self-regulation as well as governmental regulation.

As indicated by Habermas, the universalisability principle becomes more effective if guidelines are to be written, as far as possible, for present and future users of cybercommunication so as to avoid continual revision of cyber-ethical guidelines for employee procedural and public policies. As indicated, the moral principle of 'universalizability' (Habermas cited in Finlayson 2005, 80–81) can only work in the testing of norms that guide people's actions if the guidelines take into account the likely agreement on the consequences of accepting certain norms for digital media use by future users as well as current ones. Although it is not possible to assume with certainty that the guidelines will be accepted by future users, it must be emphasised that involving as many stakeholders as possible in the field of cybercommunication in the deliberations

towards the formulation of cyber-ethical guidelines can counteract many potential obstacles to achieving universalisability.

Thus, at least from a theoretical point of view, as many strategic stakeholders as possible need to be involved in decision-making processes and the drawing up of digital media-use guidelines into employee procedural and public policies. Stakeholders of NGOs would need to acknowledge the agreed-upon status of the ethical and moral guidelines, perhaps by organisations providing informed consent forms for users to complete online. Consent forms and social media-use guidelines may be based on the proposed eight ethical variables and ought to be easy to read in whatever language the user desires.

In South Africa, strategic stakeholders for the NGO sector include the South African NGO Coalition (SANGOCO), which is the umbrella body of NGOs in Southern Africa. Its Constitution assists in guiding potential users through the rules and regulations of SANGOCO. This body, along with the South African Department of Social Development, can possibly review the aspects of the Constitution that relate to the NGO sector in South Africa and include guidelines for digital media-use as part of the Constitution. Table 1 outlines the proposed digital media-use ethical guidelines for NGOs, adapted in the light of comments from the five participants from NGOs during Covid-19 from Mbinjama-Gamatham (2014, 191–194). The guidelines include digital media-use ethical guidelines that the NGO sector could adopt to self-regulate their interactions, both on social media and overarching digital media platforms. The guidelines can be adapted to suit the needs of internal and external stakeholders of relevant NGOs and be included in public procedural policies for external and legal regulation. A properly constituted set of cyber-ethical guidelines might thus be able to assist users with decisions on universally relevant moral dilemmas.

Table 1: Proposed digital media-use ethical guidelines for NGOs

1. Justice	
1.	Conduct yourself in a morally upright manner and promote good behaviour towards and treatment of others on digital media sites.
2.	Bear in mind any actions which may result in criminal activities and may result in demotion, suspension or legal repercussions.
3.	It is your duty to ensure that you keep updated on the law of the internet and digital media sites.
2. Privacy	
1.	Respect the privacy of others.
2.	It is your right to practise anonymity at the workplace while operating the NGO's digital media platforms.
3.	Ensure that the privacy settings of the digital media sites are checked every three weeks (once a month) as per job description of the gatekeeper/content manager/digital media specialist(s) of the NGO's digital media platforms.
3. Access	
1.	Even when information appears to be readily available on digital media sites, attempt to obtain permission to use the data if you intend to publish the information on other media platforms, especially in traditional media such as television, radio and other internet sites

2.	Do not use the NGO's digital media platforms to hack into other users'/companies' digital media sites. See point 2 of these guidelines, under <i>Justice</i> .
3.	Do not give the NGO's username and passwords to any member of the organisation that has not been authorised to update digital media site(s) of the NGO. More importantly, the same rule applies to the external stakeholders of the organisation.
4.	Passwords and usernames of each digital media site should be filed. If some digital media accounts are connected to an individual within the NGO, this information should be kept somewhere, at the discretion of the employer/manager. (It is recommended that digital media accounts or profiles are not connected to an individual but to the NGO itself as this will lessen the chance of the employee's details being misused for illegal activities.)
5.	Ensure that banking details of the organisation are sent to benefactors via 'secure' email after corresponding on digital media sites in order to keep an electronic trail of the communication or dialogue.
6.	Ensure that benefactors who wish to access and use the NGO's information which has been posted on digital media site(s) use and spell the authentic name of the organisation properly. This guarantees that the organisation's corporate name is consistent across digital media platforms.
4. Accuracy	
1.	All content/information that is placed on digital media platforms should first be verified by the gatekeeper/content manager/social media specialist(s) of the NGO's digital media sites.
2.	All content/information presented on digital media sites by the user must be thoroughly researched and confirmed as accurate before posting it on the internet.
3.	An NGO linked to an International NGO (INGO) should seek counsel on how to approach naming the profiles of digital sites which they create. Alternatively, the brand name can include the country, province or city where the NGO is based. This can be presented in brackets. Should the corporate name of the NGO be too long, the NGO's digital media URLs may be placed on the INGO's digital sites. The names should be consistent with the official, registered name of the NGO.
5. Truth	
1.	The NGO must be represented on digital media authentically and honestly.
2.	Gatekeepers/content managers/digital media specialists should avoid exaggerating the success stories of the NGO.
6. Human dignity	
1.	When maintaining the corporate identity and corporate image of the NGO, ensure the following: 1.1 On digital media sites, the NGO must treat its public with respect and dignity. 1.2 Photographs: The profile photo on digital media sites should be the logo of the registered NGO. 1.2.1 Photographs of children: Permission needs to be sought by relevant units and parties before posting them on digital media 1.2.2 Do not use photographs or pictures from the internet, in order to avoid copyright infringements.
7. Regulation	
1.	Read the Terms of Use of each digital media site along with the internet rules of the NGO which are embedded in this document. See pages xxx (include page numbers).
2.	Gatekeepers/content managers/digital media specialists of the NGO's digital media sites must uphold the rules and Terms of Use of social media sites and the internet.
3.	All users need to ensure that their interaction on digital media sites is self-regulated if they are not representing the NGO. The NGO takes no responsibility for users of the internet who commit cyber-related crimes and are associates of the NGO.

8. Ownership of information	
1.	If a member of the NGO is the gatekeeper/content manager/digital media specialist whose account is linked to his/her own private digital media accounts, the member must place a disclaimer on his/her personal profile stating that he/she is posting the information as an individual not representing the NGO.
2.	Information or content placed on the NGO digital media sites must not infringe intellectual property rights.
3.	Third party distributors must be identified, if possible, to track where and how the NGO's information is being used.

Conclusion

The article has provided a narrative analysis of a study of five South African-based NGOs and related literature on the NGOs' experiences with digital media and cyber-ethics during the Covid-19 pandemic. The present study provides a basis for future case studies about cyber-ethics in so far as it addressed the prominence of the eight ethical variables during the pandemic and what actions have taken place to secure the privacy and information of internet users. The POPIA and the PAIA manual have been identified to be of significance during the pandemic and may aid organisations to review their current privacy policies and make sound adjustments. One of the study's limitations was obtaining data from employers who knew very little about the problems experienced by digital media specialists while online. Where necessary, the researcher allowed other NGO members to be interviewed on behalf of employers. Other limitations included the lack of research studies on the topic, which is a positive argument for conducting the present qualitative study to identify the phenomena.

The ISCT is clearly compatible with Habermas' discourse ethics, especially as it relates to the global universalisability moral principle needed in guidelines appropriate to present and future internet users. While each variable may pose particular challenges, by drawing from the theoretical work of Habermas, it is possible to arrive at a consensus when as many strategic stakeholders as possible are involved in a decision, as long as religious or political grounds for debate are excluded. At the first level, internet users need to agree rationally to the Terms of Use of digital media platforms. This also applies to the second level, where there could possibly be a national (but also ultimately international) cyber-ethics code of conduct on the ethical use of cybercommunication. Habermas maintains that disagreement (lack of consensus) at either of the two levels is an indication that the norm that is being considered is not valid (Finlayson 2005). The second principle has to be added because of the universalisability it implies.

The eight ethical variables proposed in Table 1 can be used in future studies to advance the ISCT by formulating cyber-ethical guidelines for the Fourth Industrial Revolution, especially in light of the POPIA and the PAIA manual. This can be done by investigating how NGOs that represent some of the most vulnerable groups in society, such as the disabled, the poor, children and the elderly, are navigating the digital sphere during and after the Covid-19 pandemic. Investigation of the challenges and responsibilities of digital media specialists, digital forensics, and IT specialists in implementing and

regulating microsocial and macrosocial contracts across local, national and international boundaries could also be done using the ISCT.

Acknowledgement

This work is based on research supported in part by the National Research Foundation of South Africa (Grant Number: 129877).

References

- Abbott, L. M. 2016. "The Conceptual Public Sphere and Its Problems: Habermas, Political Action and the Arab States." *Journal of International Political Theory* 12 (3): 365–379. <https://doi.org/10.1177/1755088216651302>
- Ali, L. 2019. "Cyber-crimes – A Constant Threat for the Business Sectors and Its Growth (A Study of the Online Banking Sectors in GCC)." *Journal of Developing Areas* 53 (1): 267–279. <https://doi.org/10.1353/jda.2019.0016>
- Ast, F. 2019. "The Deliberative Test, a New Procedural Method for Ethical Decision Making in Integrative Social Contracts Theory." *Journal of Business Ethics* 155 (1): 207–221. <https://doi.org/10.1007/s10551-017-3481-y>
- Bizcommunity.com. 2020a. "Now Is the Time for a Full-service Cyber Security Solution." Accessed July 10, 2020. <https://www.bizcommunity.com/Article/196/661/205884.html>
- Bizcommunity.com. 2020b. "Redefining Modern Philanthropy in a Post-Covid-19 World." Accessed July 20, 2020. <https://www.bizcommunity.com/Article/196/848/206724.html>
- Blumenthal, P. 2018. "Facebook and Google's Surveillance Capitalism Model Is in Trouble. Regulators Start to Pump the Brakes on Big Tech's Advertising Dystopia." *The Huffington Post*, January 27. Accessed July 20, 2020. https://www.huffpost.com/entry/facebook-google-privacy-antitrust_n_5a625023e4b0dc592a088f6c
- BusinessTech. 2020. "Covid-19 Will Be Part of Daily Life in South Africa for 2 More Years: Business Group." Accessed July 20, 2020. <https://businesstech.co.za/news/business-opinion/420366/covid-19-will-be-part-of-daily-life-in-south-africa-for-2-more-years-business-group/>
- Donaldson, T., and T. W. Dunfee. 1999. *Ties That Bind: A Social Contracts Approach to Business Ethics*. Boston: Harvard University Business School Press.
- Dunfee, T. W., C. N. Smith, and W. T. Ross Jr. 1999. "Social Contracts and Marketing Ethics." *Journal of Marketing* 63 (3):14–32. <https://doi.org/10.1177/002224299906300302>

- Ellis, M. 2020. "Twitter Hack: Massive Breach Affects Bill Gates, Elon Musk, Obama, and Others." Accessed July 22, 2020. <https://memeburn.com/2020/07/twitter-hack-massive-breach-affects-bill-gates-elon-musk-obama-and-others/>
- Feenberg, A. 1991. "A Critical Theory of Technology." In *Handbook of Science and Technology Studies*, edited by U. Felt, R. Fouché, C. A. Miller and L. Smith-Doerr, 635–663. Cambridge, MA: MIT Press.
- Finlayson, J. G. 2005. *Habermas. A Very Short Introduction*. New York: Oxford University Press. <https://doi.org/10.1093/actrade/9780192840950.001.0001>
- Floridi, L. 2002. "What Is the Philosophy of Information?" *Metaphilosophy* 35 (1–2): 123–145. <https://doi.org/10.1111/1467-9973.00221>
- Gordon, W. 2008. "Moral Philosophy. Information Technology and Copyright: The Grokster Case." In *Information Technology and Moral Philosophy*, edited by J. van den Hoven and J. Weckert, 270–300. Cambridge: Cambridge University Press.
- Habermas, J. 1984. *The Theory of Communicative Action, Vol. 1. Reason and the Rationalization of Society*. Translated by T. McCarthy. Boston: Beacon Press.
- Habermas, J. 1987. *The Theory of Communicative Action, Vol 2. Lifeworld and System: A Critique of Functionalist Reason*. Translated by T. McCarthy. Boston: Beacon Press.
- Habermas, J. 1990. *Moral Consciousness and Communicative Action*. Translated by C. Lenhardt and S. Weber Nicholson. Cambridge: Polity Press.
- Hall, N., H. P. Schmitz, and J. M. Dedmon. 2020. "Transnational Advocacy and NGOs in the Digital Era: New Forms of Networked Power." *International Studies Quarterly* 64 (1): 159–167. <https://doi.org/10.1093/isq/sqz052>
- Heilweil, R. 2019. "New NGO Providing Aid to Cyberattack Victims Spotlights the Real Life Impacts of Online Hacks." Accessed July 25, 2020. <https://fortune.com/2019/10/11/cyberattack-hacking-victims-help-ngo-cyberpeace-institute/>
- Introna, L. 2005. "Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems." *Ethics and Information Technology* 7 (2): 75–86. <https://doi.org/10.1007/s10676-005-4583-2>
- Jaishankar, K. 2020. "Cyber Victimology: A New Sub-discipline of the Twenty-first Century Victimology." In *An International Perspective on Contemporary Developments in Victimology*, edited by J. Joseph and S. Jergenson, 3–19. Cham: Springer. https://doi.org/10.1007/978-3-030-41622-5_1
- Jay, M. 2019. "Habermas and Postmodernism." *Journal of Comparative Literature and Aesthetics* 42 (2): 218–229.

- Kenix, L. J., and F. Abikanlu. 2019. "A Comparative Analysis of Social Media Messaging by African-centred LGBT Refugee NGOs." *Journal of African Media Studies* 11 (3): 313–329. https://doi.org/10.1386/jams_00003_1
- Levine, L. 2019. "Digital Trust and Cooperation with an Integrative Digital Social Contract." *Journal of Business Ethics* 160 (2): 393–407. <https://doi.org/10.1007/s10551-019-04201-z>
- Macer, D. 2007. "Computing Ethics: Intercultural Comparisons. Ethical Pluralism and Social Justice." In *Information Technology and Social Justice*, edited by E. Rooksby and J. Weckert, 1899–2204. London: Information Science.
- Mbinjama, A. 2012. "Challenges to the Bill of Rights for Cyber-ethics: Social Media Use within Selected South African NGOs." Paper presented at the International Association for Media and Communication Research (IAMCR) Conference, University of KwaZulu-Natal, July 15–19.
- Mbinjama-Gamatham, A. 2014. "An Investigation of the Question of Cyber-ethics in Social Media-communications within Selected South African NGOs." PhD diss., Nelson Mandela University, Port Elizabeth.
- Mbinjama-Gamatham, A., and B. Olivier. 2020. "'Dark Technology', Aggressiveness and the Question of Cyber-ethics." *Acta Academica* 52 (1): 1–22. <https://doi.org/10.18820/24150479/aa52i1/1>
- Nchabeleng, M., C. J. Botha, and C. A. Bisschoff. 2018. "The Uses, Benefits and Limitations of Social Media for Public Relations in South African Non-governmental Organisations." *Journal of Business and Retail Management Research* 12 (3): Article #2. <https://doi.org/10.24052/JBRMR/V12IS03/ART-02>
- Outhwaite, W. 2013. *Habermas: A Critical Introduction*. Stanford: Stanford University Press.
- Pérez-Seijo, S., and G. O. Berta. 2020. "Use of 360-degree Video in Organizational Communication: Case Study of Humanitarian Aid NGOs." In *Journalistic Metamorphosis. Studies in Big Data*, edited by J. Vázquez-Herrero, S. Direito-Rebollal, A. Silva-Rodríguez and X. López-García. Vol. 70. Cham: Springer. https://doi.org/10.1007/978-3-030-36315-4_8
- Pompon, R. 2020. "What a Pandemic Can Teach Us about Cybersecurity." Accessed August 2, 2020. <https://www.bizcommunity.com/Article/196/661/202406.html>
- Reed, E. 2020. "Exxon Knew NGOs Targeted by Hacker Team." Accessed August 2, 2020. <https://www.energyvoice.com/oilandgas/americas/245117/exxonknew-ngos-targeted-by-hacker-team/>
- SA (South Africa). 1996. *Constitution of the Republic of South Africa, 1996*. <https://www.gov.za/documents/constitution-republic-south-africa-1996>

- SA (South Africa). 2000. *Promotion of Access to Information Act 2 of 2000*.
<https://www.gov.za/documents/promotion-access-information-act>
- SA (South Africa). 2002. *Electronic Communications and Transactions Act 25 of 2002*.
<https://www.gov.za/documents/electronic-communications-and-transactions-act>
- SA (South Africa). 2008. *Consumer Protection Act 68 of 2008*.
<https://www.gov.za/documents/consumer-protection-act>
- SA (South Africa). 2013. *Personal Information Act 4 of 2013*.
<https://www.gov.za/documents/protection-personal-information-act>
- SA (South Africa). 2017. *Cybercrimes and Cybersecurity Bill (B6-2017)*.
<https://www.gov.za/documents/cybercrimes-and-cybersecurity-bill-b6-2017-21-feb-2017-0000>
- SA (South Africa). 2020. *Cybercrimes Act 19 of 2020*.
<https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000>
- SANEF (South African National Editors' Forum). 2020. "Government Partners with Private Sector and NGO's to Curb Fake News during Covid-19." Accessed August 2, 2020.
<https://sanef.org.za/government-partners-with-private-sector-and-ngos-to-curb-fake-news-during-covid-19/>
- SAnews.gov.za. 2020. "South Africa: Committee Adopts Cybercrimes Bill." Accessed August 2, 2020. <https://allafrica.com/stories/202006120759.html>
- Schepers, M., and Z. Novazi. 2020. "COVI-ID: SA's Contact Tracing App Ensures Protection of Privacy." Accessed August 2, 2020. <https://www.tabacks.com/news-and-insights/2020/6/covi-id-south-africas-contact-tracing-app>
- Scott, K. 2021. "You Won't Believe What's in This Paper! Clickbait, Relevance and the Curiosity Gap." *Journal of Pragmatics* 175 (1): 53–66.
<https://doi.org/10.1016/j.pragma.2020.12.023>
- Sefora, N. M., and D. C. Dabija. 2020. "Best Practices of Non-governmental Organisations in Combatting Covid-19." In *6th BASIQ International Conference on New Trends in Sustainable Business and Consumption*, edited by R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea and C. Vasiliu. Bucharest: Academy of Economic Studies.
- Sharonova, S., and T. Beavitt. 2020. "Jurgen Habermas and Russian Philosopher-theologians Dialogue through the Century." *European Journal of Science and Theology* 16 (3): 107–117.
- Tee, K. 2021. "Understanding POPIA." Accessed August 2, 2020.
<https://www.iol.co.za/the-post/features/understanding-popia-7b3d925c-0949-4edd-8a0b-ac92c5427075>

- Umejiaku, N. O., and M. I. Anyaegbu. 2016. "Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria." *International Journal of Computer & Technology* 15 (1): 7130–7139. <https://doi.org/10.24297/ijct.v15i10.12>
- Van de Coolwijk, R. 2020. "POPI Act on Our Doorsteps." Accessed August 2, 2020. <https://www.bizcommunity.com/Article/196/661/205481.html>
- Voigt, E. 2020. "The Trial and Error of Covid-19 Digital Contact Tracing in South Africa." Accessed August 2, 2020. <https://www.dailymaverick.co.za/article/2020-07-28-the-trial-and-error-of-covid-19-digital-contact-tracing-in-south-africa/>
- Wilkinson, O. 2018. "Secular Humanitarians and the Post-secular: Reflections on Habermas and the Typhoon Haiyan Disaster Response." *Journal of Contemporary Religion* 33 (2): 193–208. <https://doi.org/10.1080/13537903.2018.1469260>