Data Commercialisation in the South African Health Care Context

M Botes*, A Olckers** and M Labuschaigne***

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed,
open access online law publications

Authors

Marietjie Botes
Antonel Olckers
Melodie Labuschaigne

Affiliation

University of KwaZulu-Natal
DNAbiotec (Pty) Ltd, South Africa
Department of Jurisprudence, School of Law, University of South Africa

Email

maria.botes@uni.lu
AOlckers@DNAbiotec.com
slabbmn@unisa.ac.za

Date Submission

28 June 2020

Date Revised

28 July 2021

Date Accepted

28 July 2021

Date published

12 August 2021

Editor Prof C Rautenbach

How to cite this article

Botes M, Olckers A and Labuschaigne M "Data Commercialisation in the South African Health Care Context" *PER / PELJ* 2021(24) - DOI http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8577

DOI
http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8577

Abstract

Realisation of the value and the commercialisation potential of data is gaining exponential momentum. The combination of historical data exploitations and the use of technologies that allow for the triangulation of data results in the collection, storage, and processing of massive amounts of data require diligent data management, including adherence to privacy and other laws, both nationally and internationally. The intrinsic value of scientific data, especially in genomics, becomes apparent when data are shared, often in collaboration with international partners, and compiled into big data sets that are subsequently used for benefit, including commercial benefit. The purpose of this article is to explore the commercialisation of data in South Africa against the backdrop of the legal framework governing the protection of personal information, confidentiality and privacy, with a specific focus on genetic and genomic information. Related issues, such as the collection and sharing of data, ownership of data and challenges about informed consent are also considered. After a brief evaluation of the African regulatory landscape relating to the protection of personal information, the article concludes with a few recommendations aimed at improving the status quo and sensitising the South African public as to the value of their data and personal information, as well as the potential uses and abuses to which their personal information may be subjected.

Keywords

Data commercialisation; privacy protection; intellectual property; data sharing; data ownership; genomic research; *Protection of Personal Information Act* 4 of 2013.

.....

> Personal data has an economic value that can be bought, sold, and traded.[1]

1 Introduction

Like many authors before them, Eggers, Hamill, and Ali emphasised that data is a currency with a history of exploitation, vividly clear from the example of retailers paying US banks $1.7 billion a year by 2015 for sending out a "targeted discount offer" to bank clients, based on clients' credit and personal records.[2]

Today the value of data is comprehended, undoubtedly not fully by all, but links are being made visible between the absurd wealth of some companies and the data that was used to accrue this wealth. This scenario is set to change, however, in the face of a public becoming more and more aware of the value of their data, and that the currency they pay to use many of these so-called free services is their data.[3] The impact of this development is particularly significant in the health care context, as argued below.

The realisation of the value of data in its different stages of quality assurance, curation, complexity, and the possible triangulation with other data is slowly starting to be appreciated by the scientific community at large.[4] However, large technology companies in the space of data management had already started decades ago to exploit their advantage of having access to data that the public was, at the time, largely unaware of. The notion of services being free was one of the prevailing thoughts of the day, when in fact the hidden fee that they were paying in return for the

* Marietjie Botes. BProc LLB LLM LLD (Unisa). Postdoctoral Researcher, Health Law and Bioethics, School of Law, University of KwaZulu-Natal; and SnT Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg. E-mail: maria.botes@uni.lu. ORCiD: https://orcid.org/0000-0002-6613-6977.

** Antonel Olckers. BSc MSc (*cum laude*) PhD (UP). CEO, DNAbiotec (Pty) Ltd, South Africa. Email: AOlckers@DNAbiotec.com. ORCiD: https://orcid.org/0000-0002-4974-5666.

*** Melodie Labuschaigne. BA (Hons) (*cum laude*) MA (*cum laude*) DLitt (Pret) LLB (*cum laude*) LLD (Unisa). Professor in the Department of Jurisprudence, School of Law, University of South Africa. E-mail: slabbmn@unisa.ac.za. ORCiD: https://orcid.org/0000-0001-6581-7204.

1 Eggers, Hamill and Ali 2013 https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html. For more detail on the exploitation of personal data, see Elvy 2017 *Colum L Rev.*

2 Eggers, Hamill and Ali 2013 https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html. For more detail on the exploitation of personal data, see Elvy 2017 *Colum L Rev.*

3 Elvy 2017 *Colum L Rev*; ss 20, 24 and 26 of the *Medical Schemes Act* 131 of 1998; Discovery 2019 https://www.discovery.co.za/corporate/how-our-business-works.

4 Elvy 2017 *Colum L Rev.*

service was their data.[5] Industry may argue that their terms of service were never hidden as it was openly stated on their websites or online portals. It is difficult to envisage, however, that the public would understand the legal terms and implications of intellectual property clauses embedded in these terms of service, where the terms are often listed together, not allowing opt-in or opt-out for individual clauses. These data[6] were used to build big conglomerates that dominate the online landscape today. It is undeniable that these collected data were valuable and often not adequately protected, as became evident after the Facebook and Cambridge Analytica scandals came to light in March 2018.[7] Educating the public in developing countries may be a challenging task, considering other complexities and past practices where the public gave their data without explicitly being told what the impact would be over the long term.

The purpose of this article is to explore the commercialisation of data in South Africa against the backdrop of the legal framework governing the protection of personal information, confidentiality, and privacy, with a focus on the protection of genetic and genomic information. This requires a consideration of closely related issues, such as the commercial value of data, the collection and sharing of data, ownership rights associated with data and challenges about informed consent. For contextualisation and comparison with the South African position, the African regulatory landscape relating to the protection of personal information is briefly assessed, followed by recommendations aimed at improving the position and educating the South African public on the potential uses and abuses to which their personal information may be subjected and how possible abuses could be averted.

Due to the complexity of the different legal regimes for the protection of data as well as the interrelation between data protection, privacy and confidentiality, this article will focus on South Africa, but where relevant to illuminate a specific issue, reference is made to foreign jurisdictions.

2 Data collection and sharing

The collection of personal information has been amplified and expedited using digital technologies, whether through social networks, mobile phones, or the storage of individual profiles in electronic format in workplaces such

5 Elvy 2017 *Colum L Rev.*
6 Elvy 2017 *Colum L Rev.*
7 Wu 2015 https://www.newyorker.com/business/currency/facebook-should-pay-all-of-us.

as in the health sector or financial institutions. All this information is capable of being aggregated to create personal profiles of people. Often the identification of a person becomes possible because of the aggregation of large quantities of a variety of information or stored metadata across different contexts. This is a tipping point where the person's data cloud has become dense enough to render an individual identity.

Different legal approaches exist relating to permission to share personal information. The American legal framework for privacy and data protection differs significantly from the laws in other countries. Unlike the "opt-in" system as contemplated in article 7 and specified further in recital 32 of the European Union General Data Protection Regulation (GDPR),[8] the United States does not have one consolidated and comprehensive or omnibus statute pertaining to data protection and privacy, but rather several sector-specific and medium-specific national privacy or data security laws that apply to financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing.[9] In the European Union (EU), article 7 and recital 32 of the GDPR, the "opt-in" model is required to be the default, which requires that a person must give his or her explicit permission before an organisation can share the information. Europe's GDPR,[10] which came into operation in May 2018, is the first large-scale effort to offer consumers more legal protection of data.[11]

In South Africa protections like those contained in the GDPR are mirrored in the *Protection of Personal Information Act* (POPIA),[12] which aims to promote the protection of personal information processed by public and private bodies, as described in chapter 3 of the POPIA. Regulations to the POPIA, published in December 2018, are mainly administrative in nature and offer little guidance to organisations on how to interpret the Act.[13] The Information Regulator is tasked to establish the codes of conduct for sectors of society in which the relevant responsible parties are operating, where appropriate measures are laid down for protecting the lawful interests of

8 Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016).

9 DLA Piper 2021 https://www.dlapiperdataprotection.com/index.html?t=law&c=US.

10 Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016).

11 The GDPR is a regulation in European Union (EU) law on data protection and privacy for all individual citizens of the EU and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

12 *Protection of Personal Information Act* 4 of 2013 (POPIA).

13 Regulations Relating to the Protection of Personal Information (GN R1383 in GG 42110 of 14 December 2018).

data subjects on unsolicited electronic communications and automated decisions.[14] In the United Kingdom a new code of conduct for artificial intelligence (AI) was published in 2019 for the National Health Service (NHS), which aims to reassure patients and clinicians that data-driven technology is safe, effective and upholds privacy.[15] The new code will also allow for the NHS to be compensated for allowing companies access to its data pool to build life-saving AI systems.[16]

In the South African health care and health research context, personal information may be obtained directly from a patient or research participant with the patient's written consent.[17] Sections 11 and 12 of the POPIA provide that the disclosure of personal information without the person's consent, with a few legal exceptions as stipulated in section 27 of the POPIA, is unlawful in South Africa. In addition, a large amount of personal health information is also disclosed with patient consent through compelled authorisations, such as with insurance applications or claims, and employment or loan applications. Unfortunately, personal information, including personal health information, is often inadvertently shared or disclosed. Breach notification normally happens only if a data custodian or responsible person knows or is informed that a breach has occurred, but breaches may sometimes occur without any knowledge of both the responsible person and the data subject. The necessary steps to be taken in the event of a breach of security are detailed in the POPIA.[18]

The inadvertent and unknown disclosure of personal health information may also happen through peer-to-peer file sharing applications. There are different peer-to-peer clients that can search and download files from various networks.[19]

Of more concern lately has been the voluntary sharing of personal health information by individuals for direct-to-consumer genetic testing (DTC). DTC genetic testing refers to testing sold directly to consumers via the

14 Chapter 7, s 60(1) of POPIA.

15 Department of Health and Social Care 2019 https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs.

16 The code published in September 2018 contains ten principles setting out how the government will make it easier for companies to work with the National Health Service (NHS) and rules of engagement between the industry and healthcare system.

17 Sections 7, 14, 15 and 16 of the *National Health Act* 61 of 2003 (NHA) detail the written informed consent requirements and provide for the protection of personal information, confidentiality and access to and protection of health records.

18 Section 22 of POPIA.

19 El Emam *et al* 2010 *JAMIA*.

internet, television, or other marketing venues without involving health care professionals, which poses a threat to genetic privacy and the appropriate handling of the disclosure of genetic results.[20] Although most DTC genetic testing companies undertake not to share confidential genetic information with third parties without consumers' consent, these policies are usually self-imposed and not governed by laws.

When it comes to privacy and breaches of privacy, stored genetic data differs from other forms of personal data in that the breach potentially extends beyond the affected individual to the individual's genetic relatives. With the increasing use of biometrics in security systems, insecure storage of genetic data may pose yet unforeseen risks for consumers. The huge data breach of Fargo Wells where the information of more than 50 000 personally identifiable accounts was leaked, resulting in high-profile clients' fearing identity theft and suing Wells Fargo, serves as an example of the materialisation of such a data security risk.[21] In similar fashion, hackers may target genetic databases to acquire data than can be used in financial or identity fraud. Other risks associated with the use of genetic data include potential genetic discrimination resulting from sharing genetic information with third parties and sharing with law enforcement or government agencies without appropriate consent. At present the DTC genetic testing industry occupies a regulatory grey area in South African law. The lack of a sufficient number of genetic counsellors who assist people with understanding genetic tests results further complicates the problem, not to mention the concern that many of the tests offered online are not fit for purpose.[22]

When health risk assessments include the gathering of genomic information, these data become evergreen to the insurance entity if it insures subsequent generations of its current members, as the data remain informative over the extent of multiple generations.

Personal health information may furthermore be sourced via health risk assessments carried out by a range of actors in the public and private sphere, including employers, medical insurers, and public health departments, to name but a few. A health risk assessment is a health questionnaire used to provide individuals with an evaluation of their health risks and quality of life. A health risk assessment is one of the most widely

20 Su 2013 *Yale J Biol Med*.

21 McGlasson 2008 https://www.bankinfosecurity.com/wells-fargo-reveals-data-breach-a-944.

22 Phillips and Charbonneau 2016 https://www.ftc.gov/system/files/documents/public_comments/2015/10/00057-98101.pdf.

used screening tools in the field of health promotion and is often the first step in multi-component health promotion programmes. A 2016 privacy breach involving personal health information occurred when the Australian Federal Health Department made public data about Medicare claims, which included the services provided to almost 2.5 million patients and the providers of those services, unique patient identification numbers, gender, year of birth, and in which of four broad geographic regions the patient enrolled with Medicare.[23] Two years after the breach, parts of the information were illegally sold on the darknet.[24]

3 Some complexities related to healthcare data in the 4IR

Every commercial enterprise aims to provide goods and services in order to make a profit. This profit motive has expanded beyond the exclusive realms of health care practice into complementary services such as health insurance and its accompanying healthy lifestyle programmes. In terms of the South African *Medical Schemes Act* 131 of 1998, medical schemes are non-profit trusts owned by their members.[25] Although registered as such, medical schemes in South Africa make considerable profit and some are further expanding their business offerings to include banking, life insurance, investments, car and home insurance, all under a single roof.[26] These business models increasingly mirror private for-profit medical facilities and services, such as commercial diagnostic laboratories and private clinics.[27]

All persons, as they progress though their days, leave a trail of data behind, what we will refer to as their "personal data cloud".[28] This personal data

---

23 Pash 2018 https://www.businessinsider.com.au/data-breach-private-health-details-medicare-2018-3.

24 Karp 2019 https://www.theguardian.com/australia-news/2019/may/16/australians-medicare-details-illegally-sold-on-darknet-two-years-after-breach-exposed.

25 Sections 20, 24 and 26 of the *Medical Schemes Act* 131 of 1998.

26 Discovery 2019 https://www.discovery.co.za/corporate/how-our-business-works.

27 Hoedemaekers and Ten Have 1998 *Medicine, Healthcare and Philosophy.*

28 We define a "data cloud" as both the passive (unintentional) and active (intentional) digital footprint that is left behind, as also defined by Techterms 2014 https://techterms.com/definition/digital_footprint. The data one leaves behind are also referred to as "digital fingerprints", as defined by Joudeh and Bevilacqua 2017 https://www.forbes.com/sites/riskmap/2017/10/20/digital-fingerprints-the-data-you-leave-behind/?sh=4f19e7907bce. They are also referred to as "online breadcrumbs" as described by Outside Insight Date Unknown https://outsideinsight.com/insights/online-breadcrumbs-the-trail-individuals-leave-behind. Given that data are not defined in POPIA, the Cambridge Dictionary defines data as follows, and the term is used in this paper in a similar context: "information, especially facts or numbers, collected to be examined and considered and used to help decision making, or information in an electronic form that can be stored and used by a computer"

cloud of apparently unrelated and unlinked data, such as going to the pharmacy, buying provisions, the route taken between two points, is highly valuable to the right person or company, however. If many personal data clouds are combined, a picture appears of what consumer items are popular, which routes are popular and what healthcare or medical products are purchased most often. To an entity that trades in a specific product, for example genetic tests, a billboard on a more popular route near a medical facility is worth paying more for than a billboard on an unpopular route, thus a road not leading to a medical facility, since they can prime their potential customers via the billboard to think about their product once they enter the medical facility that can facilitate genetic testing. To some in the commercial sector, knowing how their products perform against other brands in both content and marketing (e.g. packaging, where in the store their product is located, etc.) is invaluable. Moreover, if genomic information is part of this "personal data cloud" the information could be evergreen[29] to health insurance providers. Inherited disorders could be unknown at first, but many insurance companies become aware of such disorders when additional family members also apply for insurance. The insurer will now have contextual information available from the additional family members as well as the genetic diagnoses of the first insurance applicant to enable the insurer to triangulate this information and make valuable deductions and/or predictions from it about the health of insurance applicants.

With sufficient data, and especially with machine learning[30] (as part of AI), which is now a mainstream tool, the value of these triangulated datasets has skyrocketed. Machine learning can analyse behaviour (data points) in real time and is able to unlock predictive and personalised targeting of specific consumers, such as consumers interested in taking genetic tests.[31] In the Fourth Industrial Revolution (4IR), machine learning processes staggering amounts of data in the blink of an eye. Most consumers depend heavily on the benefits of machine learning by means of predictive texting via their mobile devices such as asking for less congested routes on their satellite mapping services or receiving targeted advertisements because of the keywords typed into their internet search engines. Individually these data points are perhaps not valuable, but collectively they increase the

(Cambridge Dictionary 2021 https://dictionary.cambridge.org/dictionary/english/data).

29 Evergreen in this context means that the data remain valuable to the company year after year. Often the value of the data does not have an expiration date as it is valuable generation after generation.

30 Hao 2018 https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/.

31 Russell and Norvig *Artificial Intelligence* 1021.

density of an individual's personal data cloud over time, making it more valuable to businesses wishing to commercialise data sets by triangulating data, as discussed above, and predicting consumer behaviours to provide targeted services, such as genetic and other health-related testing to people who have indicated a need for it through their digital behaviour.

A different type of cloud, often referred to as a storage cloud, enables a device-decoupled working style for most users of online platforms, including scientists grappling with the challenges of big data sets.[32] The question of where this storage cloud is physically located, which has a significant impact on the applicable privacy regulations, was unfortunately initially ignored. The physical jurisdiction in which the storage cloud is located dictates how the data are governed. The complex issue of the cross-border transfer of data has confounded the problem, as the user and its data could be in different geographical areas and jurisdictions. Awareness of the difficulty embedded in disentangling this Gordian knot to effectively manage data has given rise to vigorous debate amongst data scientists, policy makers and regulators, including genomics[33] researchers, especially since the publication of the Draft South African Data and Cloud Policy.[34]

In South Africa most people use the storage cloud services offered by generally available commercial platforms. Regardless of the great potential such use carries, the legal and ethical consequences of using these platforms must still be adequately addressed. Cloud computing, machine learning, and cross-border data transfers are essential for innovation and it is foreseeable that their current complexities will merely evolve over time. In our view, it also seems unrealistic to hope to uncouple data-driven work from international commercial platforms and storage clouds. At present, though, the challenges inherent in the value and physical location of data remain unresolved.[35] In the light of the POPIA, that came into operation in South Africa on 1 July 2020, the complexities related to the value of personal data will multiply. The present challenge is to educate the public, as well as health scientists, healthcare providers and insurers providing lifestyle products that entail genetic testing, for instance, to ensure a satisfactory level of awareness and understanding of informational privacy rights.

---

32 Chang and Willis 2016 *Future Generation Computer Systems*.

33 "A branch of molecular biology concerned with the structure, function, evolution, and mapping of genomes" as defined by ASSAf 2018 http://dx.doi.org/10.17159/assaf.2018/0033.

34 Proposed National Data and Cloud Policy in terms of s 3(5) of the *Electronic Communications Act* 36 of 2005, published in GN 306 in GG 44389 of 1 April 2021.

35 Thorogood 2018 *Human Genetics*.

The above challenges have been exacerbated by the COVID-19 pandemic, which requires information to be gathered rapidly and shared globally to predict outbreaks of the disease and formulate management strategies to respond to it.

In 2018 Grossman[36] observed that: "the clash of privacy and value has been a long time coming. Frankly, it's shocking it's taken so long to come to fruition." He argues convincingly that the public have not been aware of the "loose" way in which platforms have used their data as payment, and have not paid sufficient care to protecting themselves, but that the tide is slowly turning. Consumers are starting to realise the almost incalculable value of their personal data and marketers will find it difficult to build trust with clients in future if their data were obtained in dubious ways or without their consent.

The 4IR, which is described as "a fusion of technologies that is blurring the lines between the physical, digital and biological spheres",[37] has created novel ethical and legal complexities, specifically regarding data protection and commercialisation. Current legal frameworks may not be ideally suited to address the range of legal and ethical issues that have arisen as a result.[38] Current laws relating to product licensing and certification, research and development oversight and tort or delictual liability may not be adequate to managing the risks associated with machine learning and AI in general.[39] The autonomous component of AI, moreover, creates complexities relating to foreseeability and control that might render traditional regulation ineffective.[40] Balancing the ever-increasing need for data with the protection of data and with privacy rights has become more critical and challenging than ever.

36 Grossman 2018 https://www.forbes.com/sites/forbesagencycouncil/2018/07/09/data-is-currency-dont-abuse-it/#2aadd1dd43d6.

37 Schwab 2016 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

38 Cath 2018 *Philos Trans A Math Phys Eng Sci*.

39 Scherer 2016 *Harv J L & Tech*.

40 See, in general, Cath 2018 *Philos Trans A Math Phys Eng Sci*; Russell and Norvig *Artificial Intelligence* 1021. Many people have been tricked into believing that they have been communicating with a real person whilst they were communicating with a computer, a fact which attracted the attention of law enforcement because of the ability to trick people into divulging enough personal information to enable their identity to be stolen.

4 Data processing and commercialisation by the insurance industry

The legal framework for the protection of the privacy and confidentiality of personal information in South Africa draws from a variety of sources, namely the *Constitution of the Republic of South Africa*, 1996, the common law, and different sets of legislation. Access to personal records is governed by the *Promotion of Access to Information Act*,[41] which provides for the right to access to records, including health records, held by public or private bodies, provided the access is for legitimate reasons. Access may be refused if the disclosure to "the relevant person might cause serious harm to his or her physical or mental health, or well-being."[42]

The *Electronic Communications and Transactions Act*,[43] which aims "to enable and to facilitate electronic communications and transactions in the public interest", provides for the penalisation of certain offences of unauthorised access to, interception of or interference with data. Chapter 8 of the Act deals with the protection of personal information obtained through electronic transactions and makes mandatory the express written permission of the data subject for the collation, processing, or disclosure of personal information, unless the data controller is permitted or required to do so by law, in which case s/he is excused from any consent requirements.

Like the legal and ethical difficulties caused by the creation of commercial products from human tissue, the commercialisation of genomic information poses significant dilemmas in the context of privacy and consent. In the case of *NM v Smith*[44] the South African Constitutional Court held (prior to the publication of the POPIA) that the rights to privacy and dignity of three women who are HIV-positive were violated by the publication of their names and HIV status in a biography of a South African politician.[45] This violation resulted from the fact that the publisher and authors of the biography were aware that the three women had not given their express consent, but ignored this and published their names and HIV status regardless thereof.[46] Although the special personal information of the three HIV-positive women was not *per se* commercialised, it was indirectly used for commercial purposes through the act of publishing it in the biography of a South African

41 *Promotion of Access to Information Act* 2 of 2000.
42 Sections 30 and 61 of the *Promotion of Access to Information Act* 2 of 2000.
43 *Electronic Communications and Transactions Act* 25 of 2002.
44 *NM v Smith 2007 5 SA 250 (CC) (NM v Smith).*
45 *NM v Smith* paras [46]-[47].
46 *NM v Smith* par [47].

politician without the women's consent. In a dissenting judgment O'Regan J held that the right to privacy protects citizens from the publication of private medical information without consent, but that this right had to be weighed against the right to freedom of expression.[47] The court stated that the privacy and dignity of the three women could have been sufficiently protected using pseudonyms, instead of the women's real names, which would not have rendered the book any less authentic. Using pseudonyms would not have diminished the commercial value of the book and would have met the de-identification requirement contained in the POPIA as discussed below.[48]

In another case preceding POPIA, *Mistry v Interim Medical and Dental Council of South Africa*,[49] the Constitutional Court highlighted some data protection guidelines, including whether or not the information was obtained in an intrusive manner; whether the information contained some intimate aspects of a subject's personal life; whether the information was provided for one purpose but used for another; and whether it was disseminated to the press or made public when the subject "could reasonably expect such information would be withheld."[50] The Court specifically left open the precise meaning of "search" and "property" in section 13 of the interim *Constitution of the Republic of South Africa Act* 200 of 1993 that provides for the right of privacy, which includes the right of persons not to have "(a) their person or home searched; (b) their property searched; (c) their possessions seized; (d) the privacy of their communications infringed" (now section 14 of the 1996 Constitution). The Court took the view that, even though it was not specifically mentioned in the constitutional right to privacy, the protection of informational privacy was included.[51]

Despite the existence of a legal framework that protects the privacy and confidentiality of personal information in a multi-layered manner, individuals often share their personal information voluntarily or inadvertently in contexts where their information is further processed, "packaged", sold, perpetually resold, or transferred to other parties for a variety of purposes, often without their knowledge or consent, as the discussion below will further elaborate.

47 *NM v Smith* paras [147]-[148].
48 *NM v Smith* paras [46], [61] and [111].
49 *Mistry v Interim Medical and Dental Council of South Africa* 1998 4 SA 1127 (CC) (*Mistry*).
50 *Mistry* para [51].
51 *Mistry* paras [47]-[48].

5 Why the sharing of genomic data is so unique and problematic

"Special personal information" as defined in section 32(5) of the POPIA also concerns "inherited characteristics", which include genomic information. This definition, coupled with the fact that section 32(1)(b)(ii) of the POPIA allows insurance companies to process such special personal information as part of their "performance of an insurance or medical scheme agreement; or the enforcement of any contractual rights and obligations" and causes great privacy concerns, particularly where health insurance companies create spin-off companies that use genetic information for commercial purposes and the establishment of intellectual property rights in genomic data sets. It is critical to establish ownership and differentiate between genetic samples, genomic information, and genomic data sets.

Genetic samples in this context usually consist of blood samples or cheek (buccal) swabs, which constitute biological material as defined in the Regulations Relating to the Use of Human Biological Material as "material from a human being including DNA, RNA, blastomeres, polar bodies, cultured cells, embryos, gametes, progenitor stem cells, small tissue biopsies and growth factors from the same."[52] The Regulations Relating to the Import and Export of Human Tissue, Blood, Blood products, Cultured Cells, Stem Cells, Embryos, Foetal Tissue, Zygotes and Gametes define a substance as "tissue, blood, blood product or gamete",[53] which includes genetic samples. Although ownership in genetic information is not provided for in South African legislation, the general practice is that genetic samples or "banked DNA is the property of the depositor unless otherwise stipulated",[54] that the biobank is the custodian of the DNA collection and that information extracted from it belongs to the researcher or team that creates it.[55]

In terms of the South African *Copyright Act*,[56] a "literary work", irrespective of the literary quality and in whatever mode or form expressed, includes tables and compilations, such as tables and compilations of data stored or

52 Regulations Relating to the Use of Human Biological Material, issued in terms of the NHA in GN R177 in GG 35099 of 2 March 2012.

53 Regulations Relating to the Import and Export of Human Tissue, Blood, Blood Products, Cultured Cells, Stem Cells, Embryos, Foetal Tissue, Zygotes and Gametes issued in terms of the NHA in GN R181 in GG 35099 97 of 2 March 2012.

54 American Society of Human Genetics 1988 *AJHG*.

55 MRC 2014 https://mrc.ukri.org/publications/browse/human-tissue-and-biological-samples-for-use-in-research/.

56 *Copyright Act* 98 of 1978.

embodied in a computer or a medium used in conjunction with a computer.[57] A curated data set consisting of genetic information subsequently qualifies as a literary work in which the creator of such a data set enjoys copyright that will enable him or her to reproduce the data set in any manner or form, publishing the data set and causing the data set to be transmitted in a diffusion service, thereby effectively commercialising it.[58] This intellectual property right is enjoyed by the creator of the data set to the exclusion of the data subject. Although legal, the ethical nature of such commercial action is contentious, given that a full genome sequences cannot be anonymised. It is imperative to add a clause in future Data Sharing Agreements and Codes of Conduct that "no steps be taken to reverse the de-identification of genomic data."

Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations are lawfully permitted to seek access to a data subject's health or sex life to enable them to assess the risk to be insured by the insurance company or covered by the medical scheme, but subject to the data subject's not objecting to such processing.[59] Failure to object to such collection of information implies that the data subject was properly informed and provided with sufficient information to enable the data subject to either accept such information collection, alternatively to object to same. As stipulated in section 26, an appropriate family medical history, reports from general practitioners where relevant to applications for health-related policies, such as life insurance, critical illness and income protection insurance may be accessed, provided such access complies with the requirements for data protection.

Considering the above privacy and consent concerns, it is significant that 73.17 per cent of the respondents in a 2017 Swiss study on the open sharing of genomic data conducted by Haeusermann and others stated that they had either not read, or only quickly read over the terms and conditions for sharing their data while registering on openSNP.[60] It must be emphasised that the responsible party bears the burden of proof for the data subject's consent.[61] By implication, the responsible party must ensure that data subjects actually engage with the information provided to ensure sufficient

57 Definitions, s 1 – "Literary Works" (g), *Copyright Act* 98 of 1978 as amended by s 50(e) of the *Intellectual Property Laws Amendment Act* 38 of 1997.

58 Section 6 of the *Copyright Act* 98 of 1978.

59 Section 32(1)(b), Form 1 "Objection to the processing of personal information in terms of Section 11(3)" [Regulation 2] of the Regulations Relating to the Protection of Personal Information (GN R1383 in GG 42110 of 14 December 2018).

60 Haeusermann *et al* 2017 *PLoS One*.

61 Section 11(2)(a) of the POPIA.

comprehension and subsequent ethical, legal and properly informed consent. Many of the respondents in this study indicated that they would be very concerned (38.60 per cent) if employers or insurance companies should use their genotype or data to their disadvantage, although 48.54 per cent thought that such a scenario is very unlikely. Employees and the insured may be ill-informed of what can possibly be done with their genomic data, but are willing to provide consent relatively easily, nonetheless. The question of whether their consent was indeed informed is valid.

As alluded to above, the main concerns relating to direct-to-consumer or insurance genomic tests have to do with whether such tests bring any personal or clinical utility and whether the commercial availability of such tests threatens consumers or paves the way towards an increase in individual autonomy.[62] These issues must be considered within the current regulatory frameworks.

South Africans enjoy constitutionally protected rights to have their dignity respected and protected, and to bodily and psychological integrity, which includes the right to make decisions concerning reproduction and privacy,[63] as detailed in the POPIA and the *National Health Act* 61 of 2003 (NHA). All genomic and health information collected, processed, and shared affects these constitutional rights.

The NHA stipulates that all information regarding a patient and his or her health status must be kept confidential and that disclosure thereof may occur only with the patient's written consent; when necessary for a legitimate public interest; by court order; or under statutory obligation.[64] Disclosure for a legitimate purpose where access is in the patient's best interest and only when necessary is permitted,[65] whilst human biological material may also be removed or withdrawn from living persons for DNA, RNA and genetic testing for medical or dental purposes.[66] Similar permissions are found in the POPIA, which allows insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations to process health information if it is necessary for assessing

62 Vayena 2014 *J Med Ethics.*

63 Section 10, 12(2)(a) and 14 of the *Constitution of the Republic of South Africa*, 1996.

64 Section 14 of the NHA.

65 Section 15 and 16 of the NHA; written informed consent of the user or donor is obtained for long-term storage of genetic material, stem cells or research findings.

66 Regulation 5(a) "Use of human biological material" in the Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012).

the risk to be insured by the insurance company or covered by the medical scheme, including genetic testing.[67]

Cross-border sharing of health or genomic information from South Africa for commercial purposes has already proved to be problematic when not managed correctly from a regulatory point of view. In 2013 blood samples and data obtained from South African research sites were shared with Stanford University in the United States and the Wellcome Sanger Institute in the UK, strictly in terms of the research protocol and export permits and based on consent provided for research into population history and human evolution.[68] However, the whistle was blown on Sanger's negotiations with Thermo Fisher Scientific® to make microarrays using the said African data to provide a commercially cheaper form of rapid genetic testing as opposed to whole genome sequencing. The GDPR adopted by the UK and the POPIA provide similar and subsequently adequate levels of privacy protection as required by section 72 of the POPIA to allow lawful cross-border data transfers between these countries. Both the POPIA in section 13 and recital 33 in the GDPR require purpose specificity to the extent that any informed consent obtained must relate to a specific purpose or research project such as the population history and human evolution.[69]

Unfortunately, the consent obtained in the Thermo Fisher Scientific® research project did not contain consent for data to be transferred to Thermo Fisher®, neither was there any Data Transfer Agreement (DTA) providing for the commercial use of any data transferred, which drove the South African researchers involved to demand the return of all samples and data based on a complete lack of explicit informed consent to commercialise any of the genetic material and/or data described in the existing Material Transfer Agreement (MTA). Collaborative research projects like this one could ultimately serve legitimate health care purposes, which would benefit members of insurance companies, thereby expanding the scope of the use of samples and data collected by insurance companies in terms of POPIA. The scope will be expanded from allowing the processing of special personal information only for risk assessment, but – with the necessary consent – will also allow for the development of commercially viable health diagnostics or health care products. In our view the above highlights the

67 Section 32(1)(b) of the POPIA.

68 Njilo 2019 https://www.timeslive.co.za/news/south-africa/2019-10-16-stellenbosch-university-demands-return-of-dna-samples-but-uk-lab-hits-back/.

69 POPIA and Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016).

necessity for a DTA to be in place when the cross-border sharing of health or genomic data takes place.

Authorised institutions[70] deal with human biological material and subsequent data resulting from training of students in the health sciences, health research, the advancement of health sciences, therapeutic purposes and the production of therapeutic, diagnostic or prophylactic substances;[71] and keep or disclose genetic material records and other individually identifiable or related health information in any form.[72] They may release information to health insurers if a user's[73] written consent has been obtained.[74] Health insurers are allowed to legally obtain health and genetic information from authorised institutions such as biobanks which in turn would have obtained the informed consent of the user or donor for the long-term storage of genetic material, stem cells or research findings.[75] It is alarming that this regulation requires the information to be treated anonymously only if it is used for research purposes,[76] suggesting that health insurers could easily obtain identified or identifiable information for the purposes stated in their insurance agreements with people who applied to be insured to determine their risk, and possibly commercialise such material or data as described above, based on the terms contained in the insurance policy which are generally bundled and cannot be individually negotiated by a client. Only health care providers or planners are obliged to provide users with a clear explanation of how the user can use, keep and disclose their information.[77] However, the long-term consent requirement is applicable with regard to storage only, and the standard consent

70 Section 54(1) of the NHA authorises the Minister of Health, by notice in the Gazette, to designate any institution other than an institution contemplated in s 63 as an authorised institution.

71 Section 64(1) of the NHA.

72 Regulation 13 "Storage and control of flow of genetic information" in the Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012).

73 "User" means the person receiving treatment in a health establishment, including receiving blood or blood products, or using a health service (s 1 of the NHA).

74 Regulation 13(d) "Storage and control of flow of genetic information" in the Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012).

75 Regulation 13(f) "Storage and control of flow of genetic information" in the Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012).

76 Regulation 13(h) "Storage and control of flow of genetic information" in the Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012).

77 Regulation 13(b) "Storage and control of flow of genetic information" in the Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012).

requirements as contemplated in the POPIA, which oblige the health insurer to explicitly define the lawful purpose for their collection of the user's information and ensure that the user is aware of the purpose of such collection still apply.[78]

Health insurers are further entitled to process data relating to their members' special personal information for the performance of an insurance or medical scheme agreement, or the enforcement of any contractual rights and obligations,[79] such as those contained in insurance and data transfer agreements. During the processing of data in terms of a written agreement between the responsible party and the data subject, the data must be kept confidential.[80] To ensure that these agreements between both responsible parties and data subjects (insurance contracts) and responsible parties and third parties (data transfer agreements) are POPIA compliant, the consent of the data subjects must be obtained pertaining specifically to the possible commercialisation of the data.

Genomic information, on the other hand, may be lawfully processed only if a serious medical interest prevails or is necessary for historical, statistical or research activity.[81] The processing of special personal information is allowed if it happens with the medical treatment and/or care of the individual in mind. In this regard, insurers may foreseeably argue that genomic testing is necessary to inform the treatment or care plans of their members, and therefore justify genomic testing in circumstances other than those limited to serious medical conditions. Care plans, in contrast to treatment plans, which suggest that they have a medical nature, can possibly be interpreted to suggest that genomic testing can be applied to inform healthy lifestyle programmes to enhance the quality of life and longevity, to the benefit of various insurers' business philosophies and financial models.

In 2018 South Africa built the African Genomics Centre in terms of an agreement between the South African Medical Research Council (SAMRC) and the Beijing Genomics Institute (BGI).[82] This collaboration aims to strengthen bilateral relations between China and South Africa. Such collaborations and science capacities to decode large quantities of genetic

78 Sections 13(1) and (2) of the POPIA.
79 Sections 32(1)(b)(ii) and (iii) of the POPIA.
80 Section 32(2) of the POPIA.
81 Sections 32(5)(a) and (b) of the POPIA.
82 SAMRC 2018 http://www.mrc.ac.za/media-release/genomics-centre-cape-town-decode-genes.

samples are invaluable to insurers, for instance, if they can gain access to curated genomic data for their commercial purposes.

The POPIA prohibits the transfer of any personal information to third parties in foreign countries unless the foreign recipient of information is subject to a law, binding corporate rules,[83] or a binding agreement which provides an adequate level of protection that is substantially similar to the conditions for the lawful processing of personal information provided for in the POPIA.[84] South Africa's collaboration with China and the sharing of genetic samples and information between these countries both holds promise and offers challenges. The People's Republic of China has a complex framework of laws that includes some issues of privacy used to interpret data protection in the context of rights to reputation and privacy, instead of a single comprehensive data protection law.[85] This regulatory framework does not provide levels of information protection like those required by POPIA.

The United States also does not provide information protection commensurate with that provided in terms of the POPIA. The GDPR of the EU made its appearance in a US Supreme Court in the case of *United States v Microsoft.*[86] The issue was raised whether the United States may issue a search warrant to a US-based electronic communications service for data held on a server in Ireland. The case was based on a 2016 ruling in favour of Microsoft and other technology companies confirming the limitation of the geographic reach of the *Stored Communications Act*[87] to data stored in the US. What is of importance from a data privacy point of view is the court's determination "that EU law does not recognise the US legal regime as upholding Europe's 'fundamental right to privacy'".[88]

In 2015 US privacy laws again received intense attention in the case of *Maximillian Schrems v Data Protection Commissioner*.[89] As a European citizen, Mr Schrems lodged a complaint with the Irish Data Protection

---

83 Section 72(2)(a) of the POPIA. "Binding corporate rules" means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country.

84 Chapter 9 "Transborder information flows", s 72(1)(a) of the POPIA.

85 DLA Piper 2019 https://www.dlapiperdataprotection.com/index.html?t=law&c=CN.

86 *United States v Microsoft* 584 US (2018).

87 *Stored Communications Act* 18 USC 2701.

88 Phillips 2018 https://www.lexology.com/library/detail.aspx?g=42443820-3143-4ed5-9b50-b251899fad18.

89 *Maximillian Schrems v Data Protection Commissioner* Case C-362/14 (Judgement: 6 October 2015).

Commissioner when the data he provided to Facebook was wholly or partially transferred for processing from Facebook's Irish subsidiary to servers situated in the US. Mr Schrems's main concern was that the privacy laws and practices in the US did not provide adequate protection against surveillance by the US public authorities. The US does not have comprehensive data protection laws and consequently does not meet the test for adequate data protection as contemplated in the EU GDPR.[90] The Court of Justice of the European Union (CJEU), who adjudicated this case, agreed that the protective rules laid out in the data sharing arrangement between the EU and the US (known as the "Safe Harbour Decision") could actually be disregarded by the US when and where they conflicted with US national security, public interest and law enforcement requirements.[91] The CJEU ruled that any legislation permitting public authorities to access the content of electronic communications on a general basis is considered to compromise the very essence of the right to privacy and thus declared the Safe Harbour agreement between the EU and the US invalid.[92] In a further effort to allow the free flow of data between the EU and US, the EU and US have entered into the EU-US Privacy Shield. However, on 16 July 2020 the European Court of Justice also struck down this privacy shield, stating that US national security and law enforcement still interferes with and offers little protection to the data of European citizens whose data is transferred to the US.[93]

South Africa's POPIA closely resembles the EU GDPR. It is fair to deduce from the above that if US laws fail to uphold the EU's rights to privacy, US laws will in all probability also fail to provide the adequate level of privacy protection expected from POPIA and the GDPR, specifically regarding the protection of genetic and genomic information.[94] These challenges also arise when contemplating transferring personal information to other African

---

90 *Maximillian Schrems v Data Protection Commissioner* Case C-362/14 (Judgement: 6 October 2015).

91 *Maximillian Schrems v Data Protection Commissioner* Case C-362/14 (Judgement: 6 October 2015).

92 Gibbs 2015 https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

93 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* Case C-311/18.

94 There is a limited number of US federal laws governing the use of genetic data in certain circumstances, which include the *Genetic Information Non-Discrimination Act*, 2008; the *Affordable Care Act*, 2010; the *US Common Rule,* 1991; *Health Insurance Portability and Accountability Act*, 1996 (HIPAA); and the *21st Century Cures Act*, 2016. None of these laws explicitly ensures privacy or security with regard to how genetic information can be accessed, disclosed, or utilised. Dousa 2020 https://www.ccg.ai/blog/genetic-data-privacy-and-peril.

countries, given that many African countries presently do not have data protection laws in place.

The below table summarises the current personal data protection regulatory landscape in Africa:

Table 1: Africa personal data protection regulatory landscape[95]

Country	Has data privacy protection	Constitutional coverage	No data protection	Cross-border data transfer restrictions
Algeria	---	---	Yes	---
Angola	Yes	---	---	Yes
Benin	Yes	---	---	Yes
Botswana	---	---	Yes	---
Burkina Faso	Yes	---	---	Yes
Burundi	---	---	Yes	---
Cabinda	---	Yes	---	---
Cameroon	---	---	Yes	---
Cape Verde Islands	Yes	---	---	---
Central African Republic		---	Yes	---
Chad		---	Yes	---
Comoros	Yes	---	---	---
Congo-Brazzaville		---	Yes	---
Côte d'Ivoire	Yes	---	---	Yes
Democratic Republic of the Congo	---	---	Yes	---

95 Deloitte 2017 https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf.

Country	Has data privacy protection	Constitutional coverage	No data protection	Cross-border data transfer restrictions
Djibouti	---	---	Yes	---
Egypt	In process	---	---	---
Equatorial Guinea	---	---	Yes	---
Eritrea	---	---	Yes	---
Ethiopia	---	Yes	---	---
Gabon	Yes	---	---	Yes
Ghana	Yes	---	---	Yes
Guinea-Bissau	---	---	Yes	---
Guinea	---	---	Yes	---
Kenya	In process	---	---	---
Lesotho	Yes	---	---	Yes
Liberia	---	---	Yes	---
Libya	---	---	Yes	---
Madagascar	Yes	---	---	Yes
Mali	Yes	---	---	Yes
Mauritius	Yes	---	---	Yes
Mauritiania	In process	---	---	---
Mayotte	---	---	Yes	---
Morocco	Yes	---	---	Yes
Mozambique	---	---	Yes	---
Namibia	---	Yes	---	---
Niger	In process	---	---	---

Country	Has data privacy protection	Constitutional coverage	No data protection	Cross-border data transfer restrictions
Nigeria	In process	---	---	---
Reunion	---	---	Yes	---
Rwanda	Yes	---	---	---
Sao Tome	---	---	Yes	---
Senegal	Yes	---	---	Yes
Seychelles	Yes	---	---	Yes
Sierra Leone	---	Yes	---	---
Somalia	---	---	Yes	---
South Sudan	---	---	Yes	---
Sudan	---	---	Yes	---
South Africa	Yes	Yes	---	Yes
Swaziland	---	Yes	---	---
Tanzania	In process	---	---	---
The Gambia	Yes	---	---	---
Tunisia	Yes	---	---	Yes
Togo	---	---	Yes	---
Uganda	In process	---	---	---
Western Sahara	Yes	---	---	Yes
Zambia	---	---	Yes	---
Zanzibar	Yes	---	---	---
Zimbabwe	In process	---	---	---

In an effort to safeguard African biospecimens and the related data, the Alliance for Accelerating Excellence in Africa (AESA) established the Data and Biospecimen Governance Committee to review the tabulated governance framework and issues pertaining to the use and re-use of data and biospecimens originating from African sources, and to create "a pan-African normative framework that reconciles competing societal, individual and industries' interests in data and bioresources, ensuring fair access while minimising legal and ethical risks."[96] Considering the judgement by the CJEU in the Schrem's-case and its consequences on data sharing with foreign countries, this newly established committee will be investigating technologies to better track and trace samples and data to determine their origin, validate their quality, and assess the methods of ensuring that the consents and use agreements under which samples and data are being collected, generated and re-used are providing adequate and specific privacy protection.

Technologies such as blockchain should in principle be able to create a digital trust network that can protect the chain of custody over biospecimens and related data on their route through an innovation network which may ultimately lead to commercialisation.[97] This technology will allow for the keeping of a transparent record of the ownership of data, the consent given, intellectual property rights (IPRs) and the ethical and legal sharing of the data while establishing accountability for any misuse or unethical treatment of biospecimens or the related data.[98] If a foreign country does not provide adequate levels of protection, responsible parties must ensure that additional safeguards such as DTAs and specified consent are initiated to ensure that the privacy of data subjects are sufficiently protected. The EU GDPR prescribes certain requirements with which DTAs must comply, such as specific provisions, data descriptions, the controller's obligations and rights, amongst others.[99] The POPIA does not contain any provisions regarding DTAs, but it is recommended that the EU GDPR guidelines and requirements be followed or adapted when necessary.[100]

Fortunately, the POPIA makes provision for the Information Regulator "to facilitate cross-border cooperation in the enforcement of privacy laws by

96 AESA 2020 https://www.aasciences.africa/sites/default/files/Publications/Recommendations%20for%20Data%20and%20Biospecimen%20Governance%20in%20Africa.pdf.

97 Grishin *et al* 2018 *BHTY*.

98 Tiffin, George and LeFevre 2019 *BMJ Global Health*.

99 Taylor Wessing Global Data Hub 2018 https://globaldatahub.taylorwessing.com/article/data-transfer-agreements.

100 EU Date Unknown https://gdpr.eu/data-processing-agreement/.

participating in any initiative that is aimed at such cooperation."[101] This facilitative authority in collaboration with the AESA Data and Biospecimen Governance Committee, stakeholder engagement and an analysis of existing legislation in other African countries as tabulated above will lead to better scientific collaboration to benefit global health agendas if samples and related data can be shared with other African countries effectively whilst ensuring the protection of individuals' special personal information, which are some of the goals included in Regulator's 2017-2020 Strategic Plan.[102] After properly analysing the extent of the privacy that the countries listed in the above table are providing, and whether it can be considered adequate in relation to the POPIA, the Regulator could follow the example of the Privacy Commissioner for Personal Data in Hong Kong, who prepared a "white list" of places with data protection laws that are in force and provide substantially similar protection.[103] This certainty would make the sharing and commercialisation of samples and related data across borders in Africa fast, effective, and lawful.

6 Conclusion

The question regarding the commercialisation of data in the South African health care and health research context is intricately related to issues of informed consent, access to and the sharing of data, as well as privacy and the confidentiality of personal information. The value of data or personal information in its raw and processed form has been increased by advanced developments in 4IR, including AI and blockchain, creating novel legal and ethical issues. Despite the existence of South Africa's legal framework, which protects the privacy and confidentiality of personal information in a comprehensive and multi-layered manner, individuals continue to share their personal information, including their health information, voluntarily or inadvertently in contexts where their information is further processed, packaged, sold, perpetually resold, or transferred to other parties for many purposes, often without their knowledge or specific consent. This paper expresses some concerns regarding developments in genomic research in South Africa which raise questions regarding the adequacy of the levels of protection provided for South African data subjects in terms of POPIA, especially when viewed through the lens of commercialisation. This paper highlights the current developments and recommends that the South African

101 Section 40(1)(g) of the POPIA.

102 Information Regulator 2017 https://www.justice.gov.za/inforeg/docs/InfoRegSA-2017-2020StrategicPlan.pdf.

103 Greenleaf 2017 https://ssrn.com/abstract=3000766 5.

Information Regulator develop a list of jurisdictions offering adequate conditions for the lawful processing of personal information, or conditions similar to those provided by POPIA, especially in Africa, to promote ethical and legal scientific collaboration.[104] The South African public should also be sensitised as to the value of their data and personal information. They should also be informed of the potential uses and abuses to which their information may be subjected, to enable them to make sure that the consent forms or other agreements such as insurance policies that they sign allow the use of their data in line with their specific consent.

Bibliography

Literature

American Society of Human Genetics 1988 *AJHG*
American Society of Human Genetics, Ad Hoc Committee on DNA Technology "DNA Banking and DNA Analysis: Points to Consider" 1988 *AJHG* 781-783

Cath 2018 *Philos Trans A Math Phys Eng Sci*
Cath C "Governing Artificial Intelligence: Ethical, Legal, and Technical Opportunities and Challenges" 2018 *Philos Trans A Math Phys Eng Sci* 1-8 https://doi.org/10.1098/rsta.2018.0080

Chang and Willis 2016 *Future Generation Computer Systems*
Chang V and Willis G "A Model to Compare Cloud and Non-Cloud Storage of Big Data: Future Generation Computer Systems" 2016 *Future Generation Computer Systems* 56-76

El Emam *et al* 2010 *JAMIA*
El Emam K *et al* "The Inadvertent Disclosure of Personal Health Information through Peer-to-Peer File Sharing Programs" 2010 *JAMIA* 148-158

Elvy 2017 *Colum L Rev*
Elvy S "Paying for Privacy and the Personal Data Economy" 2017 *Colum L Rev* 1369-1454

Grishin *et al* 2018 *BHTY*
Grishin D *et al* 2018 "Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-

104 ASSAf 2018 http://dx.doi.org/10.17159/assaf.2018/0033.

Preserving Technologies and Equitable Compensation" 2018 *BHTY* 1-23 http://dx.doi.org/10.30953/bhty.v1.34

Haeusermann *et al* 2017 *PLoS One*
Haeusermann T *et al* "Open Sharing of Genomic Data: Who Does It and Why?" 2017 *PLoS One* 1-15 https://doi.org/10.1371/journal.pone.0177158

Hoedemaekers and Ten Have 1998 *Medicine, Healthcare and Philosophy*
Hoedemaekers R and Ten Have H "Commercialisation of Genetic Diagnostic Services" 1998 *Medicine, Healthcare and Philosophy* 217-224

Russell and Norvig *Artificial Intelligence*
Russell SJ and Norvig P *Artificial Intelligence: A Modern Approach* 3rd ed (Pearson Prentice Hall Harlow 2010)

Scherer 2016 *Harv J L & Tech*
Scherer UM "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" 2016 *Harv J L & Tech* 353-400

Su 2013 *Yale J Biol Med*
Su P "Direct-to-Consumer Genetic Testing: A Comprehensive View" 2013 *Yale J Biol Med* 359-365

Thorogood 2018 *Human Genetics*
Thorogood A "Canada: Will Privacy Rules Continue to Favour Open Science?" 2018 *Human Genetics* 595-602

Tiffin, George and LeFevre 2019 *BMJ Global Health*
Tiffin N, George A and LeFevre AE "How to Use Relevant Data for Maximal Benefit with Minimal Risk: Digital Health Data Governance to Protect Vulnerable Populations in Low-Income and Middle-Income Countries" 2019 *BMJ Global Health* 1-9 http://dx.doi.org/10.1136/bmjgh-2019-001395

Vayena 2014 *J Med Ethics*
Vayena E "Direct-to-Consumer Genomics on the Scales of Autonomy" 2014 *J Med Ethics* 310-314

Case law

European Union

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems Case C-311/18

Maximillian Schrems v Data Protection Commissioner Case C-362/14 (Judgement: 6 October 2015)

South Africa

Mistry v Interim Medical and Dental Council of South Africa 1998 4 SA 1127 (CC)

NM v Smith 2007 5 SA 250 (CC)

United States

United States v Microsoft 584 US (2018)

Legislation

South Africa

Constitution of the Republic of South Africa Act 200 of 1993

Constitution of the Republic of South Africa, 1996

Copyright Act 98 of 1978

Electronic Communications Act 36 of 2005

Electronic Communications and Transactions Act 25 of 2002

Intellectual Property Laws Amendment Act 38 of 1997

Medical Schemes Act 131 of 1998

National Health Act 61 of 2003

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

United States

21st Century Cures Act, 2016

Affordable Care Act, 2010

Genetic Information Non-Discrimination Act, 2008

Health Insurance Portability and Accountability Act, 1996

Stored Communications Act 18 USC 2701

US Common Rule, 1991

Government publications

European Union

Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)

South Africa

Proposed National Data and Cloud Policy (GN 306 in GG 44389 of 1 April 2021)

Regulations Relating to the Import and Export of Human Tissue, Blood, Blood Products, Cultured Cells, Stem Cells, Embryos, Foetal Tissue, Zygotes and Gametes (GN R181 in GG 35099 97 of 2 March 2012)

Regulations Relating to the Protection of Personal Information (GN R1383 in GG 42110 of 14 December 2018)

Regulations Relating to the Use of Human Biological Material (GN R177 in GG 35099 of 2 March 2012)

Internet sources

AESA 2020 https://www.aasciences.africa/sites/default/files/Publications/Recommendations%20for%20Data%20and%20Biospecimen%20Governance%20in%20Africa.pdf

Alliance for Accelerating Excellence in Science in Africa 2020 *Recommendations for Data and Biospecimen Governance in Africa - ASP Policy Paper 3* https://www.aasciences.africa/sites/default/files/Publications/Recommendations%20for%20Data%20and%20Biospecimen%20Governance%20in%20Africa.pdf accessed 2 July 2021

ASSAf 2018 http://dx.doi.org/10.17159/assaf.2018/0033

Academy of Science of South Africa 2018 *Human Genetics and Genomics in South Africa: Ethical, Legal and Social Implications* http://dx.doi.org/10.17159/assaf.2018/0033 accessed 9 March 2021

Cambridge Dictionary 2021 https://dictionary.cambridge.org/dictionary/english/data
Cambridge Dictionary 2021 *Data* https://dictionary.cambridge.org/dictionary/english/data accessed 9 March 2021

Deloitte 2017 https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf
Deloitte 2017 *Privacy is Paramount: Personal Data Protection in Africa* https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf accessed 30 June 2019

Department of Health and Social Care 2019 https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs
Department of Health and Social Care 2019 *New Code of Conduct for Artificial Intelligence (AI) Systems Used by the NHS* https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs accessed 20 May 2019

Discovery 2019 https://www.discovery.co.za/corporate/how-our-business-works
Discovery 2019 *How Our Business Works* https://www.discovery.co.za/corporate/how-our-business-works accessed 24 June 2019

DLA Piper 2019 https://www.dlapiperdataprotection.com/index.html?t=law&c=CN
DLA Piper 2019 *Data Protection Laws of the People's Republic of China* https://www.dlapiperdataprotection.com/index.html?t=law&c=CN accessed 30 June 2019

DLA Piper 2021 https://www.dlapiperdataprotection.com/index.html?t=law&c=US
DLA Piper 2021 *Data Protection Laws of the World: United States* https://www.dlapiperdataprotection.com/index.html?t=law&c=US accessed 15 February 2021

Dousa 2020 https://www.ccg.ai/blog/genetic-data-privacy-and-peril
Dousa B 2020 *Genetic Data, Privacy, and Peril: A Call for Greater Protections Amongst the US's Fractured Legal Landscape* https://www.ccg.ai/blog/genetic-data-privacy-and-peril accessed 17 February 2021

Eggers, Hamill and Ali 2013 https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html
Eggers WD, Hamill R and Ali A 2013 *Data as the New Currency: Government's Role in Facilitating the Exchange* https://www2.deloitte.com/insights/us/en/deloitte-review/issue-13/data-as-the-new-currency.html accessed 11 July 2019

EU Date Unknown https://gdpr.eu/data-processing-agreement/
European Union Date Unknown *Data Processing Agreement (Template)* https://gdpr.eu/data-processing-agreement/ accessed 30 June 2019

Gibbs 2015 https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection
Gibbs S 2015 *What is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?* https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection accessed 19 February 2021

Greenleaf 2017 https://ssrn.com/abstract=3000766
Greenleaf G 2017 *2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws: Trade and Human Rights Perspectives - UNSW Law Research Paper No 17-47* https://ssrn.com/abstract=3000766 accessed 2 July 2021

Grossman 2018 https://www.forbes.com/sites/forbesagencycouncil/2018/07/09/data-is-currency-dont-abuse-it/#2aadd1dd43d6
Grossman J 2018 *Data is Currency, Don't Abuse It* https://www.forbes.com/sites/forbesagencycouncil/2018/07/09/data-is-currency-dont-abuse-it/#2aadd1dd43d6 accessed 11 July 2019

Hao 2018 https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/
Hao K 2018 *What is Machine Learning?* https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/ accessed 9 March 2021

Information Regulator 2017 https://www.justice.gov.za/inforeg/docs/InfoRegSA-2017-2020StrategicPlan.pdf
Information Regulator 2017 *2017-2020 Strategic Plan* https://www.justice.gov.za/inforeg/docs/InfoRegSA-2017-2020StrategicPlan.pdf accessed 30 June 2019

Joudeh and Bevilacqua 2017 https://www.forbes.com/sites/riskmap/2017/10/20/digital-fingerprints-the-data-you-leave-behind/?sh=4f19e7907bce

Joudeh M and Bevilacqua J 2017 *Digital Fingerprints: The Data You Leave Behind* https://www.forbes.com/sites/riskmap/2017/10/20/digital-fingerprints-the-data-you-leave-behind/?sh=4f19e7907bce accessed 2 July 2019

Karp 2019 https://www.theguardian.com/australia-news/2019/may/16/australians-medicare-details-illegally-sold-on-darknet-two-years-after-breach-exposed

Karp P 2019 *Australians' Medicare Details Illegally Sold on Darknet: Two Years After Breach Exposed* https://www.theguardian.com/australia-news/2019/may/16/australians-medicare-details-illegally-sold-on-darknet-two-years-after-breach-exposed accessed 11 July 2019

McGlasson 2008 https://www.bankinfosecurity.com/wells-fargo-reveals-data-breach-a-944

McGlasson L 2008 *Wells Fargo Reveals Data Breach: Thousands of Consumer Records Compromised by Data Theft from Vendor* https://www.bankinfosecurity.com/wells-fargo-reveals-data-breach-a-944 accessed 18 February 2021

MRC 2014 https://mrc.ukri.org/publications/browse/human-tissue-and-biological-samples-for-use-in-research/

Medical Research Council 2014 *Human Tissue and Biological Samples for Use in Research: Operational and Ethical Guidelines* https://mrc.ukri.org/publications/browse/human-tissue-and-biological-samples-for-use-in-research/ accessed 24 June 2019

Njilo 2019 https://www.timeslive.co.za/news/south-africa/2019-10-16-stellenbosch-university-demands-return-of-dna-samples-but-uk-lab-hits-back/

Njilo N 2019 *Stellenbosch University Demands Return of DNA Samples - But UK Lab Hits Back* https://www.timeslive.co.za/news/south-africa/2019-10-16-stellenbosch-university-demands-return-of-dna-samples-but-uk-lab-hits-back/ accessed 18 February 2021

Outside Insight Date Unknown https://outsideinsight.com/insights/online-breadcrumbs-the-trail-individuals-leave-behind

Outside Insight Date Unknown *Online Breadcrumbs: The Trail Individuals Leave Behind* https://outsideinsight.com/insights/online-breadcrumbs-the-trail-individuals-leave-behind/ accessed 2 July 2021

Pash 2018 https://www.businessinsider.com.au/data-breach-private-health-details-medicare-2018-3
Pash C 2018 *A Data Bungle Put at Risk the Private Health Details of Millions of Australians* https://www.businessinsider.com.au/data-breach-private-health-details-medicare-2018-3 accessed 11 July 2019

Phillips 2018 https://www.lexology.com/library/detail.aspx?g=42443820-3143-4ed5-9b50-b251899fad18
Phillips F 2018 *GDPR Compliance Collides with US Law at Supreme Court* https://www.lexology.com/library/detail.aspx?g=42443820-3143-4ed5-9b50-b251899fad18 accessed 30 June 2019

Phillips and Charbonneau 2016 https://www.ftc.gov/system/files/documents/public_comments/2015/10/00057-98101.pdf
Phillips A and Charbonneau J 2016 *Giving Away More than Your Genomic Sequence? Privacy in the Direct-to-Consumer Genetic Testing Space.* https://www.ftc.gov/system/files/documents/public_comments/2015/10/00057-98101.pdf accessed 19 July 2019

SAMRC 2018 http://www.mrc.ac.za/media-release/genomics-centre-cape-town-decode-genes
South African Medical Research Council 2018 *Genomic Centre in Cape Town to Decode Genes* http://www.mrc.ac.za/media-release/genomics-centre-cape-town-decode-genes accessed 29 June 2019

Schwab 2016 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/
Schwab K 2016 *The Fourth Industrial Revolution: What It Means, How to Respond* https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ accessed 30 March 2019

Taylor Wessing Global Data Hub 2018 https://globaldatahub.taylorwessing.com/article/data-transfer-agreements
Taylor Wessing Global Data Hub 2018 *Data Transfer Agreements* https://globaldatahub.taylorwessing.com/article/data-transfer-agreements accessed 30 June 2019

Techterms 2014 https://techterms.com/definition/digital_footprint
Techterms 2014 *Digital Footprint* https://techterms.com/definition/digital_footprint accessed 2 July 2021

Wu 2015 https://www.newyorker.com/business/currency/facebook-should-pay-all-of-us
Wu T 2015 *Facebook Should Pay All of Us* https://www.newyorker.com/business/currency/facebook-should-pay-all-of-us accessed 9 March 2021

List of Abbreviations

4IR	Fourth Industrial Revolution
AESA	Alliance for Accelerating Excellence in Science in Africa
AI	artificial intelligence
AJHG	American Journal of Human Genetics
ASSAf	Academy of Science of South Africa
BGI	Beijing Genomics Institute
BHTY	Blockchain in Healthcare Today
CJEU	Court of Justice of the European Union
Colum L Rev	Columbia Law Review
COVID-19	coronavirus disease of 2019 - disease caused by the novel coronavirus SARS-CoV2
DNA	deoxyribonucleic acid
DTA	data transfer agreement
DTC	direct-to-consumer
EEA	European Economic Area
EU	European Union
GDPR	European Union General Data Protection Regulation
Harv J L & Tech	Harvard Journal of Law and Technology
HIV	human immunodeficiency virus
J Med Ethics	Journal of Medical Ethics
JAMIA	Journal of the American Medical Informatics Association
MRC	Medical Research Council (UK)
MTA	material transfer agreement
NHA	National Health Act 61 of 2003
NHS	National Health Service
Philos Trans A Math Phys Eng Sci	Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences
POPIA	Protection of Personal Information Act 4 of 2013

RNA	ribonucleic acid
SAMRC	South African Medical Research Council
UK	United Kingdom
US	United States of America
Yale J Biol Med	Yale Journal of Biology and Medicine