Penn State Journal of Law & International Affairs

Volume 10 | Issue 1

February 2022

IS POPIA BAD BUSINESS FOR SOUTH AFRICA? COMPARING THE GDPR TO POPIA AND ANALYZING POPIA'S IMPACT ON BUSINESSES IN SOUTH AFRICA

Brea Jones

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2021 VOLUME 10 NO. 1

IS POPIA BAD BUSINESS FOR SOUTH AFRICA? COMPARING THE GDPR TO POPIA AND ANALYZING POPIA'S IMPACT ON BUSINESSES IN SOUTH AFRICA

By Brea Jones[*]

[*] Brea Jones is Managing Editor of Communications of The Journal of Law and International Affairs and a 2022 Juris Doctor Candidate at The Pennsylvania State University, Penn State Law.

I. INTRODUCTION

South Africa, like the European Union, is expanding data privacy, but will business expansion follow? Over the past decade, countries across Africa have advanced technologically, these advancements demand data privacy regulations.[1] Without the proper protections in place, excessive data can be collected and sold for a profit at the expense of the people who unwittingly provide the data.[2] South Africa's Protection of Personal Information Act ("POPIA") was introduced to combat predatory data practices, and several parts of the Act were recently implemented.[3] POPIA imposes compliance requirements on businesses and organizations that collect data from South Africans.[4] Companies interested in conducting business in South Africa had until July 1, 2020, to comply with POPIA.[5]

The European Union's General Data Protection Regulation ("GDPR") shares some similarities with POPIA. The GDPR controls how businesses collect and use the data of European Union citizens.[6] Large international companies need not maintain a physical presence in Europe to be subjected to GDPR rules; any company that collects

---

[1] *See generally Connectivity in Africa is Mushrooming. And Lawyers are Seizing Their Moment*, LEGAL WEEK (Aug. 25, 2020); *Africa's Lack of Data Protection and Cybercrime Laws Has Created Deep Vulnerabilities. But Is Change On The Way?*, LEGAL WEEK (May 27, 2020).

[2] *See* Danielle Coleman, *Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws*, 24 MICH. J. RACE & L. 417 (2019).

[3] Nicole O., *South Africa's POPI Act*, PRIVACYPOLICIES (Jan. 5, 2021), https://www.privacypolicies.com/blog/popi-act/.

[4] *See* John Giles, *POPI and Consumer Rights*, MICHALSONS, (Nov. 21, 2013), https://www.michalsons.com/blog/popi-and-consumer-rights/12477.

[5] *See* PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT), https://popia.co.za/.

[6] *Are You Prepared for the GDPR?,* PRIVACYPOLICIES (April 23, 2020), https://www.privacypolicies.com/blog/prepare-gdpr.

data from European Union citizens must comply with the GDPR or risk sanctions, including large fines.[7]

In Part I, this article examines data connectivity and protection through analyzing global data connection and the rise of social media, data connection in Africa and South Africa, and the need for data protection. It explains and defines both South Africa's Protection of Personal Information Act and the European Union's General Data Protection Regulation The evolution of data connection and social media have resulted in an increased need for data privacy. Regulations like the POPIA and the GDPR enhance data privacy.

In Part II, this article compares POPIA with the GDPR and analyzes their costs of compliance. The GDPR and POPIA have much in common, but they are not the same. Understanding how the two protections differ can help businesses stay in compliance. Additionally, understanding where the two protections have similarities can save international businesses money and time by implementing measures that can meet the requirements of both protections.

In Part II, this article dissects the practical impact of POPIA on consumers and businesses. POPIA focuses on individual privacy protection, not the protection of business data; however, businesses can still benefit from compliance with POPIA. POPIA is a complex act with a lot of different requirements, many of which have practical implications.

In Part II, this article examines the potential impacts of POPIA on South Africa's business development and retention. Businesses must understand what POPIA requires so that businesses can make an informed decision on whether doing business in South Africa is worth the compliance steps. Because businesses consider several factors when determining viable locations for expansion, data privacy regulations can impact a business's expansion decision. Therefore,

---

[7] Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 368 (2019) (fines can be up 20,000,000 EUR or up to 4% of global annual turnover, whichever is higher.).

POPIA has the potential to either attract or deter businesses from operating in South Africa.

II. BACKGROUND: AN OVERVIEW OF DATA CONNECTIVITY AND PROTECTION

A. History of Data Connectivity

1. Data Connection Emerging Worldwide and The Rise of Social Media

The internet is fairly new, and the internet did not always function as it does today.[8] Today, people shop online, browse blog posts, use social media, and access internet-based apps on their cell phones.[9] But, before the creation of the World Wide Web in the 1990s,[10] the internet consisted of emails and file sharing.[11] The term "worldwide" can be deceiving; in actuality, in its early stages, the internet was inaccessible to most of the world.[12] As time progressed, the majority of the population in wealthier countries began to go

---

[8] Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina, *Internet*, OUR WORLD IN DATA (2015), https://ourworldindata.org/internet; Evan Andrews, *Who Invented the Internet?*, HISTORY (Oct. 28, 2019), https://www.history.com/news/who-invented-the-internet. ("ARPANET adopted TCP/IP on January 1, 1983, and from there researchers began to assemble the "network of networks" that became the modern Internet. The online world then took on a more recognizable form in 1990, when computer scientist Tim Berners-Lee invented the World Wide Web.").

[9] *The Evolution of Social Media: How Did It Begin, and Where Could It Go Next?*, MARYVILLE UNIVERSITY, https://online.maryville.edu/blog/evolution-social-media/#back-to-top (last visited Nov. 16, 2021) ("What began as a desktop or laptop experience shifted to mobile phones and tablets as cellular service expanded; the capabilities of cellular phones expanded, turning them into "smartphones"; and high-speed wireless internet became more readily available in homes, businesses, and public spaces.").

[10] MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Glossary/World_Wide_Web ("The World Wide Web—commonly referred to as WWW, W3, or the Web—is an interconnected system of public webpages accessible through the Internet. The Web is not the same as the Internet: the Web is one of many applications built on top of the Internet.").

[11] Roser et al., *supra* note 8.

[12] *See id.* ("[E]stimates for 1990 suggest that only half of a percent of the world population were online.").

online.[13] Although less-wealthy countries were not gaining access to the internet at the same rate as their wealthier counterparts, access to the internet around the world continued to increase each year.[14] Today, the internet allows users to communicate with people outside of their geographic location.[15] Because of the internet, the way that people conduct everyday activities has changed.[16] The internet enables the world to be more connected.

After the rise of the internet came the phenomenon that consumes the time of many people daily—social media.[17] Social media can be defined as "computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities."[18] Social media is such an integral part of today's society that it is difficult to believe it only became popular in the early 2000s.[19] Myspace, YouTube, and Facebook were some of the first social media platforms to captivate the minds of users.[20] Over time, social media use grew, and now billions of people use some form of social media.[21] Facebook and YouTube, two of the

---

[13] *See id.* ("[I]n 2016, three-quarters (76%) of people in the US were online . . . in Malaysia 79% used the internet; in Spain and Singapore 81%; in France 86%; in South Korea and Japan 93%; in Denmark and Norway 97%; and Iceland tops the ranking with 98% of the population online.").

[14] *See id.* ("But the overarching trend globally— and, as the chart shows, in all world regions— is clear: more and more people are online every year.").

[15] Zaryn Dentzel, *How the Internet Has Changed Everyday Life*, OPENMIND BBVA, https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/ ("Personal stories go public; local issues become global.").

[16] *Id.* ("The Internet has changed business, education, government, healthcare, and even the ways in which we interact with our loved ones—it has become one of the key drivers of social evolution.").

[17] *The Evolution of Social Media: How Did It Begin, and Where Could It Go Next?*, *supra* note 9.

[18] Maya E. Dollarhide, *Social Media Definition*, INVESTOPEDIA (Sep. 6, 2020), https://www.investopedia.com/terms/s/social-media.asp ("By design, social media is internet-based and gives users quick electronic communication of content. Content includes personal information, documents, videos, and photos.").

[19] *See* Roser et al., *supra* note 8.

[20] *See id.*

[21] *See generally id.*; Brian Dean, *Social Network Usage & Growth Statistics: How Many People Use Social Media in 2021?*, BACKLINKO (Feb. 01, 2021), https://backlinko.com/social-media-users ("3.96 billion people currently use social

original platforms, still lead the social media market today.[22] On average, over two billion users access Facebook monthly.[23] YouTube is the second-largest social media platform after Facebook and has almost two billion users.[24] Social media's broad reach makes it a great place for companies to market to potential consumers.[25] People are no longer just using social media—social media is using people.[26] Social media platforms often profit from advertising to potential consumers based on the data the platforms collect from the users.[27] Social media companies collect personal information to market products.[28] The average social media user scrolling through posts online may not think about the advertisements presented to them, but those advertisements are often a product of the information gathered about the user.[29]

One infamous example of a company marketing to people based on data collection is Cambridge Analytica. Cambridge Analytica used information collected about Facebook users to influence biases

---

media worldwide, up almost double from 2.07 billion in 2015 . . . . The average person has 8.6 social media accounts in 2020, up from 4.8 in 2014").

[22] *See* Roser et al., *supra* note 8.

[23] Alfred Lua, *21 Top Social Media Sites to Consider for Your Brand*, BUFFER, https://buffer.com/library/social-media-sites/#1-facebook-2-23-billion-maus ("Facebook is the biggest social media site around, with more than two billion people using it every month. That's almost a third of the world's population! There are more than 65 million businesses using Facebook Pages and more than six million advertisers actively promoting their business on Facebook.").

[24] *Id.* ("Besides being the second biggest social media site, YouTube (owned by Google) is also often known as the second largest search engine after Google.").

[25] Brady Dukart, *20 Important Benefits of Social Media Marketing Every Business Should Know*, COSCHEDULE BLOG, https://coschedule.com/blog/benefits-of-social-media-marketing-for-business/ ("While it may seem overwhelming, its importance cannot be overstated. It's so important that 97% of marketers are using social media and 78% of salespeople outsell their peers by using social media for their business.").

[26] *See* Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/.

[27] *Id.* ("Their core products, including Instagram, Messenger, Gmail, and Google Maps, don't cost money. You pay with your personal data, which is used to target you with ads.").

[28] *See generally id.*

[29] *Id.*

and preferences.[30] Some argue that Cambridge Analytica's influences played a role in Brexit and the 2016 U.S. Presidential Election.[31] Since social media data collection can have such a strong impact, data collection regulations are important. Policies that require social media users to consent before their data is collected can aid in data protection and help businesses detect which users want to receive marketing from their brand.[32] When businesses understand which users want to receive their marketing, they can customize their advertisements which "lead[s] to a higher conversion rate, social sharing, click-through, and increase marketing ROI [Return on Investment] as efforts and budgets are spent wisely."[33]

2. Data Connection in Africa

In the early stages of data connectivity, data connection in Africa was low, but in recent years, Africa has taken steps to increase data connection.[34] In the age of technology, internet access is vital for interacting and competing with other populations across the globe.[35] The world has become so technologically advanced that the internet is

---

[30] *See generally* Sam Meredith, *Here's everything you need to know about the Cambridge Analytica scandal*, CNBC: TECH (Mar. 21, 2018, 6:16 AM), https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

[31] *See id.*

[32] *See Data Protection & Social Media: How GDPR Influences Today's Social Media Platforms*, RSI SECURITY (Jan. 21, 2020), https://blog.rsisecurity.com/data-protection-and-social-media/.

[33] *Id.* ("[B]usinesses can experiment with niche marketing by creating tailored messages geared towards specific habits and needs of a clearly defined audience that has more interest in your products.").

[34] *See Connectivity in Africa is Mushrooming. And Lawyers are Seizing Their Moment*, *supra* note 1. ("In the past 10 years, Africa has experienced a huge investment in data connectivity infrastructure"); *See also* Joel Macharia, *Internet access is no longer a luxury*, AFRICA RENEWAL: INFRASTRUCTURE (Apr. 2014), https://www.un.org/africarenewal/magazine/april-2014/internet-access-no-longer-luxury ("The number of internet users on the continent grew at seven times the global average, clocking more than 3,600% growth between 2000 and 2012").

[35] *Connecting for Inclusion: Broadband Access for All*, THE WORLD BANK, https://www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all.

a necessity.[36] Unfortunately, data connection expansion is expensive[37] and the cost to expand quality internet can be high for countries and their citizens. The expense that consumers in Africa must pay contributes to the slow growth of access.[38] Even with the steps that Africa is taking to provide internet access, availability of quality internet speed is still low.[39] Notwithstanding the obstacles to expansion, as Africa increases connectivity and internet speed, Africa's economy will grow.[40] Companies are aware of the possible economic

---

[36] *Id.* ("Broadband (or high-speed) internet access is not a luxury, but a basic necessity for economic and human development in both developed and developing countries.").

[37] *See generally Achieving Broadband Access for All in Africa Comes With a $100 Billion Price Tag*, THE WORLD BANK: NEWS (Oct. 17, 2019), https://www.worldbank.org/en/news/press-release/2019/10/17/achieving-broadband-access-for-all-in-africa-comes-with-a-100-billion-price-tag ("Across Africa, where less than a third of the population has access to broadband connectivity, achieving universal, affordable, and good quality internet access by 2030 will require an investment of US $100 billion").

[38] Maxwell Karibian, *Achieving Universal Internet Access in Africa by 2030*, THE BORGEN PROJECT (July 23, 2020), https://borgenproject.org/internet-access-in-africa-2/ ("Affordability is the biggest issue concerning internet access in Africa. Internet access in many African countries is expensive compared to countries outside of the continent. Africa as a whole has the least affordable internet prices on the planet."); *Connectivity in Africa is Mushrooming. And Lawyers are Seizing Their Moment*, *supra* note 1 ("Internet connectivity on the continent is costly in relation to purchasing power, although it is becoming more affordable, and pay-as-you-go mobile services are the norm for the bulk of the population.").

[39] *See* Karibian, *supra* note 38 ("According to InternetWorldStats, roughly 39% of Africa's entire population had access to the internet as of December 2019. As of 2019, '17.8% of households in Africa had internet access at home', and '10.7% of households in Africa had a computer.' These percentages might seem low considering that computer technology is more prevalent than ever before. In Africa, however, high-quality internet access is a luxury many people cannot afford.").

[40] *Id.* ("Experts also have stressed the critical role high bandwidth internet access in Africa will have for boosting Africa's economy in the future."); *Connectivity in Africa is Mushrooming. And Lawyers are Seizing Their Moment*, *supra* note 1 ("Africa is widely recognized as "the next investment opportunity," because the European market is saturated and the youthful population on the continent represents a vast potential consumer market, said Janet MacKenzie, partner at Baker McKenzie in Johannesburg.").

opportunity available in Africa, and data protection laws may play a role in companies' decisions on expanding into Africa.[41]

3. Data Connection in South Africa

South Africa is growing in data connectivity and data regulation.[42] Universities were the first to have access to the internet in South Africa.[43] In the early 2000s, South Africa gained access to broadband wireless internet.[44] South Africa's fiber-optic cable connection grew around 2016, increasing internet quality and plans are in place to continue fiber-optic cable growth to make internet connection more reliable.[45] Currently, over half of the population in South Africa is using the internet.[46]

Internet use necessitates data privacy protection.[47] South Africans have a constitutional right to privacy "which includes the right not to have a. their person or home searched; b. their property searched; c. their possessions seized; or d. the privacy of their communications infringed," but South Africa has taken the next step by enacting the POPIA to ensure that companies have protection

---

[41] *See generally* Kendal H. Tyre Jr. , Nia Newton and Diana Vilmenay, *Franchising in Africa: Growth in the Industry and Data Privacy and Protection Issues*, 16 INT'L J. FRANCHISING L. 7 (2018).

[42] Toby Shapshak, *South Africa Has 21 Million Internet Users, Mostly On Mobile*, FORBES (July 19, 2017, 2:54 PM), https://www.forbes.com/sites/tobyshapshak/2017/07/19/south-africa-has-21m-internet-users-mostly-on-mobile/?sh=a8409f21b2d5; *POPIA – South Africa's Protection of Personal Information Act*, COOKIEBOT (Sept. 29, 2020), https://www.cookiebot.com/en/popia/.

[43] *The Internet and South Africa*, TOP 500: NEWS, https://top500.co.za/news/the-internet-and-south-africa/.

[44] *Id.*

[45] *Id.*

[46] Roser et al., *supra* note 8.

[47] *What Is Data Privacy and Why Is it Important?*, LIFELOCK (Jan. 18, 2021), https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html#:~:text=Data%20privacy%20has%20always%20been%20important.&text=A%20single%20company%20may%20possess,the%20company's%20reputation%20remains%20untarnished.

measures in place.[48] South Africa is one of the first countries in Africa to enact such a substantial data privacy regulation.[49] In fact, "South Africa's data protection legislation comes into force just as many other African countries are starting their own path towards the protection of personal information."[50]

4. The Need for Data Protection

Information sharing has become an inevitable part of using the internet.[51] When consumers go online and browse the internet, their searches may be recorded, their search history accumulated, and their patterns analyzed; when they click on websites, they are prompted to accept cookies that track their visits and activity.[52] When consumers use apps they may share their location; when they use social media, information is often gathered about the consumer to better market the consumer products.[53] Everyday consumers scroll through privacy

---

[48] CONST. OF THE REPUBLIC OF SOUTH AFRICA ch. 2 (1996), https://www.gov.za/documents/constitution/chapter-2-bill-rights#14; PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT), *supra* note 5.

[49] Paul Esselaar, *The Wild West is Dead; Long Live Data Protection*, TRALAC: BLOG (July 2, 2020), https://www.tralac.org/blog/article/14725-the-wild-west-is-dead-long-live-data-protection.html.
("South Africa's data protection legislation comes into force just as many other African countries are starting their own path towards the protection of personal information.").

[50] *Id.*

[51] Matsakis, *supra* note 26 ("The questions they ask Google uncover humanity's deepest prejudices. And their location histories tell investors which stores attract the most shoppers. Even seemingly benign activities, like staying in and watching a movie, generate mountains of information, treasure to be scooped up later by businesses of all kinds.").

[52] *Id; see generally What are cookies?*, NORTON: PRIVACY (Aug. 12, 2019), https://us.norton.com/internetsecurity-privacy-what-are-cookies.html.

[53] *Should you share your location on social media?*, EQUIFAX, https://www.equifax.co.uk/resources/identity-protection/should-you-share-your-location-on-social-media.html#:~:text=If%20you%20have%20children%2C%20they,re%20not%20at%20your%20home. (last visited Nov. 16, 2021)
("Apps like Facebook and Instagram allow you to tag your photos with the place they were taken in, and Facebook allows you to tag your statuses with your location. Meanwhile, Snapchat allows you to share your current location as you stream live, alerting your followers."); *see also* Megan Malone, *How Does Facebook Know What Ads*

agreements and click "accept," unaware of the data they are sharing.[54] With the volume of data shared every day, data privacy regulations are necessary to protect consumer information.

Companies use online platforms to market and sell their products to consumers.[55] Electronic commerce, or e-commerce, is a large and growing business.[56] Competing in today's market is hard without an online presence.[57] The need for an online presence was showcased more than ever during the 2019 Coronavirus Disease (COVID-19) outbreak. Businesses closed their brick-and-mortar locations in many cities across the world to slow the spread of the virus.[58] Companies with a strong online presence inevitably had a competitive advantage over their solely brick and mortar counterparts.[59] Even before COVID-19, having an online presence helped companies reach a broader market.[60]

---

to Show You? (Example), VICI: BLOG, https://www.vicimediainc.com/how-does-facebook-know-what-ads-to-show-you/ (last modified Feb. 4, 2019) ("The way Facebook determines what ads to show you is based a lot around the information you provide by your online activity.").

[54] Kim Hart, *Privacy policies are read by an aging few*, AXIOS: TECHNOLOGY (Feb. 28, 2019), https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html ("[M]ost people skip right to the "I agree" box on a privacy policy without actually reading it . . . .").

[55] *What is Social Media Marketing?*, BUFFER, https://buffer.com/social-media-marketing (last visited Nov. 16, 2021).

[56] *See generally Ecommerce*, BIG COMMERCE: ARTICLES, https://www.bigcommerce.com/articles/ecommerce/#ecommerce-timeline (last visited Nov. 16, 2021).

[57] *See generally Why Does Your Business Need an Online Presence?*, CHRYSALIS COMMUNICATIONS: BLOG, https://thinkchrysalis.com/blog/why-does-your-business-need-an-online-presence/ (last visited Nov. 16, 2021).

[58] *See generally* Walter Loeb, *Retailers Are Choosing To Close To Slow The Spread Of Coronavirus*, FORBES (Mar. 16, 2020, 7:10 AM), https://www.forbes.com/sites/walterloeb/2020/03/16/retailers-are-choosing-to-close-to-slow-coronavirus/?sh=34a8a6101904.

[59] Jes Gonzalez, *5 Reasons Why Having an Online Presence Is Essential for Your Small Business*, ALL BUSINESS, https://www.allbusiness.com/5-reasons-online-presence-essential-small-businesses-106737-1.html (last visited Nov. 16, 2021).

[60] *See generally Advantages and Disadvantages of Creating an Online Presence for Your Business*, SMALL BUSINESS RAINMAKER: BLOG (Jan. 9, 2021), https://www.smallbusinessrainmaker.com/small-business-marketing-

Consumers also benefit from e-commerce,[61] with many products and services only a click away. But those clicks carry risks. When consumers shop online they share a considerable amount of data.[62] When ordering a product, consumers may share their email, name, address, and credit card information. If a website is hacked, the consumer's information can be stolen and used without their consent.[63] Regulations that require companies to notify customers when their information may have been breached are critical.

Seeing the potential to capitalize on consumer information, companies known as "data brokers" were formed solely to collect and sell consumer data.[64] Data brokers search multiple sources and collect publicly held information on a range of topics, including "browsing history, social media connections, and online purchases."[65] Other companies then purchase the information data brokers collect and use it to better market to consumers.[66] Often, consumers do not know that their information is being collected.[67] These predatory practices

---

blog/advantages-and-disadvantages-of-creating-an-online-presence-for-your-business.

[61] *See generally Benefits of E-commerce to customer*, CLOUD TALK: BLOG (Jan. 22, 2019), https://www.cloudtalk.io/blog/benefits-of-e-commerce-to-customer#:~:text=Customers%20can%20buy%20any%20product,from%20their%20workplace%20or%20home.&text=E%2Dcommerce%20is%20convenient%20when,and%20the%20merchandise%20is%20yours.

[62] *What Data Are You (Unwittingly) Sharing When You Shop Online? – Decrypted Series #2*, FORTKNOXSTER (Sept. 10, 2019), https://fortknoxster.com/blog/what-data-are-you-unwittingly-sharing-when-you-shop-online-decrypted-series-2/.

[63] *See generally* Mike Wood, *With an Increase in Online Shopping, Prepare for an Increase in Data Breaches*, ALL BUSINESS, https://www.allbusiness.com/increase-online-shopping-prepare-increase-data-breaches-115448-1.html (last visited Nov. 16, 2021).

[64] *What Are Data Brokers – And What Is Your Data Worth?*, WEBFX (Mar. 16, 2020), https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/
("data brokering is a multi-billion dollar industry made up of companies who collect consumer data and sell it to other companies, usually for marketing purposes.").

[65] Matsakis, *supra* note 26.

[66] *See id.*

[67] Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS (Mar. 9, 2014), https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ ("I think most people have no idea that it's being collected

illustrate the need for regulation of the data brokering industry to protect unwitting consumers from having their information stored and sold.

What would meaningful data privacy regulations do to protect the consumer? They would ensure that companies have a plan in place for if and when consumer data is breached.[68] Effective regulations would control what information could be collected, for what reasons, and how much of that data could be stored.[69] Additionally, meaningful regulations would mandate training on data protection for companies that collect consumer data.[70] Countries across the world are implementing strong data privacy regulations that could change the way data is collected and shared.[71]

5. South Africa's Protection of Personal Information Act

The Protection of Personal Information Act (POPIA) is a data privacy regulation enacted by the South African parliament to protect consumer data from wrongful use.[72] South Africa has been implementing POPIA for several years.[73] Certain sections of POPIA were initiated in 2014, but the remainder of the act, excluding sections 110 and 114(4), was not commenced until July of 2020.[74] POPIA has

---

and sold and that it is personally identifiable about them, and that the information is in basically a profile of them.").

[68] Jingcong Zhao, *Understanding Data Privacy and Why It Needs to Be a Priority for Your Business*, HYPER PROOF (Feb. 5, 2020), https://hyperproof.io/resource/understanding-data-privacy/#:~:text=Data%20collection%20regulations%20provide%20guidance,their%20data%20is%20being%20collected.

[69] *See id.*

[70] *See id.*

[71] *What's Data Privacy Law In Your Country?*, PRIVACYPOLICIES (Spet.4, 2019), https://www.privacypolicies.com/blog/privacy-law-by-country/ ("A relatively recent legal development, privacy laws have now been enacted in over 80 countries around the world.").

[72] PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT), *supra* note 5.

[73] *Id.*

[74] PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT), *supra* note 5 ("The commencement date of section 1, Part A of Chapter 5, section 112 and

several guidelines that businesses must abide by when operating in South Africa, which can be broken down into the following eight categories, called "conditions": (1) Accountability ("C1"), (2) Processing Limitation ("C2"), (3) Purpose Specification ("C3"), (4) Further Processing Limitation ("C4"), (5) Information Quality ("C5"), (6) Openness ("C6"), (7) Security Safeguards ("C7"), and (8) Data Subject Participation("C8").[75] [76] POPIA will impact how businesses structure their data privacy measures and may impact business expansion into South Africa. Because businesses see data protection compliance as an additional cost, compliance must be profitable. Therefore, similar to other regulations, POPIA implements fines for non-compliant businesses.[77] Before companies can properly comply with POPIA, they must first understand POPIA's requirements.

POPIA's first category (C1), Accountability, requires that data processors comply with the other categories of POPIA and assign a responsible party to ensure compliance throughout the organization.[78] C2, Processing Limitation, restricts how data can be processed.[79] The Processing Limitation category has several sub-requirements. Data processors must: [(a)]Process data in a way that doesn't risk the data subject's privacy; [(b)] [p]rocess only relevant data with a given purpose; [(c)] [o]btain consent from the data subject before processing (and keep proof of consent); [(d)] [p]rotect the legitimate interest of the data subject; [(e)] [a]llow data subjects to object to processing and/or withdraw consent at any time; and [(f)] [s]top processing data after an objection or withdrawal of consent.[80]

---

section 113 is 11 April 2014. The commencement date of the other sections is 1 July 2020 (with the exception of section 110 and 114(4).").

75 Nicole O., *supra* note 3.

76 *See generally* PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT), *supra* note 5.

77 *See* Nicole O., *supra* note 3.

78 *Id.* ("It stipulates that the responsible party has the responsibility of ensuring the rest of the conditions are in place before processing data. The responsible party must also ensure compliance both when deciding to process data and during the processing of the data.").

79 *Id.* ("The second condition - Processing Limitation - places strict controls on what it means to lawfully process data.").

80 *Id.*

C2 also requires that data be collected from the data subject and not a third party unless "the data is public record or is deliberately made public or if you have the consent to do so or if doing so does not violate the legitimate interest of the data subject."[81] C3, Purpose Specification, specifies how long data processors can keep data and what reasons they can use to collect data.[82] Data subjects must be aware of why data processors are collecting their data.[83] C4, Further Processing Limitation, expands on categories two and three. The Further Processing Limitations ensure that data processors only further process data that aligns with their purpose.[84] C5, Information Quality, requires that the data collected be accurate.[85] C6, Openness, essentially requires that data processors document the data they collect and promulgate a privacy policy to inform data subjects of the data processor's practices.[86] C7, Security Safeguards, requires that data processors enact measures to protect against hacking.[87] C7 also requires that in the case of a breach, the data processor take specified steps to notify data subjects.[88] C8, the final category, Data Subject Participation, has several important sections. C8 gives data subjects the right to access their data and request changes to the data.[89] It also prohibits the collection of certain personal information and criminal

---

[81] *Id.*

[82] *Id.* ("The idea that you must collect information only for a 'specific, explicitly defined and lawful purpose' related to one of your normal activities is at the heart of the law.").

[83] *Id.*

[84] *Id.* ("Conditions 2 and 3 aren't the only processing limitations. Condition 4—Further Processing Limitation— continues to elaborate on how you can and can't process data. The main point noted here says that you must only process data in ways compatible with the purpose you stated.").

[85] *Id.* ("Condition 5 says that you must take steps to ensure the data you collect and subsequently process is accurate and complete.").

[86] *Id.*

[87] *Id.* ("To meet these obligations, you must perform a risk assessment test, ensure the maintenance of safeguards, verify the effectiveness of the safeguards, and ensure new updates are provided to prevent new deficiencies or risks.").

[88] *Id.* ("Condition 7 also provides a long list of requirements if a responsible party believes its security is compromised.").

[89] *Id.* ("[T]hey have access to their personal information, including learning what information the responsible party has the option to ask for a description or record. The data subject also has the right to request corrections . . . ").

behavior unless an exception applies.[90] Additionally, C8 prohibits the collection of children's data unless an exception applies.[91]

6. General Data Protection Regulation

The General Data Protection Regulation is a data privacy regulation established/enacted/instituted by the European Union to protect the private information of citizens.[92] Any business collecting data from a European Union citizen or engaging in a financial transaction with a European Union citizen must comply or face penalties.[93] Arguments have been made that the GDPR could set the standard for data privacy across the globe.[94] The GDPR was adopted in 2016 and was put into effect on May 25, 2018.[95] For a simple breakdown of the GDPR, this article will focus on the main GDPR requirements. The GDPR has seven major requirement categories ("RC"): (1) Obtaining Consent ("RC1"); (2) Timely Breach Notification ("RC2"); (3) Right To Data Access ("RC3"); (4) Right To Be Forgotten ("RC4"); (5) Data Portability ("RC5"); (6) Privacy By Design ("RC6"); and (7) Potential Data Protection Officers ("RC7").[96]

---

[90] *Id.* ("Condition 8 also has several parts. Part B refers to the prohibition of processing of special personal information (including religious beliefs, health information, biometric information, etc.) or criminal behavior.").

[91] *Id.*

[92] *See id.*

[93] *See id.*

[94] *See generally* Rustad & Koenig, *supra* note 7 ("Many difficulties remain to be overcome, but the GDPR is rapidly evolving into the transnational gold standard of data protection, applicable to all domestic and cross-border transfers of personally identifiable data.").

[95] *See The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Nov. 16, 2021) ("In 2016, the EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years . . . The GDPR is now recognized as law across the EU. Member States have two years to ensure that it is fully implementable in their countries by May 2018.").

[96] Sam Saltis, *GDPR Explained In 5 Minutes: Everything You Need to Know*, CORE DNA (Nov. 5, 2020), https://www.coredna.com/blogs/general-data-protection-regulation.

RC1, Obtaining Consent, requires that terms and conditions are understandable, and that consent is easily given and revoked.[97] RC2, Timely Breach Notification, requires that companies report breaches within seventy-two hours.[98] RC3, Right To Access Data, states that customers may request their data, and companies are required to provide the data with information on how they are using the data.[99] RC4, Right To Be Forgotten, gives customers the right to have their data deleted.[100] RC5, Data Portability, allows customers to take their data and use the data somewhere else.[101] RC6, Privacy By Design, requires the company data systems to be designed in a certain secure manner.[102] What Privacy By Design fully entails is still unclear.[103] RC7, the final category, Potential Data Protection Officers, states that

---

[97] *Id.* ("Your terms of consent must be clear. This means that you can't stuff your terms and conditions with complex language designed to confuse your users. Consent must be easily given and freely withdrawn at any time.").

[98] *Id.* ("If a security breach occurs, you have 72 hours to report the data breach to both your customers and any data controllers, if your company is large enough to require a GDPR data controller. Failure to report breaches within this timeframe will lead to fines.").

[99] *Id.* ("If your users request their existing data profile, you must be able to serve them with a fully detailed and free electronic copy of the data you've collected about them. This report must also include the various ways you're using their information.").

[100] *Id.* ("Also known as the right to data deletion, once the original purpose or use of the customer data has been realized, your customers have the right to request that you totally erase their personal data.").

[101] *Id.* ("This gives users rights to their own data. They must be able to obtain their data from you and reuse that same data in different environments outside of your company.").

[102] *Id.* ("This section of GDPR requires companies to design their systems with the proper security protocols in place from the start. Failure to design your systems of data collection the right way will result in a fine.").

[103] *GDPR Privacy by Design*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/privacy-by-design/ (last visited Nov. 30, 2021) ("Nevertheless, there is still uncertainty about what 'Privacy by Design' means, and how one can implement it. This is due, on the one hand, to incomplete implementation of the Directive in some Member States and, on the other hand, that the principle "Privacy by Design" which is in the General Data Protection Regulation, that the current approach in the data protection guidelines, which requires persons responsible already to include definitions of the means for processing TOMs at the time that they are defined in order to fulfil the basics and requirements of 'Privacy by Design').

depending on the company size and the level of data connection, companies may have to appoint a Data Protection Officer.[104]

III. ANALYSIS: THE GDPR AND THE POPIA IN ACTION

A. Comparing The GDPR and The POPIA

The GDPR and the POPIA are very similar. In fact, the POPIA has been referred to as an unofficial "stepping stone to GDPR compliance."[105] Although the regulations are very similar overall, the differences are worth noting to ensure compliance.

The application of the regulations differs. Unlike the POPIA, the GDPR covers all members of the European Union and is not limited by jurisdiction.[106] The POPIA covers personal information processed in South Africa.[107] However, the GDPR only covers natural people, whereas the POPIA covers natural people and legal entities.[108] So, although the GDPR is not limited in jurisdictional reach, the GDPR is limited in who is entitled to protection (natural people only).

The organizational roles outlined in the regulations are similar, but the GDPR includes a larger variety of roles. Under the POPIA, organizations handling data may take on the role of either controller or processor, whereas the GDPR includes additional roles such as joint reasonable parties, third parties, and recipients.[109].

---

104 Saltis, *supra* note 96 ("In some cases, your company may need to appoint a data protection officer (DPO). Whether or not you need an officer depends upon the size of your company and at what level you currently process and collect data.).

105 *See* Russell Nel, *GDPR matchup: South Africa's Protection of Personal Information Act*, INT'L ASS'N OF PRIVACY PROF'LS (Sep. 5, 2017), https://iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/; *PoPI vs. GDPR*, MEDIUM (Aug. 6, 2018), https://medium.com/black-ink-advisory/popi-vs-gdpr-956093118061.

106 *See* Nel, *supra* note 105; Cynthia Yav, *Perspectives on the GDPR from South Africa*, 2 INT'L J. DATA PROTECTION OFFICER, PRIVACY OFFICER & PRIVACY COUNS. 19 (2018).

107 Nel, *supra* note 105.

108 Yav, *supra* note 106.

109 *Id.*

Both regulations incorporate Data Protection Officers, but the requirements for when a company must have a Data Protection Officer differ slightly. Not all companies regulated by the GDPR require a Data Protection Officer.[110] Depending on the size of a company and the scale of the company's processing, the company may need to have a Data Protection Officer under the GDPR.[111] However, the POPIA requires Data Protection Officers for all organizations.[112] That means that a company operating under POPIA must appoint a Data Protection Officer or the head of the organization will be deemed the company's Data Protection Officer.[113]

Data breach notification is required under both regulations, but time specifications differ slightly. The GDPR's notification requirements are very strict. Under the GDPR, if a breach occurs, the organization must report the breach within seventy-two hours of discovery.[114] The POPIA is not as clear on when a report must be done. The POPIA only requires notification "as soon as reasonably possible."[115] Although the GDPR may be viewed as having a strict notification requirement, the GDPR sets out a clear standard for organizations to follow to stay in compliance. Sometimes lenity can lead to ambiguity.

While both the GDPR and POPIA impose penalties for noncompliance, the GDPR imposes a much higher fine than the POPIA.[116] The GDPR imposes a fine of twenty million euros or a percentage of global revenue, whichever is higher, whereas the POPIA imposes a fine of ten million South African Rand.[117] Although the financial burden may be lower under the POPIA, the POPIA also

---

110 *See PoPI vs. GDPR*, *supra* note 105.

111 *Id.*

112 *Id.*

113 *Id.* ("PoPI states that should a company not have a Data Protection Officer, this role falls to the head of the organization (typically the CEO or executive officer). Should the role be delegated to another member of the organisation [sic] it must be done formally and in writing.").

114 Yav, *supra* note 106, at 20.

115 *PoPI vs. GDPR*, *supra* note 105.

116 *Id.*

117 *Id.*

allows for criminal sanctions.[118] Therefore, the GDPR arguably has a potential for a higher fine and the POPIA has a potential for a higher penalty.

Privacy by design and impact assessment requirements differ between the two regulations. The GDPR requires that privacy be built "into the design, operation, and management of a given system, business process, or design specification."[119] The POPIA does not require privacy by design.[120] Furthermore, "[a]n additional mandate by the GDPR is the obligation for conducting data protection impact assessments and maintaining records of such assessments, this is an aspect which POPIA does not specify."[121] However, the POPIA's security safeguard requirement could be read to include impact assessments.[122] Therefore, privacy by design and impact assessments are requirements only specified by the GDPR.

Only the GDPR incorporates data portability, specifying that data subjects be able to request to have their data transferred from one controller to another.[123] The POPIA does not specify data portability.[124] In this aspect, the GDPR adds an additional protection/service for data subjects.

Overall, the GDPR and the POPIA are similar in many ways; however, the GDPR reaches more countries than POPIA, sets out a clear seventy-two hour notification requirement, implements higher monetary fines, requires privacy by design and impact assessments, and allows for data portability. Whereas the POPIA protects not only natural people but also legal entities, requires data protection officers for all companies, and imposes criminal sanctions. If an organization is already in compliance with the POPIA, it would only have to implement privacy by design, impact assessments, and data portability standards to comply with the GDPR. If an organization is already in

---

118 *See Id.*; Yav, *supra* note 106, at 20.
119 Yav, *supra* note 106, at 20.
120 *Id.*
121 *Id.*
122 *PoPI vs. GDPR*, *supra* note 105.
123 Yav, *supra* note 106, at 20.
124 *Id.*

compliance with the GDPR, it will likely not have to take any major additional steps to comply with the POPIA.

B. What is The GDPR Costing Businesses In The EU?

Data regulation compliance comes at a cost.[125] Since the GDPR and the POPIA have many similarities, examining the costs associated with GDPR compliance helps illuminate the costs associated with POPIA compliance. Compliance with the GDPR has proven to be expensive for many companies.[126] Companies located outside of the European Union are experiencing higher compliance costs because many EU companies already have measures in place that comply with the GDPR.[127] The International Association of Privacy Professionals estimates that compliance will cost U.S. Fortune 500 companies 7.8 billion dollars and will cost U.K. FTSE 350 companies 1.1 billion dollars.[128]

To ensure their compliance with GDPR regulations, businesses are facing increased legal costs. [129] While companies want to ensure they are following the necessary steps, the regulation's complexity virtually requires interpretation from legal counsel to

---

125 *Non-Compliance 2x The Cost Of Compliance. Can You Afford The Risk?*, GLOBAL SCAPE, https://www.globalscape.com/resources/infographics/data-compliance-costs (last visited Nov. 16, 2021).

126 Oliver Smith, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown*, FORBES (May 2, 2018, 2:30 AM), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=3848e37534a2 ("Fortune 500 and FTSE 350 businesses have been forced to spend billions of dollars in a frenzy ahead of the 25 May deadline for the EU's new data law, Forbes has discovered.").

127 *Id.* ("This huge difference in cost compared to their European peers is because many of the requirements of GDPR already exist in EU law and companies have advanced systems in place to deal with them.").

128 *Id.* ("Big British firms have now sunk a combined $1.1 billion preparing for GDPR, according to estimates compiled by the International Association of Privacy Professionals (IAPP) and EY. For American companies, the combined figure has reached a whopping $7.8 billion.").

129 *Id.* ("But, as we've seen time and time before, the new rules have been left deliberately vague, forcing corporates and startups alike to invest in (expensive) legal experts to interpret what GDPR means for them.").

understand it. For example, many businesses struggle to determine what satisfies the RC1 consent requirement of the GDPR.[130] Although the cost for legal counsel is high, the possible fine for non-compliance is much higher; thus, companies are justifying the additional costs of legal services for regulatory interpretation to prevent larger costs associated with non-compliance later.

Additional costs include updating technology to process information correctly, hiring a Data Protection Officer, training employees on compliance measures, and monitoring compliance.[131] If a company wants to avoid complying with the GDPR, "[t]here are two ways. . . stop doing business in Europe entirely, or dump the personal data you're holding—and both are proving popular."[132] Some businesses with a small presence in the European Union may decide to stop doing business with EU citizens altogether rather than take on costly compliance measures or risk the cost of noncompliance.[133] Other businesses may try to delete the data they have on EU citizens in order to avoid the GDPR altogether.[134]

C. The POPIA's Impact on Consumers

The POPIA, like the GDPR, was created to protect data subjects and their personal information.[135] Although the POPIA may not have as many strict requirements as the GDPR, the POPIA still confers substantial benefits to the consumer. Both businesses and

---

130 *Id.* ("But there's confusion among businesses around what exactly constitutes 'consent' under the new rules and whether consent given in the past is still valid—and their concern is quite valid given the maximum fine for non-compliance with GDPR is 4% of annual turnover or €20 million ($24.6 million).").

131 *See id.*; Jonas De Oliveira, *How Much does GDPR Compliance Cost?*, SECURITY METRICS, https://www.securitymetrics.com/blog/how-much-does-gdpr-compliance-cost (last visited Nov. 12, 2021).

132 Smith, *supra* note 126.

133 *Id.* ("Meanwhile, Dayanim says some of Paul Hastings' U.S. clients only have small European operations and are having "to think very hard about whether they really want to do business with EU data subjects.").

134 *Id.* ("British pub giant Wetherspoons recently came to a smart conclusion, rather than checking consent for all the email addresses it's collected over the years, it took a sledgehammer to the problem and deleted its vast email database.").

135 PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT), *supra* note 5.

consumers should be aware of the consumer impacts of the POPIA. The impacts may change the way consumers value their personal data and the way businesses value consumers.

Consumers can protect their information and can choose the companies with which they share their information.[136] This consumer impact stems from the requirement that consumers consent to sharing their personal information. The power of consumers to decide who may access their personal information is extremely important and often overlooked. As emphasized in "The Need for Data Protection" section above, consumers share a lot of information every day, and that information is very valuable to the companies that collect it. Now, under the POPIA, consumers may choose which companies have the privilege of storing their personal information.

Consumers can choose which business communications they want to receive. For instance, "[c]onsumers can opt-out of communication from businesses by unsubscribing from unwanted communications, such as email or SMS marketing."[137] The ability to opt-out at any time helps ensure that consumers are offering ongoing consent. Businesses may be more cognizant of the marketing they create and how often they share the marketing materials in an effort to keep subscribing consumers satisfied and not overwhelmed.

Consumers can ask what personal information of theirs a business possesses and then request that the business delete the information.[138] This requirement showcases ongoing consent at its finest. Having personal information deleted seems like the logical step after impacts one and two. For instance, Consumer A is browsing for clothing online and stumbles across a new boutique. After glancing over the company's privacy policy, Consumer A consents to sharing personal information with the company. Consumer A is bombarded with email and text promotions for the boutique and decides to opt-

---

136 *POPI Act to fuel better customer experiences for South Africans*, MEDIA UPDATE (Apr. 15, 2020), https://www.mediaupdate.co.za/marketing/148390/popi-act-to-fuel-better-customer-experiences-for-south-africans.

137 *Id.*

138 *Id.*

out. But what about all the personal information the company already collected? Consumer A has a right to know what personal information the company has, and have the information deleted.

Consumers can complain to the business or the Information Regulator if the consumer feels that their privacy is not being respected.[139] Businesses must comply with the POPIA and recognize the rights that the POPIA confers to consumers. If companies are not in compliance, they may face penalties. The Information Regulator is appointed to enforce the POPIA.[140] With these measures in place, consumers can report companies if the companies violate the consumer's rights.

D. The POPIA's Impact on Businesses

POPIA will undoubtedly impact how businesses operate in South Africa.[141] If a company has little to no data protection measures in place, adjustment to the POPIA may prove burdensome. The main burden associated with complying with the POPIA is cost. Appointing a Data Protection Officer, training employees, and ensuring the quality of data are just a few of the compliance requirements outlined above[142] which can prove costly.[143] As the article previously analyzed, the POPIA and the GDPR have many similarities.[144] Since the two

---

139 *Id.*

140 *See* INFORMATION REGULATOR (SOUTH AFRICA), https://www.justice.gov.za/inforeg/ (last visited Nov. 16, 2021) ("The information regulator (South Africa) is an independent body established in terms of section 39 of the protection of personal information act 4 of 2013. It is subject only to the law and the constitution and it is accountable to the national assembly. The information regulator is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of the promotion of access to information act, 2000 (act 2 of 2000), and the protection of personal information act, 2013 (act 4 of 2013).").

141 *See What Businesses Need To Know About POPIA And The GDPR*, SERR SYNERGY, https://serr.co.za/what-businesses-need-to-know-about-popia-and-the-gdpr (last visited Nov. 16, 2021).

142 Nicole O., *supra* note 3.

143 *See* Smith, *supra* note 126.

144 *See* Nel, *supra* note 105.

regulations are similar, the cost of GDPR compliance implies a similar cost for POPIA compliance.[145]

Compliance with the POPIA can also be beneficial for businesses. As consumers become more aware of their privacy rights, they look for companies with effective privacy measures in place to protect their data.[146] Companies that are compliant with strict data privacy regulations may be able to gain trust with consumers and collect more data as a result.[147] Companies can build strong reputations for processing data ethically and enhance their brand image. If a company is known for having data breaches and not protecting consumer information, they are less likely to receive new customers or have new customers consent to data processing.[148] For businesses with e-commerce platforms, consumers need to be able to trust that their financial and other personal information is protected while making a purchase. Compliance with the POPIA may give consumers a sense of data security. Additionally, as previously analyzed, once a company is POPIA compliant, they are likely only a few steps away from being

---

145 *See* Smith, *supra* note 126.

146 *See* Thomas C. Redman & Robert M. Waitman, *Do You Care About Privacy as Much as Your Customers Do?*, HARV. BUS. REV. (Jan. 28, 2020), https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do ("That approach may soon prove short-sighted. What does this intro sentence reference? A 2019 survey conducted by Cisco of 2,601 adults worldwide examined the actions, not just attitudes, of consumers with respect to their data privacy. (Robert led the work, Tom advised.) The survey reveals an important new group of people — 32% of respondents — who said they care about privacy, are willing to act, and have done so by switching companies or providers over data or data-sharing policies. We call this group privacy actives and, to our best knowledge, this is the first time such a group has been identified.").

147 *See id.*

148 *See* Doug Drinkwater, *Does a data breach really affect your firm's reputation?*, CSO (Jan. 7, 2016), https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html. ("Customers, for one, will often vote with their feet. UK-based fraud prevention company Semafone last year found that the overwhelming majority of people would not do business with a company that had been breached, especially if it had failed to protect its customers' card data. In the survey, conducted by OnePoll, 86.55 percent of 2,000 respondents stated that they were 'not at all likely' or 'not very likely' to do business with an organization that had suffered a data breach involving credit or debit card details. The numbers were slightly lower if home and email addresses and telephone numbers had been lost.").

GDPR compliant.[149] For businesses considering expanding to the EU, meeting the requirements of the POPIA could mean that they are more prepared to enter the European Union.[150]

Africa's economy has grown over the past few years,[151] and as a result, companies are starting to open franchises across Africa.[152] A big concern with franchising is data privacy.[153] Consumer information processed by a franchisee is often shared with the franchiser.[154] If a franchisee in South Africa shares consumer data with a franchiser in the United States and the franchiser's data is breached, the company may be subject to penalties if the proper data privacy measures are not in place.[155] Companies considering franchising in South Africa will likely have to be POPIA compliant.[156]

E. Business Expansion In South Africa

Companies consider several factors when deciding on international business expansion.[157] Some factors that may present

---

149 Nel, *supra* note 105.

150 Yav, *supra* note 106, at 20 ("POPIA might be considered as an intermediary to assuring compliance to the GDPR. Organizations which are not already in compliance with POPIA will certainly not meet the threshold of compliance of the GDPR, whereas organizations who already have sound company practices as per POPIA in relation to data protection will have significantly less problems in adapting to the new legislation.").

151 Tyre Jr. et al., *supra* note 41 ("The African Development Bank estimates that by 2030, much of Africa will attain lower-middle to middle class majorities and consumer spending will expand to US$2.2 trillion.").

152 *Id.* at 8.

153 *Id.* at 9. ("Other legislative reforms that may impact franchising across the continent relate to data privacy and protection.").

154 *Id.* ("franchisors do not maintain complete control over their franchisees, and therefore rely on customer data and financial records provided by franchisees to ensure that franchisees' operations are meeting brand standards.").

155 *See id.* at 10.

156 *Id.* at 11 ("POPIA is expected to become effective by the end of 2018, so businesses planning on conducting international business within the country must ensure their data privacy and protection policies and procedures protections are compliant with the Act.").

157 *See* Chad Brooks, *Going Global: How to Expand Your Business Internationally*, BUSINESS NEWS DAILY (May 8, 2019), https://www.businessnewsdaily.com/8211-expand-business-internationally.html.

challenges when expanding internationally include language and cultural differences, international compliance and regulatory issues, packaging, slower pace, and local competition.[158] In addition to the challenges that companies face when expanding internationally, companies need to ensure that the market in the country they are expanding to can sustain their business. South Africa's data connectivity, economy, and data privacy regulations may influence business development in South Africa.

As analyzed earlier, data connectivity in South Africa is expanding.[159] Companies complete a variety of tasks that require data connectivity.[160] In addition to companies using the internet to complete tasks, consumers also use the internet to complete transactions. E-commerce is constantly growing, making internet transactions an important part of doing business.[161] If South Africa

---

158 *See id.* ("No major business decision is without its hurdles, but global expansion comes with its own unique set of obstacles.").

159 *See generally* Roser et al., *supra* note 8; *The Internet and South Africa*, *supra* note 43 ("The South African government announced its national broadband fibre-optic policy, South Africa Connect, in 2014 and aims to provide fibre connection to every home by 2020, ensuring faster, more reliable, stable, affordable and accessible Internet services.").

160 *See* Catherine Capozzi, *Importance of Technology in International Business*, BIZ FLUENT (Sept. 26, 2017), https://bizfluent.com/about-7542416-importance-technology-international-business.html. ("The most important modes of technology in international business include electronic communication such as emails, texts, faxes and virtual conferences. Tracking methods for shipping and purchasing is another huge technological innovation, as it allows businesses to verify the delivery of goods and the quantity of inventory purchased. Electronic spreadsheets and databases are other inventions that allow international companies to manage and store their information with greater ease. Put some of this in the body of the text – the text itself is redundant to prior discussion, but this information is really interesting.")

161 *See E-commerce worldwide - statistics & facts*, STATISTA (Oct. 26, 2020), https://www.statista.com/topics/871/online-shopping/. ("Over the last few years, e-commerce has become an indispensable part of the global retail framework. Like many other industries, the retail landscape has undergone a substantial transformation following the advent of the internet, and thanks to the ongoing digitalization of modern life, consumers from virtually every country now profit from the perks of online transactions.")

continues to increase connectivity and quality, it may become a more attractive location for business expansion.[162]

The details of South Africa's economy are beyond the scope of this article, rather, the article examines technology's role in South Africa's economic growth. Increased data connection can promote economic growth.[163] Increasing internet access is positively correlated with an increase in job creation.[164] In addition to job creation, access to quality internet helps facilitate e-commerce.[165] South Africa is a leader in the continent for digital job creation and has a "strong consumer demand for digital businesses."[166] Other factors that show South Africa's strong potential for digital and economic growth are South Africa's low frequency of power outages, South Africa's high digital transparency measures, and South Africa's ranking as a financial hub.[167]

---

[162] *See generally* Bhaskar Chakravorti & Ravi Shankar Chaturvedi, *Research: How Technology Could Promote Growth in 6 African Countries*, HARV. BUS. REV. (Dec. 4, 2019), https://hbr.org/2019/12/research-how-technology-could-promote-growth-in-6-african-countries ("With 64% internet penetration, and broadband and mobile internet speeds below the global median, South Africa should increase internet access to a broader cross-section of its population and improve the quality of the access.").

[163] *See generally* Karibian, *supra* note 38 ("Experts also have stressed the critical role high bandwidth internet access in Africa will have for boosting Africa's economy in the future.").

[164] *See id.* ("Makhtar Diop, the World Banks' Vice President for Infrastructure, stated that 'the digital agenda is first and foremost a growth and jobs agenda.' He goes on to explain that 'broadening internet access means creating millions of job opportunities.'").

[165] *See id.* ("For many Africa countries, e-commerce is heavily underutilized, but installing suitable, accessible internet throughout the continent can make conducting e-commerce internationally a top priority for most African businesses.").

[166] *See* Chakravorti & Chaturvedi, *supra* note 162 ("South Africa is a regional leader in the Ease of Creating Digital Jobs, buoyed by strong consumer demand for digital businesses and an institutional environment that offers supportive regulations, comparing favorably against key emerging market nations in Latin American and Asian/Southeast Asian regions. South Africa is also a regional leader in the deployment of several emerging technologies, such as biometric data and payment cards to deliver social security, drones in mining, which helps keep it at the innovative edge.").

[167] *See id.* ("South Africa also has several facilitating factors that reinforce its strengths: on a continent that struggles with power outages, it has the lowest

Data privacy regulations are just one group of regulations out of many that impact how businesses operate.[168] No matter where a company does business, they will likely have to comply with some form of regulation. By regulating data privacy through the POPIA, South Africa sets out compliance measures companies must take to ensure the privacy of data subjects.[169] Companies looking to do business in South Africa can now look to the POPIA to see how to properly collect data in South Africa.

F. Businesses should consider the POPIA as a benefit of expanding into South Africa.

Businesses should consider the POPIA as a benefit of expanding into South Africa. Businesses expanding into South Africa can look to the POPIA to understand how to comply with South African data regulations rather than entering the country without specific requirements and running the risks of unknown violations. Additionally, the POPIA eliminates the new data regulations emerging after the company begins conducting business in an unregulated atmosphere. Removing the legal uncertainty for data protection in South Africa makes expansion into South Africa less risky.

The POPIA is also beneficial because by complying with the POPIA, a business is closer to complying with the GDPR.[170] Therefore, if a business is looking to expand into the EU in the future or is already present in the EU, complying with the POPIA may be less burdensome and may even align in most parts with the GDPR. However, as discussed above, unlike the GDPR, the POPIA allows for criminal penalties.[171] The criminal penalty may initially discourage some businesses from doing business in South Africa, but businesses

---

frequency of monthly outages among the countries studied; it has high digital transparency measures, including a relatively strong Freedom on the Net score; and it was ranked 19th globally as a financial hub by the World Economic Forum, which also scored the country highly for having one of the most advanced transport infrastructures in the region.").

168 Bill Williams, *How Does the Law Affect Businesses?*, MYSTORY (Feb. 7, 2017), https://yourstory.com/mystory/6d7c3b1641-how-does-the-law-affect-businesses-.

169 *See generally* Nicole O., *supra* note 3.

170 Nel, *supra* note 105; Yav, *supra* note 106, at 20.

171 *See generally PoPI vs. GDPR*, *supra* note 105.

will not have to face any penalties if they comply with the legislation and the imposition of a criminal penalty is unlikely.[172] Additionally, the monetary penalty for the POPIA is less than the GDPR.[173] Businesses may also be hesitant in expanding to South Africa because the POPIA is a new regulation without established case law. However, businesses may look at the case law emerging in relation to the GDPR to see how the requirements for the GDPR are being enforced since the GDPR and the POPIA share similarities. Businesses may also ask why they should expand into a country where data connectivity is still advancing. Businesses that expand into South Africa now while data connectivity is expanding will have a competitive advantage over companies that expand into South Africa later after the data connection is already established. The first businesses to expand into South Africa can build a customer base and establish loyalty to the business's brand which will help the companies compete as South Africa's economy grows, and other businesses expand into the country. Overall, the POPIA should not discourage businesses from expanding into South Africa. In fact, businesses should consider the POPIA a benefit of expanding into South Africa.

IV. CONCLUSION

Overall, the GDPR and the POPIA are similar in many ways; however, the GDPR reaches more countries than POPIA, sets out a clear seventy-two-hour notification requirement, implements higher monetary fines, requires privacy by design and impact assessments, and allows for data portability. Whereas the POPIA protects not only natural people but also legal entities, requires data protection officers for all companies, and imposes criminal sanctions. If an organization is already in compliance with the POPIA the only major changes the organization would have to make to become compliant with the GDPR would be to implement privacy by design, impact assessments,

---

[172] *Protection of Personal Information Act Summary*, MICHALSONS, https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia (last visited Nov. 16, 2021).

[173] *See generally PoPI vs. GDPR*, *supra* note 105.

and data portability. If an organization is already in compliance with the GDPR, the organization will likely not have to take any major additional steps to be in compliance with the POPIA.

The article then analyzed the GDPR's cost on businesses in the EU. Since the GDPR and the POPIA have many similarities, it is important to know the cost of compliance with the GDPR to predict POPIA compliance cost. The GDPR is costing international businesses more than EU companies to comply with the GDPR.[174] The two ways to avoid the GDPR are to stop doing business in Europe or get rid of personal data.[175]

The article analyzed the POPIA's impact on consumers. Consumers can choose who they share their data with, opt-out of marketing communications, ask what information a company has on the consumer, and have it deleted, and complain to the business or Information Regulator if the consumer feels the consumer's data is not being handled correctly.[176] The article goes into detail about the implications of these consumer benefits.

The article analyzed the POPIA's impact on businesses. Businesses will mainly be impacted by the cost of complying with the POPIA. Appointing a Data Protection Officer, training employees, and ensuring the quality of data are just a few of the compliance requirements outlined above which can prove costly.[177] Businesses will also benefit from complying with the POPIA. Consumers are becoming more aware of data privacy and companies can build a strong reputation for protecting consumer data by complying with data regulations and as a result aid in customer growth and retention.[178] Additionally, compliance with the POPIA can put companies closer to complying with the GDPR.[179]

---

174 Smith, *supra* note 126.

175 *Id.*

176 *POPI Act to fuel better customer experiences for South Africans*, *supra* note 136.

177 See generally Smith, *supra* note 126.

178 Redman & Waitman, *supra* note 146.

179 Nel, *supra* note 105; Yav, *supra* note 106, at 20.

The article analyzed the POPIA's impact on business expansion in South Africa. Companies look at several factors when deciding if they want to expand into different countries. South Africa's data connectivity, economy, and data privacy regulations may influence business development in South Africa. South Africa is increasing data connectivity.[180] The article did not examine South Africa's economy in detail; however, the article discussed technology's role in South Africa's economic growth. Increased data connection can promote economic growth.[181] Data privacy regulations are just one group of regulations out of many that impact how businesses operate.[182] No matter where a company does business, they will likely have to comply with some form of regulation.

---

[180] *See generally* Roser et al., *supra* note 8; *The Internet and South Africa*, *supra* note 43.

[181] *See generally* Karibian, *supra* note 38.

[182] Williams, *supra* note 168.