Can the social contract theory justify data rights violations? A review of South Africa's contact tracing regulations

AUTHOR: Rumbidzai Matamba and Chenai Chair | COUNTRY: South Africa

INTRODUCTION

We are slowly becoming aware of the proliferation of our data by different companies and entities across different sectors due to a data "spillage" as we access the digital conveniences and necessities of the world that we live in today. These companies and entities range from advertising, insurance, banking, and even government sectors. Companies and entities that have a significant influence on our quality of life, how we navigate the world today and how we are treated politically, socially and economically. While acknowledging that a simple search for the price of a laptop will result in being hounded by various laptop manufacturers and vendors, and having, inadvertently, let this become a running joke of the 21st century, we were not prepared for governments to utilise our data without our consent and to not have any legal recourse to this obvious violation of our right to privacy, as it is espoused in different international legal instruments and Principle 9 of the African Declaration of Internet Rights and Freedoms.[1]

The current pandemic has resulted in a need for solutions to "flatten the curve", including lockdowns and digital solutions such as contact tracing. The latter raises questions on the balance of privacy rights with public health data. This essay employs the use of the South African government's contact tracing initiatives in response to the COVID-19 pandemic and some public perceptions on these initiatives to assess whether the social contract theory can be employed as a tool to justify privacy violations for public health.

1 https://africaninternetrights.org/articles

BACKGROUND

As the second largest economy in sub-Saharan Africa,[2] South Africa is aaccess to communication services. Across its nine provinces, the highest percentage of households with access to cellular phones is 96.5% and the lowest is 77.1%.[3] Households with neither cellular phones nor landlines come in at a low 10.3%.[4] Over half of the population – 53% – make use of mobile internet, but the country's high data prices, the lack of internet-enabled devices and low digital literacy rates are barriers to internet use.[5]

African countries have been slow to adopt data protection regulations: only 14 out of the 54 countries on the continent have signed the African Union's Convention on Cyber Security and Personal Data Protection and only 25 countries have passed their own individual data protection laws.[6] South Africa's data protection law, the Protection of Personal Information Act 4 of 2013 (POPIA), is set to commence on 1 July 2020 with a one-year grace period for full compliance by companies.

Be that as it may, South Africa recognises the constitutional right to privacy. However, this right may be infringed where there are larger public interest considerations that outweigh the impact on privacy. Further, the lawful interception and monitoring of communications by law enforcement agencies is dealt with in separate legislation, the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (RICA),[7] although the contact tracing provisions passed have different objectives from RICA.

METHODOLOGY

The main premise this essay seeks to answer is whether an adage of Hobbes' social contract theory, that people are willing to give up certain rights and live according to a moral code if the remainder of their rights are guaranteed, can be used to justify the violation of online privacy rights. To do this, we conducted a desk review of the contact tracing initiatives employed by the South African government and sought public input on the conceivability of this theory through a short survey. This survey was in the form of a questionnaire, distributed online,

2 Delport, J. (2020, 24 March). Africa's Top 10 wealthiest countries ranked by GDP. *ITNews*. https://www.itnewsafrica.com/2020/03/africas-top-10-wealthiest-countries-ranked-by-gdp

3 Independent Communications Authority of South Africa. (2019). *ICASA Annual Report 2019*. https://www.icasa.org.za/legislation-and-regulations/icasa-annual-report-2019

4 Ibid.

5 Research ICT Africa. (2018). *After Access: The State of ICT in South Africa*. https://researchictafrica.net/2018/09/10/state-of-ict-in-south-africa

6 Sylla, A., & Ford-Cox, A. (2019, 14 October). Overview of Data Protection Laws in Africa. *Hogan Lovells*. https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2#:~:text=Today%2C%20out%20of%2054%20countries,be%20on%20the%20legislative%20agenda

7 Several provisions in RICA were struck down by the high court in September 2019 after being found to be problematic to the extent the state was using the instrument to spy on citizens. See: amaBhungane. (2020, 19 February). Advocacy release: Concourt to hear amaB's Rica challenge. https://amabhungane.org/advocacy/advocacy-release-concourt-to-hear-amabs-rica-challenge

in which 25 people responded to questions about whether they are aware of the South African government's contact tracing initiatives, whether they are aware of the POPIA and what their take is on the negotiation between their right to privacy and the need for contact tracing surveillance for the greater good. The survey is not representative of the South African population, nor may results be inferred. As such, we welcome any collaboration for further in-depth research on public perceptions on contact tracing initiatives. However, the survey provides insight relevant for the purposes of this study.

SOUTH AFRICAN COVID-19 RESPONSES AND HUMAN RIGHTS ONLINE

As the national lockdown began, the South African government passed regulations to address, prevent and combat the spread of COVID-19 under the Disaster Management Act 57 of 2002. Regulation 10 of this effort provides for the use by the Director General of Health of one's location and movement data, from their electronic communications service provider, without their informed consent, for inclusion in the South African COVID-19 tracing database.[8] This not only applies to one person, but to everyone that is presumed to have been in contact with them from the period during which the pandemic has been reported and is still active in South Africa, i.e. from March 2020 onwards.[9] Under these regulations, the data collected is used for contact tracing purposes only in response to the COVID-19 pandemic, and the data is to be retained for a period of six weeks after being obtained; thereafter it is to be destroyed.[10] The regulations further include transparency provisions in the form of safeguards to protect the right to privacy and give an oversight role to a retired Constitutional Court judge. The judge, appointed by the Minister of Justice, receives a weekly report stating the names and details of any person traced using the COVID-19 tracing database and provides oversight only on the tracing process. As of 3 April, it has been reported that 1,500 people's data has been shared to be used in the tracing database.[11]

Contact tracing is a supplement to on-the-ground testing and physically warding off COVID-19 through social distancing and constant washing and sanitising of hands. It presents governments with an opportunity to identify people who may have been exposed to COVID-19 and advise them to self-quarantine before they expose other people to the virus. In the survey we conducted as part of our research into public perceptions on contact tracing, 52% of the 25 respondents felt contact tracing was necessary but still indicated that they worried about their right to privacy.

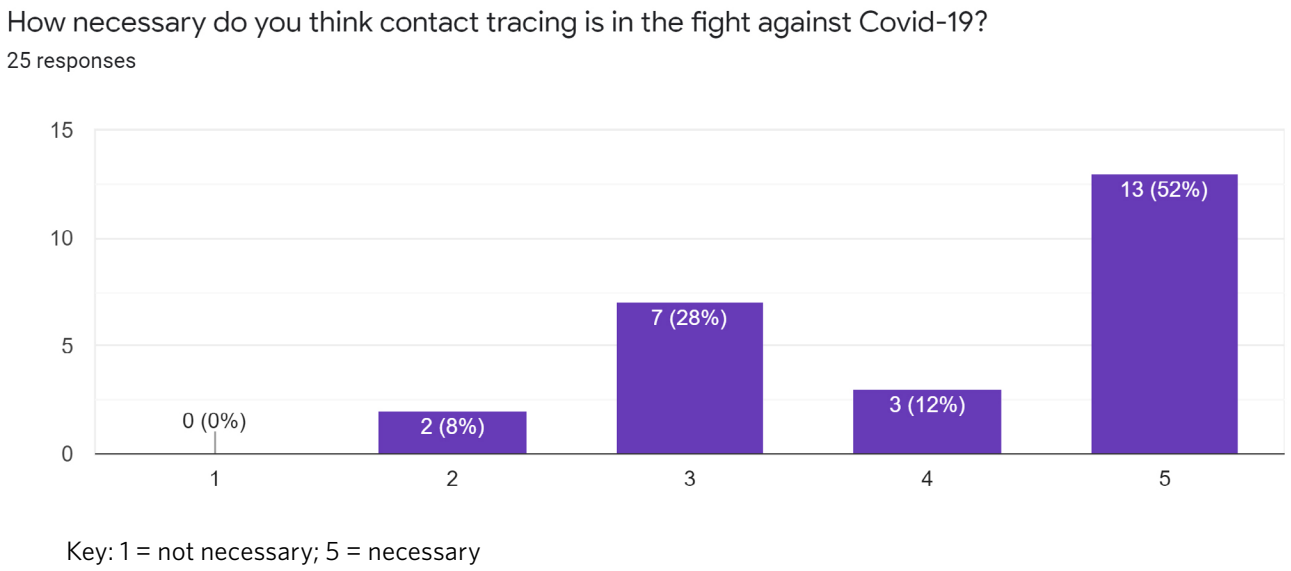
---

8 Department of Cooperative Governance and Traditional Affairs. (2020). Disaster Management Act, 2002: Amendment of Regulations Issued in Terms of Sections 27(2). www.cogta.gov.za/?p=7871

9 Ibid.

10 Ibid.

11 Gershgorn, D. (2020, 9 April). We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World. *OneZero*. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9



↑ Contact Tracing against Covid-19
Source: Chenai Chair | Rumbidzai Matamba

And rightfully so, because, as the Amabhungane Centre for Investigative Journalism pointed out, the regulations are not entirely error-free.[12] For example, for the purposes of contact tracing, the interception of communications in the ordinary course of events is permitted, but there is no post-spying notification during the process. This means that anyone whose communication data has been intercepted is not alerted to this until six weeks after the national state of emergency has lapsed.[13] This provides ample opportunity for the system to be abused and for this abuse to go unnoticed.[14]

Furthermore, the regulations provide that the tracing database must be stripped of any identifying information, and the de-identified data may only be used for public health research going forward. However, there is no indication on whether the process of de-identifying the data will be monitored and who the responsible party for monitoring it will be. Storing data is also a fraught process – and these databases, filled with detailed personal data, might draw the attention of hackers before it has been de-anonymised.[15] Given several examples where encrypted data has been de-anonymised – for example, US President Donald Trump's location data was recently de-encrypted,[16] and the

12 Hunter, M., & Thakur, C. (2020, 3 April). Advocacy: New Privacy Rules for Covid-19 Tracking a Step in the Right Direction, but.... *amaBhungane*. https://amabhungane.org/advocacy/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but

13 Ibid.

14 Ibid.

15 Wild, S. (2020, 5 May). COVID-19: Geolocation Tracking Fuels Concerns Around Privacy and Data Protection. *Africa Portal*. https://www.africaportal.org/features/covid-19-geolocation-tracking-concerns-privacy-data

16 Thompson, S. A., & Warzel, C. (2019, 20 December). How to Track President Trump. *The New York Times*. https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html

South African government itself has been hacked before[17] – the implications of contact tracing on the right to privacy are dire.

The South African government has also approached other technology companies to identify suitable projects that may assist in its efforts against COVID-19. One such project is a partnership with the University of Cape Town to develop a smartphone app to assist the government with tracking people who may have come into contact with anyone who is COVID-19-positive.[18] The app is called Covi-ID and it has a GDPR-based privacy policy. Covi-ID also voluntarily submits to the data protection act (POPIA). The app is voluntary at this stage and requires personal information such as your COVID-19 status and your location. This information is stored on the user's phone using a technology called self-sovereign identity, which is not a centralised government or private sector database.[19] This means that the user has full authority and control over who can access their data, what they can access the data for, and how long they can have access to this data.[20] Additionally, the Department of Health also launched a WhatsApp-based symptom-reporting process which, unfortunately, does not set out any terms and conditions of use, information on who is processing the information, or where else it might be shared.[21]

Although the POPIA is not yet in full force, the Information Regulator whose role is mandated by the act issued a guidance note to clarify the legality of the contact tracing provisions. The guidance note provides for the limitation of the right to privacy when enlisting the use of personal information of data subjects for the purposes of containing the COVID-19 virus.[22] The Information Regulator is of the opinion that these contact tracing initiatives do not violate POPIA provisions and that if anyone tests positive for COVID-19 they have a duty to share this information with the government so that it may act accordingly.[23]

← Covid-19 WhatsApp database
Source: bloomberg.com/news/articles/2020-03-25/whatsapp-service-in-south-africa-goes-global-in-who-virus-fight

17 Kubheka, A. (2020, 18 March). Hackers Hit Government Websites. *IOL*. https://www.iol.co.za/dailynews/news/kwazulu-natal/hackers-hit-government-websites-45122121

18 Norton Rose Fulbright. (2020). *Contact tracing apps: A new world for data privacy*. https://www.nortonrosefulbright.com/en-za/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy

19 Georg, C. (2020, 5 April). Covi-ID: Privacy-Preserving COVID-19 Status Verification. *Medium*. https://medium.com/coviid/covi-id-privacy-preserving-covid-19-status-verification-c11d59ec92f6

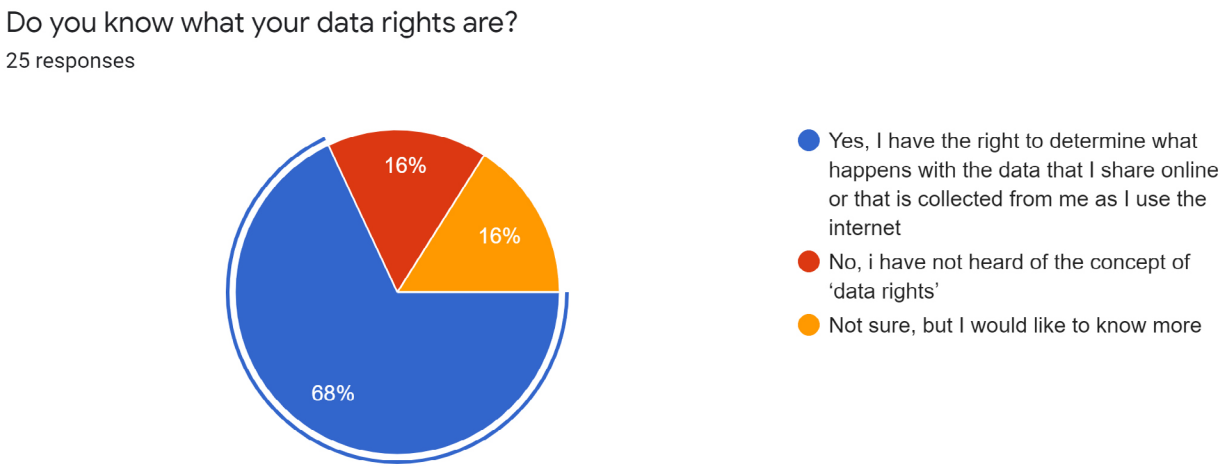
20 Ibid.

21 Norton Rose Fulbright. (2020). Op. cit.

22 Information Regulator (South Africa). (2020, 3 April). Guidance Note on the Processing of Personal Information in the Management and Containment of COVID-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPIA). https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

23 Ibid.

While the Covi-ID app has in-built functions to protect the right to one's privacy, the WhatsApp initiative is lacking in that department, as one is not even aware of who they are sharing their information with. We note, at this point, that our survey results indicated that 32% of our respondents were not aware of their data rights. The ambiguity of the widely used WhatsApp database (it reached about 1.5 million users within the first week of use) highlights the need to have privacy by design, so that even where people are not aware of their rights, they are still protected. It is necessary that the right to privacy online is protected despite data subjects' awareness of this right.



↑ Data Rights
Source: Chenai Chair | Rumbidzai Matamba

Moreover, these two mobile initiatives also raise accessibility issues because, as noted above, 47% of the South African population does not have access to the internet. Consequently, 47% of the population does not have access to the tech systems employed to mitigate COVID-19 by sharing important information relating to this pandemic. Therefore, the issue is not only the implications of these technologies on privacy rights; it extends to the right to not be discriminated against on the basis of one's socioeconomic status and the right to access to information. Another concern around the acquisition of people's data is "function creep", which is when data is collected for one reason and then used for another.[24] South Africa is not outside the realm of doing this, because it has shown an inclination towards humanitarian abuses, for example, 12 people have been killed by the police and the South African National Defence Forces since March 2020.[25] Critics worry that, while the data will initially be collected to track COVID-19, it will also be put to other uses, such as spying on political rivals, or be sold to companies.[26] Overall,

24 Wild, S. (2020, 5 May). Op. cit.

25 Karrim, A. (2020, 3 April). UPDATE | Lockdown: 3 die allegedly at the hands of the police. *News24*. https://www.news24.com/news24/southafrica/news/lockdown-number-of-deaths-from-police-action-rises-to-8-surpasses-sas-covid-19-casualties-20200403

26 Wild, S. (2020, 5 May). Op. cit.

there is no sense of ownership of our data – disembodying the data collected and increasing online rights violations.

A SOCIAL CONTRACT APPROACH TO BALANCING PRIVACY BREACHES FOR PUBLIC HEALTH DATA?

The internet has become an interplay between two tendencies: a necessary means of access and a tool used to constrain liberty and privacy. There are increasing calls for the right to privacy online to be ensured in internet governance.[27] While some contact tracing technologies are lightweight and temporary, others are pervasive and invasive and lean more towards constraining liberty and privacy.[28] For example, Chinese contact tracing technologies are more invasive, as they collect identity and location information as well as one's online payment history, so that they can watch for those who break quarantine rules.[29] South African contact tracing technology, as far as we know, can be classified as less pervasive, as it is only limited to identification and location data. However, as the COVID-19 pandemic rages on, technologists are rushing to build applications and services for contact tracing and the South African government has shown an interest in procuring these private technologies.

While the threat of further privacy violations can be mitigated by the regulations passed by the government, public and private technological companies are notorious for harvesting data, which the contact tracing initiatives have given them free reign over. The threat for further privacy violations does exist, and so the contact tracing initiatives present an opportunity to renegotiate the terms with which we use technology; how governments can regulate technology; and how governments and public or private corporations can cooperate for the trustworthy use of artificial intelligence and technology.[30] If this opportunity is not taken, we might observe a slow surrender of public liberties in the name of using surveillance technologies in the battle against COVID-19 and other potential novel viruses.[31]

The social contract theory put forward by Hobbes in political philosophy posits that citizens give up a portion of their rights and live by a moral code for a guarantee of their remaining rights.[32] The South African constitution is a manifestation of the social contract theory, as it indoctrinates certain guaranteed rights

27 African Declaration on Internet Rights and Freedoms Coalition. (2020). *Position Paper in Response to the Covid-19 Pandemic*. https://africaninternetrights.org/wp-content/uploads/2020/06/AfDec_COVID-19_Position-paper_Eng.pdf

28 O'Neill, P.H., Ryan-Mosley, T., & Johnson, B. (2020, 7 May). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker

29 Ibid.

30 Louradour, S. (2020, 20 April). How to create a trustworthy COVID-19 tracking technology. *World Economic Forum*. https://www.weforum.org/agenda/2020/04/covid-19-coronavirus-tracking-technology

31 Ibid.

32 Ginsberg, R. (1974). Kant and Hobbes on the Social Contract. *The Southwestern Journal of Philosophy, 5*(1), 115-119.

in exchange for our rights to be self-serving and self-governing. Every society that has established norms has also established mechanisms to enforce those norms.[33] While contact tracing is a necessary tool in addressing COVID-19, these surveillance technologies can also be a very powerful tool of social control.[34] This is why societies tend to impose limits on the ability of authorities to place individuals under surveillance against their will or without their knowledge.[35]

The idea of a social contract to justify the violation of online rights stems from the realisation that increased ownership of our personal data does not guarantee us protection.[36] While we all have the right to, ordinarily, consent to the use of our data, the existence of this right has not protected us from national surveillance to address the current pandemic. The issue is not about how we can personally own our individual data and shut out others from accessing it, because our individual data on its own is not very useful, but when combined with other data it shapes societies and its impact varies across socioeconomic status, gender, ethnicity and religion.[37] For example, algorithms work by collecting vast amounts of data from numerous sources to create patterns and predict behaviour. That is why many of the problems around unfair uses of data cannot be solved by controlling who has access to it.[38]

The solution in the form of the social contract theory involves controlling not who has access to data, but how data is used morally, i.e. the use of data for our convenience and not to harm us. This is why the social contract theory works as justification for the violation of privacy rights online: the reassurance that what we give up as a collective is in exchange for the betterment of our navigation in the modern world, and during this pandemic, to protect and promote our right to good health.

33 K. N. C. (2019, 13 December). Surveillance is a fact of life, so make privacy a human right: Interview with Lawrence Capello. *The Economist*. https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

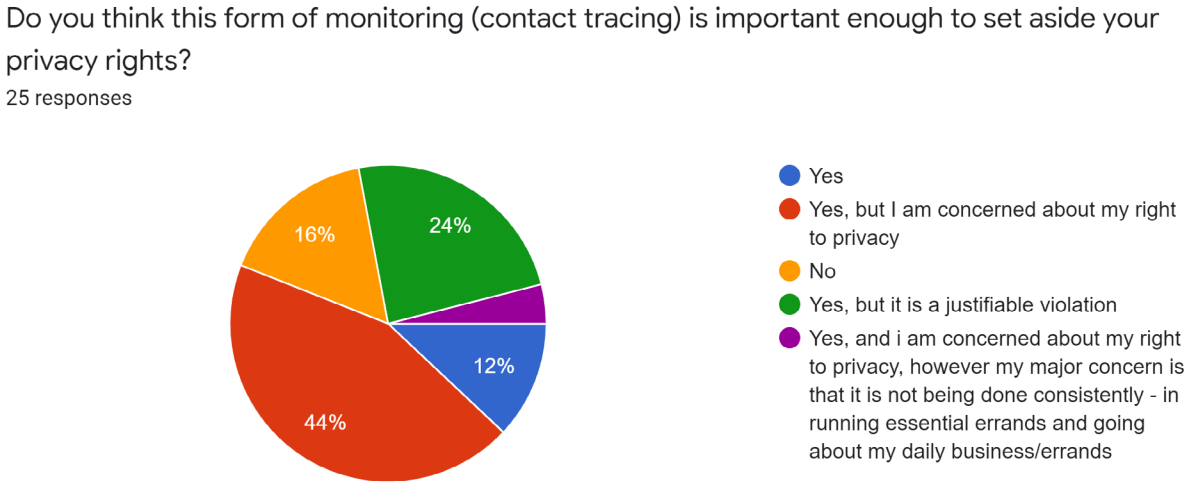
34 Ibid.

35 Ibid.

36 Tisne, M. (2018, 14 December). It's Time for a Bill of Data Rights. *MIT Technology Review*. https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights

37 Tisne, M. (2018, 14 December). Op. cit. and Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*. https://doi.org/10.1177%2F2053951717736335

38 Ibid.



↑ Contact Tracing and Privacy Rights
Source: Chenai Chair | Rumbidzai Matamba

The graph above indicates some willingness to renegotiate rights, and we are of the opinion that if we have more transparent systems in place, the public would be more comfortable with an exchange of the proportions brought about by the contact tracing initiatives on the right to privacy. Much like how we exchanged the right to be self-governing for the rule of law.

This social contract would work in conjunction with government regulations because tech companies cannot be left to devise their own ethics. The idea is to have a balance of power that regulates this exchange, much like how the executive, judiciary and legislature operate to facilitate and protect the guarantees contained in the South African constitution. If we can achieve this, data rights cease to just be about privacy, but also encompass the right to securing a space for individual freedom and agency while participating in modern society without discrimination or fear of who is collecting your data and what it will be used for.[39]

CONCLUSION

Using South African contact tracing initiatives – their shortfalls and justifications – this essay drew on the social contract theory to assess whether it could be used to justify negotiating privacy rights for purposes of assuring public health. The conclusion is that the idea of a social contract, whereby one trades off certain rights for a guarantee of their remaining rights, is viable as illustrated through the trade-off of some data rights for contact tracing for the purposes of responding to a public health crisis. This gives us some insight into how we can justify the sometimes unavoidable use of our data without our consent, and the protections that must be put in place to justify the violations. Continuous research is needed to assess where the public stands with this trade-off on privacy for public health to ensure justification for the social contract theory approach.

39 Tisne, M. (2018, 14 December). Op. cit. and Taylor, L. (2017). Op. cit.

While a new moral code is possible, a comprehensive solution between the public, public and private tech companies and the South African government is needed. It is highly recommended that the Director General of Health take a more decentralised approach when collecting the data for contact tracing and storing it for future use. This will mitigate the privacy concerns raised above. Therefore, one branch has to be tasked solely with collecting the data, another branch with de-identifying the data, and, perhaps, the information regulator overseeing these processes to limit privacy violations. It also requires transparency with the public and awareness raising of the process in play. A new social contract must be created, based on trust and cooperation and taking on a multistakeholder approach. For this, governments across the world must provide appropriate regulatory frameworks, which ensure that technologies are designed for use in ways that are compatible with, and for the advancement of, democracy.