LEGAL CHALLENGES OF ESTABLISHING JURISDICTION OVER CLOUD DATA: ADDRESSING THE GAPS IN SOUTH AFRICA'S CYBERCRIME LEGISLATIVE FRAMEWORK

A thesis submitted in fulfilment of the requirements of a Doctor of Philosophy Degree in Law at the University of the Witwatersrand, Johannesburg

By

Name: Melody Musoni

Student Number: 334438

May 2023

Supervisor: Professor Jonathan Klaaren

ACKNOWLEDGEMENTS

Conducting a PhD research during a global pandemic has been challenging. News about millions of people succumbing to Covid-19 left me emotionally drained, mentally exhausted, and constantly worried. During such a tumultuous time, I am grateful to the people who stood by me and provided me with the emotional, moral, and professional support I needed.

Mom and dad, this is for you. To my mother, Florance Chihumbiri Musoni and my father, Samson Musoni, thank you for raising me and providing me with an environment which allowed me to think outside the box. I also want to thank my siblings for their moral support, Ian Musoni, Martha Loveness Musoni, Simbarashe Musoni and Tafadzwa Sharon Musoni. I am grateful to my supervisor Professor Jonathan Klaaren for your guidance, research opportunities and support.

I made promises to a 12-year-old rural girl from Hurungwe District in Mashonaland West Province in Zimbabwe. The promise was to go against odds to attain the highest educational qualifications. Note to self – Melody, you have done it. You have shattered the glass ceiling and fulfilled those seemingly impossible promises you made to yourself.

I want to thank colleagues and friends who have been providing me with various opportunities such as platforms to share my research, engage with other academic scholars, opportunities to writing book chapters and providing me with moral support: Prof Sizwe Snail, Mr Lucien Pierce, Prof Franziska Sucker, Dr Kiru Pillay, Dr Luci Abrahams, Prof Manoj Maharaj, Dr Christian Djeffal, Prof Reto Steiner, Prof Siri Gloppen, and Ms Nicola Green, to mention just a few.

Above all, I want to say thank you Lord Jesus Christ for your grace which has been the machinery behind every success. To God be the glory, honour, and praise!

ABSTRACT

This thesis discusses the problems presented by the emerging technology of cloud computing during cybercrime investigations. One of the main challenges with cloud computing technologies is the lack of clarity on jurisdiction and whether law enforcement agents can exercise unilateral enforcement jurisdiction over remote cloud data. The thesis signifies the challenge by demonstrating how remote access to cloud data can potentially infringe on the sovereignty of foreign states, violate international law, and infringe on people's privacy rights. The underlying concern with cybercrime investigations in the cloud context is that the current laws are not only territorial, but they are also outdated and lacking the ability to complement and address technological advancements. The central question discussed is whether the jurisdictional principles need to be revised to address innovative technological advancements or if the traditional principles suffice and can continue to be of application.

At present, there are diverging views and approaches to dealing with cloud data jurisdiction for criminal investigation purposes. Some scholars, judges and law officers still rely on traditional jurisdictional principles and apply them to cyberspace and cloud environments. They do not see the justification to have separate laws to address activities in cyberspace. However, others advocate for the acclimatisation of new laws to meet the technological changes. Compounding this difference in opinion is the uncertainty in legal frameworks on cybercrime. Such uncertainty has left the topic vacillating between the views of territorialists and those of data exceptionalists. Similarly, South Africa's position on this issue is unequivocal as various pieces of legislation address the issue of cloud jurisdiction differently. This makes this study of utmost importance.

This thesis argues that law should be developed to address the technological changes presented by cloud computing technologies. Traditional jurisdictional principles which emphasise on geographical territory are not sufficient to address the unique features of cloud data. Pre-internet based jurisdictional principles should not be directly applied in cyberspace or cyber-environments. It is important for law to be developed in a manner which allows it to adequately address technological developments. One way of achieving this is by reformulating jurisdictional principles to conform with the emerging technologies. Apart from law, lawyers and law makers should leverage the use of other regulatory modalities such as code to regulate online conduct. Code can play the role of law which can effectively regulate cyberspaces as well as solve the data jurisdictional problem. This thesis supports the notion of reformulation of jurisdictional principles to address these challenges. In addition, it also points out the importance of reinforcing the current measures in place to address jurisdictional challenges.

ABBREVIATIONS AND ACRONYMS

4IR	4th Industrial Revolution
AI	Artificial Intelligence
ACHPR	African Charter of Human and Peoples' Rights
ACRWC	African Charter on the Rights and Welfare of the Child
APEC	Asia Pacific Economic Cooperation
ARPANet	Advanced Research Project Agency Network
ASEAN	Association of South East Asian Nations
AU	African Union
AUC	African Union Commission
AWS	Amazon Web Services
BATX	Baidu, Alibaba, Tencent and Xiaomi
CIA	Confidentiality Integrity Availability
COE	Council of Europe
DCS	Department of Correctional Services
DDOS	Distributed Denial of Service
DHA	Department of Home Affairs
DHS	Department of Human Settlement
DNS	Domain Name System
DOC	Department of Communications
DOD	Department of Defence
DOJ	Department of Justice
DOS	Denial of Service
DSD	Department of Social Development
DTPS	Department of Telecommunications and Postal Services

EAC	East African Community
EC	European Commission
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECOWAS	Economic Community of West African States
ECTA	Electronic Communications and Transactions Act
ECPA	Electronic Communications Privacy Act
ECSP	Electronic Communications Service Provider
EFF	Electronic Frontier Foundation
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
GAFAM	Google, Apple, Facebook, Amazon and Microsoft
GCA	Global Cybercrime Agenda
GDPR	General Data Protection Regulation
GPAA	Government Pension Administration Agency
GPCE	Government Public Cloud Ecosystem
IaaS	Infrastructure as a Service
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICTs	Information and Communication Technologies
INTERPOL	International Criminal Police Organisation
IoTs	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4

Ipv6	Internet Protocol Version 6
ISO	International Organisation for Standardization
ITU	International Telecommunication Union
ISP	Internet Service Provider
IT	Information Technology
LEA	Law Enforcement Agents
MISS	Minimum Information Security Standards
MLA	Mutual Legal Assistance
MLATs	Mutual Legal Assistance Treaties
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology
NCPF	National Cybersecurity Policy Framework
NDCP	National Data and Cloud Policy
NDP	National Development Plan
NPC	National Planning Commission
OECD	Organisation for Economic Cooperation and Development
PaaS	Platform as a Service
PAIA	Promotion of Access to Information Act
PCIJ	Permanent Court of International Justice
PFMA	Public Finance Management Act
POPIA	Protection of Personal Information Act
PPPs	Public Private Partnerships
SaaS	Software as a Service
SADC	Southern African Development Community
SANDF	South African National Defence Force

SAPS	South African Police Service
SCO	Shanghai Cooperation Organisation
SITA	State Information Technology Agency
SIM	Subscriber Identity/Identification Module
SMME	Small Medium and Macro Enterprises
SMS	Short Messaging Service
SONA	State of the Nation Address
SOP	Standard Operating Procedures
SSA	State Security Agency
TOR	The Onion Routing
T-CY	Cybercrime Convention Committee
UDHR	Universal Declaration on Human Rights
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US	United States
USA	United States of America
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WSIS	World Summit on the Information Society
WWW	World Wide Web

CONTENTS

CHAPTER 1: THE INTERNET, CLOUD COMPUTING AND CYBERCRIME

I. INTRODUCTION

'When the World Health Organisation declared Covid-19 a global pandemic in 2020[1], there was very little expectation on how rapid digital transformation was going to take place. Most governments forced industries, businesses, and institutions to shut down as part of the lockdown restrictions. The direct effect of the lockdown was the emergence of the culture of remote working, remote schooling and increase in e-commerce and e-government. Under 'the new normal', there was a surge in the use of information and communication technologies, the internet, and cloud-based services. Covid-19 can be said to have been the primary contributory factor towards drastic digital transformation and it certainly sped up the process for the 4th Industrial Revolution.'

From the inception of the internet to the present day, there have been drastic changes and technological advancements in the purpose and use of the internet. When the USA congress made the decision to commercialise the internet[2], it never envisaged the explosion in global connectivity, use of the internet and the integral role of ICTs in the economy. Neither did the founding fathers of internet regulation, like John Perry Barlow[3], conceive of an idea where the internet would become indispensable with everyday activities and could possibly not be viewed as an abstract and self-regulated space. The erstwhile days when only computers could access the internet have sunk into oblivion as we progress into the information age, the digital age, or the 4IR.[4] The 4IR is characterised by IoT devices which are constantly accoutred with the same abilities as traditional computers to be connected to the internet. There are now blurred lines between traditional computers and IoT devices. Once connected to the internet, IoT devices can interconnect with other objects over internet networks. Consequently, IoTs

[1] Available at *https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020* accessed on 31 August 2021.

[2] The commercialisation of the internet was spearheaded by the US congress back in 1992. When the internet was first developed by the US DOD it was for security purposes and acted as a backup or recovery system in the event of a nuclear attack. During the ARPANet project, the DOD wanted to link its network to various radio and satellite networks. The internet infrastructure was designed in such a manner that it would continue to reroute communications should it be destroyed or unavailable. Murdoch Watney 'The evolution of legal regulation of the internet to address terrorism and other crimes' (2007) *TSAR* 494 at 494.

[3] John Perry Barlow was the founding member of the EFF. During the Davos conference of 8 February 1996, Barlow made a Declaration of Independence of Cyberspace in which he argued that governments had no sovereignty or jurisdiction over cyberspace. Available at *https://www.eff.org/cyberspace-independence* accessed on 3 January 2020.

[4] Klaus Schwab coined the term Fourth Industrial Revolution to be the next type of industrial revolution that we have shifted into. He defined the term as how technologies like artificial intelligence, autonomous vehicles and the Internet of Things are merging with humans' physical lives. Available at *https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab* accessed on 13 January 2020.

have created a new global infrastructure that allows for information or data to be exchanged. Ultimately, the physical medium now co-exists with the new electronic medium.[5]

Fortuitously, the internet is now competing with the terrestrial world as an alternative platform for human activity.[6] The proliferation of the internet has spawned a new, non-spatial arena where physical activities can be conducted online.[7] This new online space created by the internet is synonymously referred to as cyberspace, the digital world or electronic environment. The recent technological developments on the use of AI have also advanced cyberspace into yet another new space called the metaverse.[8] The internet has opened new communication avenues[9] and technology companies have harnessed the power of the internet to create social media and networking platforms. Indisputable evidence reflect that the dominant number of internet users access the internet for purposes of social media. The prominent social media platforms with extensive number of subscribers or users are Facebook (now Meta), Twitter, Instagram, WhatsApp, YouTube, WeChat and TikTok.[10] Apart from radically transforming how people communicate, the internet has also drastically elevated how business is conducted. As an example, electronic commerce is now the core for various business models.[11] This has even been accelerated by the Covid-19 pandemic which saw a sharp increase in the use of online shopping. One can note that the internet and emerging new technologies have discombobulated traditional business models. For example, technology has changed our understanding of money. Blockchain technologies have enabled the creation of virtual currencies such as bitcoin and the most recent non-fungible tokens, which have gained momentum over fiat currencies. Meanwhile, cloud computing technologies are replacing traditional models of providing IT services.

---

[5] Murdoch Watney 'Cybercrime and the investigation of cybercrime' in Papadopoulos S & Snail S *Cyberlaw @SAIII: The law of the internet in South Africa* 3 ed at 335.

[6] Susan W Brenner 'Fantasy crime: The role of criminal law in virtual worlds' (2008) 11 *Vanderbilt Journal of Entertainment and Technology Law* 1 at 1.

[7] Ibid at 3.

[8] The metaverse has been defined as 'a combination of multiple elements of technology, including virtual reality, augmented reality and video where users "live" within a digital universe.' Mike Snider and Brett Molina 'Everyone wants to own the metaverse including Facebook and Microsoft. But what exactly is it?' USA Today 10 November 2021.

[9] ICTs and social media and social networking platforms allow for real time communication amongst unlimited participants regardless of geographical locations. Facebook, Twitter, Instagram, Telegram, WhatsApp, Facetime, to mention but a few.

[10] Facebook currently has a global reach of over 2,26 billion users. Twitter has over 329 million users. Instagram has around 1 billion users. WhatsApp has over 1,33 billion users. YouTube has over 1,90 billion users. WeChat has around 1 billion users. TikTok has nearly half a billion users. Available at *https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/* and *https://www.internetworldstats.com/stats.htm* accessed on 25 December 2019.

[11] Electronic commerce allows people to pay their taxes online without having to stand in long queues available at *http://www.sarsefiling.co.za/* accessed on 25 December 2019; purchase products at the click of the button, different mobile apps allow people to do business from ordering food on Mr D App available at *https://www.mrdfood.com/* accessed on 25 December 2019; or getting transport on Uber App available at *https://www.uber.com/za/en/* accessed on 25 December 2019.

Whilst crime has always existed before the internet, one can note that the internet and technologies have accelerated the speed, extent, and impact of crime. For example, a crime such as fraud used to be committed against a limited number of people within a specific territory. However, with the use of the internet and technology, such a crime can be committed against countless number of victims located anywhere in the world. The rapid influx of computers and technology, the exponential growth in the number of internet users and massive technological developments has given birth to yet other forms of crime called cybercrimes. As we progress into the 4IR where digitalisation and the internet play a major role, it is important to discuss about cybercrimes as ICTs will continue to be exploited for criminal activities.[12] The prevalence of cyberattacks has shifted the discussion from viewing cybercrimes as media sensationalism or a fabrication of cyber-attack incidents[13] to taking cyber threats and attacks seriously. Recent events, as shall be discussed later in this study, reflect that cyberattacks and cybercrimes are on the rise and cybercrime laws should become firmly embedded in the public crime agenda as something that must be policed.[14] Ironically, LEA also leverage the same ICTs when conducting criminal investigations.[15] The same hacking tools used by criminals to commit crime can also be used by LEA to access and seize electronic evidence. IT developments can therefore be seen to present many opportunities for both criminals and LEA.[16] Some of the techniques available to law enforcement agencies as well as the legality in using such techniques will be discussed in chapter 4 of this study.

Cybercrime has become a serious threat to fundamental human rights, to the rule of law and to the functioning of democratic societies.[17] The right to privacy and the protection of personal data can be threatened by cybercriminals when they unlawfully access people's personal data. When malicious software is disseminated on computer systems, it endangers the property of citizens, businesses, and governments. Some cybercrimes represent attacks against dignity and integrity of individuals, including children. For example, dissemination of intimate images and child pornography. An attack against media, civil society organisations and individuals also threatens the freedom of expression. Democracy is threatened when cybercriminals attack democratic institutions such as governments, parliaments, and government infrastructure. Overall, cybercrime threatens international peace and stability in that

[12] Jonathan Clough 'Cybercrime' (2011) 37 *Commonwealth Law Bulletin* 671 at 671.
[13] David Wall 'The internet as a conduit for criminal activity' in Pattavina, A *Information Technology and the Criminal Justice System* (2015) at 85.
[14] In the early 2000s, cybersecurity experts were leading discussions on cybersecurity. Many assumed that the discussions were economically motivated, and cybercrime was not a major risk. Ibid at 79.
[15] Mark O'Brien 'Clear and present danger? Law and the regulation of the internet' (2005) 14 *Information and Communications Technology Law* 151 at 151.
[16] O'Brien ibid at 160.
[17] Council of Europe 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Final report of the T-CY Cloud Evidence Group' (September 2016) (T-CY Report) at para 9.

military conflicts and political disagreements are often accompanied by cyberattacks.[18] Modern economies and governments' overreliance and dependence on internet and technology makes cybercrime a matter of primary concern for everyone. Each year, there are trillions of security incidents recorded and millions of attacks against computers and data.[19] This justifies the need for and importance of proper criminalisation of cyber criminality and efficient cybercrime investigation procedures.

Proper policing of cyberspace requires efficient and effective criminal procedural processes. Cybercriminals are only successfully prosecuted if LEA have been able to investigate the crime and lawfully conducted searches and seizures. In the case of cybercrime investigations, the relevant evidence is usually in the form of data. When criminals use ICTs and IoT devices, the devices process bountiful amounts of data. The data may be stored on these IoT devices, or it can be stored on remote servers. In most instances, such data are relevant as evidence when LEA are investigating cybercrimes or traditional crimes. Technological developments have resulted in increased amounts of such data being hosted or stored not on ICTs or IoTs but rather in the cloud. The use of cloud computing technologies for storage of data may be a challenge or inconvenience to LEA who may be investigating a crime. This is mainly because cloud computing may potentially result in electronic evidence being stored in foreign, unknown, multiple, and shifting jurisdictions.[20] As will be discussed in this study[21], LEA's access to remote transborder data may raise jurisdictional challenges and conflicts. Abraha correctly points out that the problem with access to cross border data is acute for African countries that are primarily receivers of foreign based internet services, where digital evidence required for domestic criminal investigations may be held overseas.[22] Cybercrime prosecutions are only successful if the jurisdictional hurdles are carefully navigated in compliance not only with national laws but with international law alike.

II. THE INTERNET AND CYBERCRIME OPPORTUNITIES

Before this study focuses on cybercrimes and cloud computing, it is important to have a discussion on the role of internet in the commission of crime. As will be discussed in chapter 3, without the internet, there would not be 'true cybercrimes'[23]. The internet also plays a pivotal role in the provision of cloud services and most features of cloud services are attributed to the internet. Understanding some of the

[18] Ibid.
[19] T-CY Report para 10.
[20] T-CY Report para 11.
[21] Chapter 2 and chapter 4 of this study will demonstrate the technical challenges and legal jurisdictional challenges related to cloud computing as major risks for the rule of law in cyberspace.
[22] Abraha H Halefom 'Government access to digital evidence across borders: Some lessons for Africa' in KM Yilma *The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties* (2020) 1 at 13.
[23] Wall introduced the term 'true cybercrimes' when he differentiated between crimes that are enabled by the computer and crimes that can cease to exist when the computer or internet is taken away. David Wall 'Cybercrime, media and insecurity: The shaping of public perceptions of Cybercrime' (2008) 22 *International Review of Law, Computers & Technology* 45 at 55.

unique features of the internet is relevant in situating this chapter in the broader discussion on legal challenges in establishing jurisdiction over data, particularly electronic evidence held in the cloud.

a. Does the internet transform crime?

Before the advent of the internet, crime and criminal activities were mainly restricted or confined within clearly defined spaces or territories. For criminals to have an international reach, the options were to either coordinate with other criminal syndicates in foreign countries or physically move from one country to the other to commit crime. All this has changed due to the internet. Through the internet, it is easier for crime to become global even when the perpetrators have not left their countries of residency. When one considers modern computer networks and the internet infrastructure, one can note that they are global by nature. A person in one country can make use of IT services being offered by another person in a foreign country. The ability to make use of internet and IT services also means that a crime can be committed remotely. The global nature of such a crime is facilitated by the internet and technology. These features of the internet have constantly challenged the conventional perspectives that criminal law is local in nature[24] or restricted to the territorial jurisdiction in which the offence was committed.[25] The globalisation of the internet widens the scope of harm in the sense that attacks can either be from local cybercriminals or from foreign-based criminals.[26] The global, yet local nature of cybercrime is what Wall has termed glocalisation.[27]

Most countries have been experiencing an increase in the accessibility and uptake of technology and the internet.[28] By the end of 2021, 22% of the total population in Sub-Saharan Africa was using mobile internet.[29] Progressively, the internet is increasingly becoming more affordable and accessible which ensures its availability to both offenders and victims.[30] New technologies such as botnets and automation have a potential to magnify the potential impact of offending particularly in relation to facilitating the crime of disseminating malicious software.[31] One piece of software launched on the internet can replicate and attack millions of computers at the same time.[32]

[24] Jonathan Clough 'The Council of Europe Convention on Cybercrime: Defining "Crime" in a digital world' (2012) 13 *Criminal Law Forum* 363 at 365.
[25] Clough op cit note 12 at 674.
[26] Clough op cit note 12 at 680.
[27] Wall op cit note 13 at 79.
[28] Clough op cit note 12 at 673.
[29] 'The state of mobile internet connectivity 2022' GSMA Report. Available at https://www.gsma.com/r/somic/, accessed on 11 April 2023.
[30] Clough op cit note 12 at 673.
[31] Clough p cit note 12 at 673.
[32] Bert-Jaap Koops 'The internet and its opportunities for cybercrime' (2011) 9 *Tilburg Law School Legal Studies Research Paper Series* 735 at 740.

Apart from having a global reach, the internet also increases the scale of the crime.[33] The notable events of the 'I love you' virus incident demonstrated the global nature of cybercrime as well as its local effects.[34] The recent WannaCry ransomware attack which encrypted 230 000 computers worldwide, including computer files for South African based company, Telkom is also a reminder of the global effects of a cyber-attack. The WannaCry worm was able to infiltrate computers within a short period of four hours.[35] Victims from a single cyberattack incident can potentially include thousands of people, businesses, and governments. The sheer number of people online also provides an unprecedented pool of potential offenders and victims. The growth in the number of internet users as well as the use of cloud-based services has been steadily increasing over the years. As of 31 March 2021, the estimated number of internet users across the globe was over five billion people.[36] Of Africa's population of slightly over one billion people, more than five hundred million people are internet users.[37] This is a significant increase from the estimate of four million internet users in the year 2000.[38] Africa's internet penetration rate is currently at 43.2 per cent while the world total internet penetration rate is 65.6 per cent.[39] These high numbers of internet users indicate that the internet has the potential to exacerbate the scale of committed offences.

The internet makes it convenient for perpetrators to look for vulnerable computer systems anywhere in the world from the comfort of their homes or internet café.[40] The transnational nature of cybercrime means that the traditional meaning of 'crime scene' must be interpreted differently.[41]

---

[33] Mohammed Chawki and Ezekiel Uzor Okike 'Fighting cybercrime: Issues for the future' (2009) *African Journal of Crime and Criminal Justice* 1 at 114.

[34] Onel de Guzman was a university student in the Philippines who disseminated the 'I love you' virus. The virus infiltrated computers of over 45 million internet users in over twenty countries. The monetary damages caused by the virus ranged from between two US$ to ten billion US$. This all happened in the short space of two hours. During that time, it was not a crime to disseminate a virus in the Philippines. This meant that Mr Guzman could not be extradited to the countries which suffered the damages to stand trial. As a result, Mr Guzman could not be prosecuted both in the Philippines and the USA. The 'I love you' virus is also called the lovebug. Michael Nycyk *Computer hackers and hacking: Exploring those lurking behind the screen* (2018) 1 at 7.

[35] The WannaCry ransomware attack was a global epidemic that took place in May 2017. This ransomware attack spread through computers operating Microsoft Windows. User's files were held hostage, and a Bitcoin ransom was demanded for their return. Available at *https://www.kaspersky.co.za/resource-center/threats/ransomware-wannacry*, accessed on 28 December 2019.

[36] Actual estimated statistics being five billion, one hundred and sixty-eight million, seven hundred and eighty thousand, six hundred and seven. Available at *https://www.internetworldstats.com/stats.htm*, accessed on 1 March 2022.

[37] Available at *https://www.internetworldstats.com/stats.htm*, accessed on 1 March 2022.

[38] Available at *https://www.internetworldstats.com/stats.htm*, accessed on 25 December 2019.

[39] Available at *https://www.internetworldstats.com/stats.htm*, accessed on 25 December 2019. Previous studies conducted in 2013 indicated that internet penetration rate in Africa was at 16 %. Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, Steve Chon and Chen Da 'Crime in cyberspace: Offenders and the role of organised crime groups' (2013) *Australian National University Cybercrime Observatory Working Paper* 1 at 2.

[40] Koops op cit note 32 at 740.

[41] Fawzia Cassim 'Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players' (2011) *The Comparative and International Law Journal of Southern Africa* 123 at 125.

Traditionally, the term 'crime scene' meant a physical place where the offender committed the crime and where the evidence of the crime could be gathered. With the internet, one cannot pinpoint the actual object of the crime, location of the perpetrator, location of the victims as well as location of the evidence to prove the commission of the crime. The object of traditional crimes is mostly tangible in nature as the main perpetrator is generally physically present during the commission of the crime.[42] The crime is predominantly committed and investigated within the borders of the same country and jurisdiction and choice of law is seldom an issue of dispute.[43] However, with offences committed over the internet, it is not always straightforward to point out the location of the crime or the location of the evidence to prove the crime. Corollary to this is that criminal laws which may be of application to traditional crime may not be appropriate to apply to unlawful conduct taking place over the internet.

The internet challenges traditional principles governing crime. The exploitation of victims over the internet calls for lawmakers to amend existing criminal laws as well as create new offences to bring criminal justice to victims. As will be discussed in chapter 3, the misuse and abuse of the internet and technologies bring about the creation of crimes that never existed in the past. These crimes will be referred to as true cybercrimes. The snail-paced nature of most legal systems can never be parallel to the fast-paced developments in technology. Criminals are mindful of the lacunae in laws regulating conduct in cyberspace both within national territories and at an international level. In territories where there is some form of internet regulation, the laws are either inadequate on prescribing unlawful conduct as cybercrimes or inadequate in having appropriate measures to promote mutual legal assistance with other countries. The global nature of the internet and cloud services, coupled with the different legal systems and legal frameworks on internet regulation enable criminals to confidently launch their operations in other countries. Criminals are aware that either other countries do not have jurisdiction to prosecute them or do not have the laws in place which criminalises certain conduct. Criminals therefore enjoy the safe havens that have emerged due to lack of regulation in different countries.

The internet has created new forms of crime. As will be discussed in chapter 3 of this study, there are various crimes which came into existence due to the misuse or abuse of the internet and technologies. Crimes such as DOS attacks, ransomware, crypto jacking and cyber-fraud are examples of crimes which were perpetrated as a result of the internet. In most cases, existing criminal laws may not be adequate to address these novel offences. Some of the laws will not be able to address the complexities associated with investigation of cybercrime.[44]

While the above discussion has demonstrated that the internet transformed crime, during the nascent stages of the internet, there were concerns that there was not enough evidence to support the

[42] Watney op cit note 5 at 334.
[43] Ibid.
[44] Ibid at 337.

global reach of cybercrime[45] or to give a clearer picture of the scale of the problem.[46] Some considered reports on cyberattacks and cybercrime as giving a distorted picture.[47] This made it difficult for cybercrime to be included in official crime statistics.[48] A further factor that was identified as complicating the gathering and comparison of national crime statistics was the fact that cybercrimes are committed in or have effects in at least two states and in some states risking multiple reporting or no reporting at all.[49] Brenner and Goodman raised concerns over the cybercrime statistics and surveys and suggested that the statistics could have been biased so as to promote the services of information security companies.[50] Inadequate data on reported cybercrimes was also due to lack of police with expertise and/or resources to detect or investigate cybercrime.[51] The absence of criminal investigations means that accurate records on cybercrime may not be available. Reputational damage was also identified as another reason why incorrect statistics on cybercrime was recorded as organisations feared negative publicity if they were to report an attack on their computer systems.[52] Incorrect statistics and lack of evidence-based research on cybercrime activity in cyberspace can impede the development of sound countermeasures.[53] This position has also changed over the years as more research and surveys have been conducted which indicated the prevalence of cybercrime activities. Further, the coming into force of data protection laws have also made it mandatory for organisations to report on cyberattacks and data breaches.[54]

b. What role does internet regulation play in the context of cybercrimes?

Internet regulation plays a key role in the prevention and combating of cybercrime. Regulation of the internet is important not only in criminalizing unlawful conduct as offenses, but also in addressing procedural issues, jurisdictional challenges, foster international cooperation and providing parameters for internet service provider responsibility and liability.[55] Internet regulation can be defined as having clearly defined rules which address any unlawful conduct taking place on information systems or computer systems. Regulation of the internet also asks questions around jurisdiction to prescribe laws, jurisdiction to adjudicate over cyber-related matters and jurisdictional authority to enforce the law. The

[45] Marc D Goodman and Susan W Brenner 'The emerging consensus on criminal conduct in cyberspace' (2002) 10 *International Journal of Law and Information Technology* 139.
[46] Clough op cit note 12 at 674.
[47] Ibid.
[48] Ibid.
[49] Goodman and Brenner op cit note 45 at 156 - 157.
[50] Ibid at 158 -159. Actual losses are difficult to quantify, but include direct costs of repairing systems and software, the loss of access or services to users and consequent damage, the loss of valuable data and the loss of revenue from site operations.
[51] Clough op cit note 12 at 674.
[52] Ibid.
[53] There is lack of evidence about the extent, role and nature of organised crime groups operating in cyberspace. Broadhurst et al op cit note 39 at 9.
[54] Section 22 of the Protection of Personal Information Act 4 of 2013.
[55] United Nations Office on Drugs and Crime 'Comprehensive Study on Cybercrime' 2013 United Nations at xviii.

importance of regulating the internet is to make accountable those who commit crime online as the effects of crime can be experienced in the real world.[56] Due to the global nature of the internet and cybercrime, governing of cybercrime should entail a combination of laws where the crime is committed and where the impact of the crime is experienced.[57] Electronic information may be linked to a person in the real world.[58] The 'I love you' virus is one of the earlier cases which highlighted the need for regulation of online conduct, and the implementation of robust cybercrime laws[59] in different countries.[60]

One can argue that the resistance to internet regulation specifically on regulating harmful and unlawful activities online can also be attributed to the constant debate on whether cybercrimes are any different from traditional crimes to warrant separate legislative framework. Brenner and Koops had correctly noted that new laws criminalising cybercrime are only relevant if there are material differences between the traditional crimes and cybercrimes.[61] Some have argued that there is a lack of clarity on what is particularly 'cyber' about cybercrimes[62] to justify the need to adopt new specific laws. After a critical investigation on public perceptions of cybercrime, Wall concluded that the conceptualisation on cybercrimes is causing people to confuse rhetoric from reality.[63] If people are confused about whether there is a crime or not, this has the effect of making it difficult to adopt new laws focused on cybercrimes. Some of the notable differences between cybercrimes and traditional crimes is that cybercrimes appear to be largely free of physical time frame and instantaneous.[64] 'If there is topography of the internet, it is expressed more in terms of levels of access to the internet and language rather than in terms of physical geography'.[65]

The above discussion has alluded that the internet infrastructure is unique from the terrestrial environment to which our criminal laws are hinged on, which clarified and justified why cybercrimes

[56] Watney op cit note 5 at 335.
[57] Ibid. Clough correctly noted that although many offences are transnational in nature, cybercrime presents unique challenges due to the inherently transnational nature of the underlying technology which justifies the need for harmonisation of laws. Harmonisation of laws has the effect of eliminating or reducing the incidence of safe havens. Jonathan Clough 'A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation' (2014) *Monash University Law Review* 698 at 700 – 701.
[58] Watney op cit note 5 at 335.
[59] Research study conducted in Nigeria pointed that cybercrime laws are not properly implemented. A.C. Onuora, D.C. Uche, F.O. Ogbunude and F.O. Uwazuruike 'The challenges of cybercrime in Nigeria: An overview' (2017) *AIPFU Journal of School of Sciences* 1 at 4.
[60] Other countries such as Tanzania face the same challenge of not having adequate laws which accommodate modern cybercrimes such as transmission of harmful codes and unauthorised access to information. Metson Robinson *A critical analysis on the status of cyber crimes and legal reforms in Tanzania* (unpublished LLM thesis, University of Mzumbe 2015) 1 at 5.
[61] Susan W Brenner & Bert-Jaap Koops 'Approaches to cybercrime jurisdiction' (2004) 4 *Journal of High Technology Law* 1.
[62] Wall op cit note 23 at 45.
[63] Ibid at 48.
[64] Wall op cit note 13 at 87.
[65] Ibid.

should be viewed as different from traditional crimes. One can argue that with the technological innovations which have resulted in the evolution of crime, new set of rules need to be implemented to govern cybercrimes. Such technological innovations include cloud computing technologies. Instead of continuously relying on rigid territorially based principles on sovereignty, technological innovations have warranted the evolution of jurisdictional principles.

Post's bridge analogy[66] signifies the following issues which justifies internet governance and regulation. First, when laws are drafted, lawmakers seek to address the *status quo* and prevailing circumstances. This is what makes law relevant, clear, and not vague. Secondly, when law is made, lawmakers cannot premonition how technological events can disrupt and overturn the legal principles at that point in time.[67] Technological developments come from different camps outside of lawmakers' expertise. It should be noted that law and policy will continue to lag innovation. Cachalia and Klaaren correctly pointed out that 'law constitutes an adaptive resource that can and should respond to disruptive technological change and re-examining concepts and creating new, more adequate conceptions'.[68] This obviously requires time for lawmakers to draft and deliberate on how the law should be devised. Indeed, today's contemporary legal debates on disruptive technologies may potentially be rendered irrelevant as new innovative solutions enter the market. This would require the law and the legal discourse to re-adapt and respond to such new technologies in a way that ensures effective legal regulation. Like Post's analogy of a bridge which could no longer sustain the increase in traffic, laws can also become outdated with changes in the economy which warrants the need to either revamp the laws entirely or extend the law to accommodate the changes.

Lastly, development of common law or other antiquated criminal statutes is not always a viable legal recourse and at times it is imperative to introduce a completely new set of laws. Post correctly noted that due to the volumes of information that the internet can instantaneously process, most laws need to be revised to catch up with the internet scale up. During the embryonic stages of the internet, arguments for the application of existing criminal laws to cybercrimes made sense.[69] However, there has been drastic changes in technology which justifies the need for new cybercrime laws. At the time of finalisation of this study, South Africa promulgated its cybercrime law which addressed the loopholes

[66] In demonstrating why traditional laws are not applicable to unlawful conduct committed in cyberspace, Post illustrated with an analogy of a bridge that was built with a carrying capacity of 1000 vehicles per hour which is suddenly expected to carry 10 billion vehicles within the same time frame. David G Post 'The challenges of cyberlaw' in Sean A Pager and Adam Candeub *Transitional Culture in The Internet Age* (2012) 18 at 22.

[67] New technologies have changed the face of regulatory frameworks. For example, finance-related laws were passed when the definition of legal tender was very restricted. Today, a lot of people are transacting in cryptocurrency and these types of transactions are not regulated as the lawmakers never envisaged the development of the blockchain technology.

[68] Firoz Cachalia and Jonathan Klaaren 'Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional law of privacy in South Africa: Towards a public law perspective on constitutional privacy in the era of digitalisation' (2021) 14 *Digital Pathways Oxford Paper Series* 1 at 32.

[69] Susan W Brenner 'Is there such a thing as "virtual crime"?' (2001) 4 *California Criminal Law Review* 1 para 129.

under its common law and existing statutory framework. This study examines this new law and points out the jurisdictional hurdles and loopholes when investigating criminal conduct in cyberspace. It argues that technological innovations will continue to challenge cybercrime laws and principles on jurisdiction, and it is important for legal frameworks to address these new technological changes.

c. What is the relevance of criminal law in cyberspace?

As will be noted in this study, the criminal justice system is lagging well behind technology. There are several problems and challenges within South Africa's criminal justice system[70] as well as criminal justice systems in other countries. Such challenges beg the question of whether criminal law provides effective recourse to address unlawful and harmful conduct online. For example, with the crime of cyberstalking or cyberbullying, the victim can change their device or social media security settings to block any further communication from the perpetrator. At the same time, the victim can approach different service providers and request them to take down any content which may be used to harass or bully them online. This relief is much effective and quicker compared to solutions provided in terms of criminal law. If there are other effective and expedient avenues to address unlawful and harmful conduct online, why then do we need criminal law? Theories of punishment may provide an answer to this question.

There are different theories[71] in criminal law which justify criminal law and its punitive measures. One of these theories is the deterrence theory, which seeks to deter individuals and society from committing crime.[72] The rationale behind the deterrence theory is that if punishment is imposed, it sends out a message to people that crime will be punished and will result in people refraining from engaging in criminal conduct.[73] Snyman debunked the correctness of this theory in the South African context. He argues that there is a misconception that the effectiveness of the deterrence depends on the severity of the punishment and that the theory is accordingly effective only if a relatively severe punishment is prescribed and imposed. His argument is that the success of the theory depends on the probability for successful investigation and prosecution.[74] Criminal laws can only succeed in deterring unlawful conduct if the police can identify the perpetrator, investigate the crime, and for the perpetrator

[70] Snyman has correctly noted that South Africa's criminal justice system is dysfunctional. There is an alarming increase in crime rate, ineffective policing and prosecution of criminals and the congested prison system. CR Snyman *Criminal Law* 5 (ed) (2008) at 21 and 24.

[71] The theory of retribution seeks to restore the balance that has been disturbed by the commission of the crime. Ibid at 11. The preventive theory is aimed at preventing crime. The success of the preventive theory depends largely upon the ability of a court to establish beforehand which accused are so dangerous from society. Ibid at 15. The reformative theory seeks to bring reformation to the offender as it focuses on the reasons why the offender committed the crime. It could have been because of some personality defects, psychological factors stemming from his background. Ibid at 18.

[72] Ibid.

[73] Ibid.

[74] Ibid.

to be prosecuted and serve their sentence.[75] The deterrence theory was also prevalent among scholars who advocated for a new law in South Africa to replace the Electronic Communications and Transactions Act.[76] The argument was that the ECT Act lacked harsher sentences and penalties.[77]

In support of Snyman's argument, this study submits that the deterrence theory plays an insignificant role in South Africa particularly with the prosecution and conviction of cybercriminals. Though statistics released by South Africa's National Cybersecurity Hub and cybersecurity companies indicate an increase in cybercrimes in the country, there are fewer prosecutions of true cybercrimes. Cybercrime still pays in South Africa. Cyberattacks are increasingly becoming the norm. For example, the Department of Justice[78], the City of Johannesburg[79], an electricity supply company[8081], Transnet[82], multiple banks and several companies were victims of cyberattacks and reported cyberattack incidents. Despite the media having reported and covered these events, there is no information on whether the perpetrators were identified, or the arrests were made. Failure to bring perpetrators to justice may suggest that the criminal sanctions are not effective.

Legal measures play a key role in the prevention and combatting of cybercrime. Law is a dynamic tool that enables the state to respond to new societal and security challenges, such as the appropriate balance between privacy and crime control.[83] For an effective, transparent, and fair criminal justice system, criminal laws should be clear and there should be clarity and certainty on what constitutes crime. When dealing with crime committed online, the question that begs to be asked is what role does legislation play in regulating crime committed in cyberspace? Considering that online crime relies much on technology, which is constantly changing, are legal instruments the most appropriate in addressing cybercrime or should we consider technical measures? This study shall revert to this discussion when it considers the role played by code in addressing some of the legal challenges currently faced in the cybercriminal justice system.

---

[75] Ibid.
[76] Electronic Communications and Transactions Act, 25 of 2002.
[77] Cassim op cit note 41 at 132.
[78] Sesona Ngqakamba 'Justice department IT system brought down in ransomware attack' 9 September 2021 News 24. Available at *https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909,* accessed on 14 September 2021.
[79] Admire Moyo 'City of Johannesburg hit by cyber attack' 25 October 2019. Available at *https://www.itweb.co.za/content/dgp45qaG8gZ7X9l8*, accessed on 14 September 2021.
[80] Melody Musoni 'South Africa's "smart cities" and cybersecurity' 27 July 2019 iAfrikan News. Available at *https://www.iafrikan.com/2019/07/27/is-south-africa-cyber-ready-for-smart-cities/,* accessed on 14 September 2021.
[81] 'Ransomware hits Johannesburg electricity supply' 26 July 2019 BBC News. Available at *https://www.bbc.com/news/technology-49125853*, accessed on 14 September 2021.
[82] Ryan Gallagher and Paul Burkhardt 'Death kitty ransomware linked to South African port attack' 29 July 2021 Bloomberg. Available at *https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-port*s, accessed on 14 September 2021.
[83]UN Report op cit note 55 at 51.

One of the notable challenges when criminalising cybercrimes are the difficulties in defining the laws which provides for the apprehension and prosecution of cybercriminals.[84] An adequate legislative framework is a necessary requirement for the investigation and prosecution of cybercrime.[85] As a consequence of the constant technological advancement and subsequent development of cybercrime, lawmakers must continuously respond to the developments and monitor the effectiveness of existing legal approaches.[86] Drafting cybercrime legislation separately may result in significant duplication and waste of resources.[87] It is also necessary to monitor the development of international standards and strategies.[88] While this might seem straightforward, it raises some difficult issues. Goodman and Brenner correctly note that states criminalise cyber-related offences differently. There is a lack of uniformity on the extent to which laws address cyber-specific offences.[89]

The principle of *nullum crimen sine lege* (no crime without law) requires that the conduct constituting any criminal offence must be described clearly in law.[90] The UN Cybercrime Report further noted that there should be extended protection of traditional legal interests against new forms of computer related acts and new objects required may include definitions such as computer data or computer information and legal interests such as the integrity of computer systems.[91] The other issue is how does a country's cybercrime laws, or lack of such laws, impact on other countries? As a result of the failure to have cybercrime legislation by the Philippines government, a Philippine national was not prosecuted despite inflicting damage in 20 countries. The Love Bug cyberattack was an early example which illustrated the fragile nature of the modern networked world.[92] Nations must modernize their criminal procedural and substantive laws. The justification for an adequate framework of cybercrime emanates from the understanding that existing criminal laws are antiquated, and their procedural processes are unsuitable in cyberspace. For example, most search warrants only authorise the search and seizure of tangible evidence instead of electronic evidence.[93]

It is imperative for countries to have criminal and procedural laws that provide for the prevention, detection, investigation, and prosecution of cybercrime.[94] Regulation of conduct on the internet by one country is insufficient. This is mainly because an investigating state cannot obtain assistance from a foreign state to investigate a crime if such conduct is not considered as a crime in the

[84] Goodman and Brenner op cit note 45 at 141.
[85] Marco Gercke 'Europe's legal approaches to cybercrime' (2009) 10 *ERA Forum* 409 at 410.
[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Goodman and Brenner op cit note 45 at 141.
[90] UN Report op cit note 55 at 53 - 54.
[91] Ibid.
[92] Goodman and Brenner op cit note 45 at 142.
[93] Ibid.
[94] Watney op cit note 5 at 336.

foreign state.[95] Laws promoting foreign cooperation during crime investigations should provide expedited processes for LEA as electronic trails can easily be covered up.[96] Ultimately, criminal laws which promote foreign cooperation, foreign assistance, evidence sharing and intelligence sharing during cybercrime investigations facilitates locating of a criminal.[97] This can potentially lead to successful prosecutions and convictions.

In sum, criminal law plays an important role in cyberspace. Laws on cybercrime set standards on how users of computer devices and the internet should behave. Cybercrime laws help to deter perpetrators and protect citizens. They recognise the importance of protecting individual privacy during investigations by providing minimum protection standards in areas such as evidence gathering, data handling and retention and enable cooperation between countries in criminal matters involving cybercrime and electronic evidence.[98]

d. A primer to jurisdictional principles

Cloud computing technology is an emerging internet-based technology which is disrupting the traditional models of computing. Cloud computing technology is reshaping data processing[99] and data management.[100] It defies geographical boundaries and limitations and allows for data to be stored on a cloud server hosted from a data centre located anywhere in the world. Through the technology of cloud computing, a cloud user located in South Africa can have their data stored in the cloud on a server hosted in a foreign state. When cloud computing services converge with IoTs, a transnational, multi-jurisdictional environment is created.[101] LEA operating in this environment face a multitude of conflicting laws. The striking unique features of cloud computing and the internet is its ability to hold unlimited amounts of data, instantaneous processing of data and automatic relay of data to any location in the world.[102] It has been noted that due to the proliferation of computers and the internet, digital evidence is rapidly becoming the predominant form of evidence adduced in legal proceedings.[103] With

[95] Watney op cit note 5 at 336.
[96] Ibid.
[97] Ibid.
[98] UN Report op cit note 55 at 53.
[99] The types of data that can be stored and processed in cyberspace is vast and includes confidential information, sensitive and critical information, personal data and financial data. In the world of digital technology, information or data is increasingly becoming commodified and has been termed 'the new gold' or 'the new oil'. In exchange for free online services, companies may request personal data from consumers. Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna 'The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54 *Common Market Law Review* 1309 at 1427.
[100] The commodification of data is subsequently creating a new political economy of information capital. Wall op cit note 13 at 79.
[101] Ian Walden 'Accessing data in the cloud: The long arm of the law enforcement agent' in Pearson Siani & Yee George *Privacy and Security Cloud Computing* (2013) 45 at 45.
[102] Cloud computing allows for the storage of huge amounts of data without occupying and using up of space in the physical world.
[103] Stephen Mason 'Electronic evidence: dealing with encrypted data and understanding software, logic and proof' (2014) 15 *ERA Forum Journal of the Academy of European Law* 25.

the prevalence of cloud computing, it is undeniably imperative that jurisdictional issues relating to cloud services be critically investigated and discussed as relevant evidence is oftentimes stored in cloud structures outside the investigating state. Svantesson correctly proffered that 'the mobility of data undermines the utility of several traditional anchor points'.[104]

As the level of digitalisation in South Africa increases due to embracing the 4IR[105] and emerging technologies, laws should be put in place to adapt to these technological changes. In addition, lawmakers, the judiciary, and LEA should understand the logic of cloud computing and digital data.[106] In the absence of this understanding, lawmakers cannot adequately regulate how cloud computing and other technologies[107] function, which may consequentially lead to the passing of premature regulation which may stifle innovation.[108] Alternatively, the slower adoption of relevant laws could lead to safe havens for criminals.

Amid this digital transformation, two things stand out. First, is the increase in the amount of data generated by ICTs. Second, is the opportunity for new avenues for crime. This study is aimed at the rise in the use of cloud computing services and how these technologies present novel challenges for law enforcement. It is not surprising that malevolent criminals exploit internet opportunities for egregious activities.[109] Criminals tend to be the early adopters of new technologies.[110] They understand

---

[104] Dan Jerker B Svantesson *Internet and Jurisdiction: Global Status Repo*rt (2019) at 31.

[105] On 9 April 2019, the President of the Republic of South Africa, Mr Cyril Ramaphosa appointed members of the Presidential Commission on the Fourth Industrial Revolution (4IR). The Presidential Commission on the Fourth Industrial Revolution- The Department of Telecommunications and Postal Services GN 209 GG 42388 of 9 April 2019. The appointment of the 4IR Commission followed the President's State of the Nation Address on 7 February 2019 (#SONA2019) in which he emphasised on the technological changes that South Africa and the world are facing, available at *https://www.gov.za/speeches/president-cyril-ramaphosa-response-debate-state-nation-address-2019-14-feb-2019-0000* accessed on 29 April 2019. The 2017 National e-Strategy identified the 4IR as one of the three pillars which have a significant, catalytic potential on growth and development. The strategy proposed a digital industrial revolution working group whose function include mobilising society towards the transformation of South Africa into a digital society and knowledge economy by maximising the opportunities brought by the Digital Industrial Revolution. National e-Strategy Digital Society South Africa GN 887 GG 41242 of 10 November 2017. Section 5 of the Electronic Communications and Transactions Act 25 of 2002 mandated the Minister of Communications to develop a national e-strategy.

[106] Svantesson mockingly points out that judges and legislators find it challenging to grasp cyberspace concepts that 'the average five-year-old tosses about with breezy familiarity'. Svantesson op cit note 104 at 31.

[107] Some of the technologies in the 4IR include artificial intelligence, the blockchain, 3D printing and the internet of things. Artificial Intelligence (AI) are computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision making and translation between languages. Oxford Dictionary. A blockchain is a database that is distributed across multiple computers. Karen EC Levy 'Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law' (2017) 3 *Engaging Science, Technology, and Society* 1 at 2.

[108] Anton Didenko 'Regulating fintech: Lessons from Africa' (2018) 19 *San Diego International Law Journal* 311 at 329.

[109] Exploitation of digital technologies to commit or facilitate crime has been around for almost as long as the technology itself. However, it was the proliferation of personal computing in the 1980s and the widespread availability of the internet in the 1990s which created the modern cybercrime environment, and this is further exacerbated by the increase in the use of the Internet of Things and ICTs. Clough op cit note 24 at 365.

[110] Lawrence Trautman 'Virtual currencies: Bitcoin and what now after liberty reserve, silk road and Mt Gox?' (2014) 20 *Richmond Journal of Law and Technology* 1 at 6.

the illimitable possibilities and opportunities that the internet presents[111] and with each new phase of technological innovation, criminals devise innovative ways to manipulate the internet infrastructure and ICTs to commit unlawful activities which we now call cybercrimes.[112] As Clough correctly noted, there is no better illustration of the maxim that *'crime follows opportunity*' than cybercrime.[113] It is human nature to find ways in which to exploit technology for nefarious purposes.[114] Conveniently for criminals, there is always a gap between law and technology. Criminals understand that despite certain conduct being unsavoury, there are usually inadequate laws to criminalise such activities as offenses. Some of the conduct in cyberspace has not been defined as crime[115] which leaves room for criminals to continue to engage such activities without the involvement of law enforcement officials.

The law on jurisdiction informs us that when a crime has been committed within the territory of a state, that state is able to exercise jurisdiction over the crime. This jurisdiction could be the authority of that state to pass laws (prescriptive jurisdiction[116]), to adjudicate matters (adjudicative jurisdiction[117]) and to enforce the laws (enforcement jurisdiction[118]). South African criminal laws empower South African courts to exercise jurisdiction over offences.[119] South Africa's statutory framework on criminal law is quite extensive and different criminal law statutes contain provisions on jurisdiction. This study will mainly focus on the Cybercrimes Act, the CPA and the ECT Act. Other pieces of legislation will be used as points of reference. Courts enjoy the powers to adjudicate over criminal cases or to issue

[111] New technologies increase the computing power of devices, the storage space and reduces costs. Wall correctly anticipated that the IoTs will likely further increase both the spread of and the scope of online criminal opportunities. Wall op cit note 13 at 80 - 81.
[112] The definition for cybercrime is discussed in section II of this chapter.
[113] Clough op cit note 12 at 671.
[114] Clough op cit note 24 at 365.
[115] One famous examples is the May 2000 love bug virus case. Onel de Guzman was a university student in the Philippines who disseminated a virus which was later dubbed the I love you virus. The virus infiltrated computers of over 45 million internet users in over 20 countries. The monetary damages caused by the virus ranged from between US$2 to US$10 billion. This all happened in the short space of 2 hours. During that time, it was not a crime to disseminate a virus in the Philippines. This meant that Mr Guzman could not be extradited to the countries which suffered the damages to stand trial. As a result, Mr Guzman could not be prosecuted both in the Philippines and in other countries like the USA.
[116] A state can exercise prescriptive jurisdiction where it creates laws and regulations governing conduct within its borders. Through prescriptive jurisdiction, a state can pass laws that address its unique socio-political and socio-economic systems, including criminal laws, regulations and codes on criminal law. Kate Westmoreland & Gail Kent 'International law enforcement access to user data: A survival guide and call for action' (2018) *Canadian Journal of Law and Technology* 225 at 233.
[117] Adjudicative jurisdiction is where the courts in a state can hear disputes about the application of the law. These disputes are usually heard or adjudicated before a state's judicial court systems and tribunals. For a South African court to exercise adjudicative jurisdiction over a cybercrime, the cybercrime must have been committed in the Republic. With international crimes, our courts have exercised adjudicative jurisdiction even where the crimes were committed outside South Africa by foreign authorities. *National Commissioner of South African Police Service v Southern African Human Rights Litigation Centre & others* 2014 ZACC 30.
[118] Enforcement jurisdiction is the authority of a state's law enforcement officers to enforce the state's laws through compulsory process by executing search warrants or arresting suspects.
[119] All offences can be tried in the Magistrates court with the exception of treason, rape and murder. Section 89 of the Magistrate's Court Act 32 of 1944.

warrants to LEA to exercise their enforcement powers. There are various grounds that the courts may rely on to exercise jurisdiction over cybercrimes. Section 24 of the Cybercrimes Act sets out these jurisdictional grounds. Some of the jurisdictional grounds are similarly worded in different criminal statutes. First, in terms of the Cybercrimes Act, a South African court can exercise jurisdiction if the accused was arrested in the territory of South Africa, on board a vessel, a ship, an off-shore installation or fixed platform, or an aircraft registered or required to be registered in South Africa.[120] A similar provision is contained in the CPA which permits a magistrate to issue an arrest warrant where the offence was committed within the area of jurisdiction of such magistrate.[121] Chapter 5 of the CPA empowers LEA to exercise their enforcement powers to arrest a person suspected of committing a crime, with a warrant or without a warrant depending on the circumstances.

Secondly, South African courts can exercise jurisdiction if the person to be charged is a South African citizen, is a company incorporated under the laws of South Africa or any body of persons, corporate or unincorporated, in South Africa.[122] This is also known as the nationality jurisdiction.[123] Thirdly, where a cybercrime was committed in the territory of South Africa or on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in South Africa at the time that the offence was committed, South African courts can exercise jurisdiction.[124] Similar provisions can be found under the ECT Act. Section 90 of the ECT Act provides that a court in South Africa trying an offence under the Act has jurisdiction where the offence was committed in South Africa[125] or on board any ship or aircraft registered in South Africa or on voyage or flight to or from South Africa at the time the offence was committed.[126] Where the criminal matter is brought before a Magistrate's court, the offence must have been committed within the distance of four kilometres beyond the boundary of the district or of the regional division.[127]

The fourth ground that courts can rely on to exercise jurisdiction is if the preparatory actions necessary to commit any offence took place in South Africa or on board a vessel, a ship, an off-shore installation or fixed platform, or an aircraft registered or required to be registered in South Africa at the time when the act, action or part of the offence took place.[128] The ECT Act contains a similar provision

[120] Section 24 (1) (a) of the Cybercrimes Act 19 of 2020.
[121] Section 43 (1) (b) of the Criminal Procedure Act 51 of 1977.
[122] Section 24 (1) (b) of the Cybercrimes Act. Section 90 (c) of the ECT Act provides that the court has jurisdiction if the offence was committed by a South African citizen or a permanent resident or person carrying out business in South Africa.
[123] Christopher L Blakesley and Dan Stigall 'Wings for talons: The case for the extraterritorial jurisdiction over sexual exploitation of children through cyberspace' (2004) *Wayne Law Review* 109 at 120.
[124] Section 24 (1) (c) of the Cybercrimes Act.
[125] Section 90 (a) of the Electronic Communications and Transactions Act 25 of 2002.
[126] Section 90 (d) of the ECT Act.
[127] Section 90 (2) of the Magistrate's Court Act.
[128] Section 24 (1) (d) of the Cybercrimes Act.

that jurisdiction of the court is established if any act of preparation towards the offence or any part of the offence was committed in South Africa.[129]

LEA also exercise territorial enforcement jurisdiction by conducting searches and seizures of anything found within their jurisdiction. Section 20 of the CPA provides that a state may seize anything which is concerned in or on reasonable grounds believed to be concerned in the commission or suspected commission of any offence whether within the Republic or elsewhere.[130] The state may also seize anything which may afford evidence of the commission or suspected commission of an offence whether in the Republic or elsewhere or which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.[131] Section 28 of the Cybercrimes Act provides that a police official may, in accordance with the provisions of chapter 4 of the Act, search for, access or seize any article, within South Africa. Section 29 of the Cybercrimes Act provides for the exercise of territorial jurisdiction and seem to provide for the exercise of extraterritorial jurisdiction by LEA as well.[132] Section 82 of the ECT Act provides a cyber inspector with the powers to inspect, search and seize any premises or information system.

The fifth ground to exercise jurisdiction if an offence affects any person, a restricted computer system, a public body or any business in South Africa.[133] Here, there is no indication whether the person carrying out these activities has to be in South Africa or not. What is important is that the effects of the crime are experienced in South Africa. South African courts also have jurisdiction over an offence committed outside South Africa against any South African citizen or resident, a restricted computer system in South Africa, against a registered company or body or persons in South Africa or against a government facility of South Africa including an embassy or other diplomatic or consular premises.[134] Section 24 (1) (e) and (f) demonstrate that South African law permits South African courts to exercise adjudicative jurisdiction even in cases where the crime was committed extraterritorially. This study will analyse the challenges of these provisions of the Cybercrimes Act. At this stage, it is important to highlight that in criminal law, states limit the exercise of extraterritorial jurisdiction to cases in which there is a direct and substantial connection between the state exercising jurisdiction and the matters committed within their territories or having an effect within their territories. This extraterritorial jurisdiction also extends to matters affecting nationals of that state, or to acts threatening the security of that state.[135] With traditional crimes such as murder, arson, burglary, rape, and theft, it was very easy

[129] Section 90 (b) of the ECT Act.
[130] Section 20 (a) of the CPA.
[131] Section 20 (b) and (c) of the CPA.
[132] Reference to the different sub-sections of section 29 of the Cybercrimes Act shall be discussed further in this study.
[133] Section 24 (1) (e) of the Cybercrimes Act.
[134] Section 24 (1) (f) of the Cybercrimes Act.
[135] John Dugard *International Law: A South African Perspective* 2 ed (2003) at 135.

to determine the state that had jurisdiction over the crime. This usually entailed identifying the location or scene of the crime, which usually fell within clearly defined geographical borders of a state. Even when it came to the gathering of evidence of the crime, the evidence was usually found in an identifiable geographical territory. Territory was thus used as the determining factor to decide whether a state could exercise jurisdiction or not.

Territoriality constitutes one of the cornerstones of the international legal order, the '*pilier d'assises du droit pénal international*'.[136] It has been argued that 'relying on the internet is dubious as it prevents states from effectively investigating and prosecuting cybercrimes'.[137] This study focuses on the legal challenges faced by LEA when seeking access to evidence stored by means of cloud computing services on foreign based data centres. Scholars have correctly cautioned that failure to address jurisdictional challenges come at a high cost, not only for individuals but for juristic persons and governments alike. Without addressing jurisdictional issues in the cloud, we are left with legal uncertainty and in a lacuna in our legal framework. Human rights such as freedom of expression, right to receive and impart information and the freedom of association and right to privacy are all restricted if there is no legal certainty on jurisdiction in the cloud. Such uncertainty also leads to loss of some key cross border benefits of the internet. Without clarity on jurisdiction, there is an inability to address online abuses and cybercrimes which may potentially result in an increase of online abuses. At the same time, uncertainty also means that it is costly for businesses to rely on cloud services if they are not able to know which states may have jurisdiction over their activities. In sum, a failure to properly address jurisdiction in the cloud will result in losses for all stakeholders.[138]

Addressing cybercrime is nearly impossible without dealing with jurisdictional issues, particularly cross border searches and seizures. Jurisdictional challenges emerge when dealing with criminal elements that are taking place in cyberspace, the internet or online digital environment. Questions have been posed on whether a state is able to exercise enforcement jurisdiction in conducting criminal investigations taking place in cyberspace. Enforcement jurisdiction is usually bound by a state's territory. In the absence of any special circumstances or express permission, a state cannot enforce its laws in another state's territory.[139] Through globalisation and international trade, states are increasingly exercising extraterritorial jurisdiction. As discussed above, the cloud environment may present challenges for LEA who may be seeking for electronic evidence. Due to limitations on enforcement jurisdiction, there is no clarity for LEA on whether they have the authority to seize, or access evidence held in remote cloud servers. The default position is usually that where data are hosted

[136] Maillart Jean Baptiste 'The limits of subjective territorial jurisdiction in the context of cybercrime' (2019) 19 *ERA Forum* 375 at 376.
[137] Ibid.
[138] Svantesson op cit note 104 at 40.
[139] Westmoreland & Kent op cit note 116 at 233.

on foreign servers, LEA may not be permitted to access the data. Incidentally, service providers may not be willing to disclose data due to conflict of laws. Questions relating to which state has jurisdiction over data stored in the cloud are relevant and necessary when investigating crime and gathering electronic evidence.

The objective of this research study is to conduct an in-depth analysis of the jurisdictional challenges that cloud data presents to cybercrime investigations. Such an analysis involves asking pertinent questions around the territoriality or extra territoriality of data. The understanding being that when cloud data are classified as extraterritorial, there is need to follow principles of international law to access such cloud data for criminal investigation purposes. The succeeding section discusses these research questions in detail.

III. RESEARCH METHODOLOGY

To address the identified research problems and answer the research questions, the study relies on two types of research methodologies, namely desktop research and comparative legal research.

a. Desktop research

The study analysed the existing literature on cybercrime investigations, procedural aspects when gathering electronic evidence, cloud computing and the territorial jurisdictional challenges presented by cloud computing and the legislative framework on cybercrimes. For an informed, engaging, and balanced debate, the study considered academic writings found in books, journal articles, position papers, policy frameworks, conference presentations and legal opinions found in different online publications. The study also analysed various pieces of legislation, regulations, and policies within the South African context.[140]

b. Comparative legal research[141]

A discussion on cloud computing or cybercrime is global in nature. The dynamic nature of the legal issues justified a comparative study. The comparative analysis considered how the international community is responding to the topical issues raised. This involved considering the relevant treaties

[140] This type of research is doctrinal research or black letter law approach which 'relies extensively on using court judgements to explain law', relies on legal text, court case law, legislative acts and internet-based sources. Mike McConville and Wing Hong Chui *Research Methods for Law* 2ed (2017) 1 at 4.

[141] International and comparative legal research is very important due to the 'increasing influence of international and supra-national legal materials, and the increasing need for legal scholars to refer to materials from a variety of jurisdictions. Ibid at 7.

and conventions such as the Budapest Convention[142] and the Malabo Convention.[143] Broadly, the work by the Council of Europe is important in shaping the future of cybercrime investigations, gathering of evidence, data jurisdiction and data protection.

The study also considered how other countries responded to the issue of unilateral cross border access to data. The relevance of this comparative study is that the domestic laws of the considered country studies have an international law-making effect. For instance, court judgements in Europe have shaped global laws around data jurisdiction. Countries such as the US have promulgated laws like the CLOUD Act which also have the effect of international rulemaking.

IV. WHAT ARE THE RESEARCH QUESTIONS AND OBJECTIVES?

It is important to clarify that the study notes the importance of a discussion around cross border jurisdiction in different aspects from domains, intellectual property, and the digital economy. However, due to limitation in space, this study will not discuss these interesting focus areas. The study discusses cross-cutting issues in public international law and private international law. To limit the scope, the study will only discuss the relevant principles where context requires. This is because some areas are subject to public international law and some to private international law. The study focuses on personal data, content data, communications data, subscriber information, metadata which may be relevant for evidential purposes. It doesn't focus on any other data as broadly defined.

The objectives of this research study are to identify and address the jurisdictional challenges that cloud computing presents particularly during investigation of cybercrimes. It focuses on transborder access to cloud data which contains evidence relevant to the investigation of cybercrimes. It is important to note that the principles discussed also apply *mutatis mutandis* to gathering of evidence for traditional crimes. The discussion considers South Africa's statutory requirements on enforcement jurisdiction as well as international precepts. The study notes that there are barely any academic discussions on cross border data access within the South African context.[144] Bearing in mind the potential human rights violations associated with crime investigations, the research also discusses human rights protections during cross border access to electronic evidence.

---

[142] The Budapest Convention plays an important role in shaping cybercrime laws, promoting international efforts to curb cybercrimes as well as its efforts to address the problem of cross border access to electronic evidence. Council of Europe Convention on Cybercrime (ETS No. 185). South Africa signed the Budapest Convention on 23 November 2001. As of 10 April 2023, South Africa had neither ratified nor acceded to the Budapest Convention. There are currently 68 ratifications or accessions by states. African countries which have ratified or signed the Convention include Cabo Verde, Ghana, Morocco, Nigeria, and Senegal. Available at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185, accessed on 10 April 2023.

[143] African Union Convention on Cyber Security and Data Protection 2014. Adopted by the 23rd ordinary session of the assembly held in Malabo, Equatorial Guinea on 27 June 2014 (the Malabo Convention).

[144] The gap is not only with South Africa. Abraha also notes the lack of academic and policy discourse addressing the challenge in the African context. Halefom op cit note 22 at 29.

A discussion on jurisdiction paradigmatically focuses on territorial sovereignty. This research discusses the role of cloud computing technologies in developing jurisdictional principles applicable to cloud data. Governments, cloud service providers, businesses and academic scholars have developed diverging views on data and jurisdiction. Koops and Goodwin for instance, emphasised that any enforcement action beyond the exercise of the territorial principle requires the express consent of affected states.[145] This is because when LEA access evidence in another state that amounts to violation of the other state's sovereignty. On the contrary, Svantesson considers such an interpretation as overzealous and out of line.[146] This research embarks on a mammoth task of discussing whether jurisdictional principles should be reconceptualised, and is some cases re-examined particularly when dealing with conduct in cyberspace. It addresses the question whether the time has come to formulate or revise jurisdictional principles which should regulate cloud computing and the gathering of electronic evidence stored in the cloud. To achieve the research objectives, the study seeks to address the following research questions:

Research question 1

What jurisdictional challenges do cloud computing services present during cybercrime investigations?

Research question 2

How should states determine jurisdictional principles applicable to remote cloud data?

Research question 3

Do criminal laws in South Africa adequately address cloud jurisdictional challenges?

To address these three main research questions involves unpacking the problems of cloud computing technologies and asking further pertinent questions around which state has jurisdiction to access remote cross border data, whether unilateral access to remote cloud data amounts to the exercise of extraterritorial jurisdiction and how jurisdiction should be determined in cases of encrypted data and data held on the dark web. The proceeding section explains these problems in detail.

a. Which state has jurisdiction to access electronic evidence stored in the cloud?

The rules governing cross-border access to data are a topic of significant, ongoing importance for those involved in cybercrime investigations, forensic investigations, technology companies,

[145] Bert-Jaap Koops & Morag Goodwin '*Cyberspace, the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law (*Tilburg Law School Legal Studies Research Paper Series, Issue 5, 2014) 1 at 24.

[146] Svantesson op cit note 104 at 109.

privacy advocacy groups and governments in general.[147] Cloud computing services create multiple jurisdictions applicable to both the cloud service user and the cloud service provider.[148] This raises a lot of jurisdictional questions which may have a potential impact on how cybercrimes are investigated. When data are hosted on servers in multiple countries, South African law is not clear whether each state where the servers are located can exercise jurisdiction. The law is also not clear over whether the place where the owner of the data is located will have primary jurisdiction over the foreign based data. Due to the nature of cloud services, cloud data may be accessible from potentially any location in the world. This feature of cloud data raises the question of whether a state which can access the data remotely can exercise enforcement jurisdiction over the foreign based cloud data.

Most cloud service providers play a central role during crime investigations and gathering of evidence. Cloud providers are usually in control of data and exercise the discretion of where cloud data should be hosted. In most cases, service providers provide LEA with assistance in obtaining access to sought after cloud evidence. Most cloud service providers operating in South Africa like Google[149], IBM[150], Amazon[151], and Microsoft[152] are foreign-owned entities. This means that foreign states have jurisdiction over these cloud service providers and potentially may exercise jurisdiction over the data they host. Some of the cloud service providers may not have any registered offices in the state which is investigating the crime and seeking cloud evidence. The investigating state may find it challenging to exercise enforcement jurisdiction over such foreign based entities. Interesting questions which may arise are whether the place where the cloud service provider is established have jurisdiction or whether the state where the cloud servers are hosted have jurisdiction over the cloud data?

When a criminal has committed a cybercrime anonymously, the investigation of the cybercrime may start off with locating the computer or computer network system used by the perpetrator or suspect. The purposes of this step are two-fold. First, the location of a computer narrows down the search to identify the perpetrator. Second, the location of the computer also provides clarity on which state has jurisdiction over the sought-after evidence. This step is quite critical in discovering the perpetrator's identity and collecting evidence to build a successful prosecution.[153] Ideally, before accessing evidence stored in the cloud, LEA should establish whether they have jurisdiction over the cloud data or they should apply for permission from a foreign government. In cases where LEA already

[147] Jennifer Daskal 'Privacy and security across borders' (2018-2019) 128 *Yale Law Journal Forum* 1029 at 1030.
[148] Jatinder Singh, Jean Bacon, Jon Crowcroft, Anil Madhavapeddy, Thomas Pasquier, W Kuan Hon & Christopher Millard *Regional Clouds: Technical Considerations* (2014).
[149] Available at *https://about.google/, accessed* on 28 June 2021.
[150] Available at *https://www.ibm.com/za-en?lnk=m, accessed* on 28 June 2021.
[151] Available at *https://www.amazon.com/, accessed* on 28 June 2021.
[152] Available at *https://www.microsoft.com/en-za, accessed* on 28 June 2021.
[153] Ahmed Ghappour 'Searching places unknown: Law enforcement jurisdiction on the dark web' (2017) 69 *Stanford Law Review* 1075 at 1090 – 1091.

know the identity of the suspect, they may overlook taking into consideration the likelihood that the sought-after data may be outside their jurisdiction.

As will be demonstrated in this study, establishing jurisdiction over cybercrimes is a complex task as jurisdiction is usually bound by a state's territory. Cloud computing compounds the problem of jurisdiction due to its unique features. The cloud presents another jurisdictional problem in that bits and bytes of the evidence may be scattered in different clouds hosted in different parts of the world. This makes it extremely difficult for LEA to obtain authorisation from all the states that have territorial jurisdiction based on data location. When a state fails to properly define or criminalise certain conduct as crime and fails to appropriately address jurisdictional issues arising from cloud computing, cybercriminals go unpunished.[154] Cloud data is not generally stable and often moves between servers, locations, and jurisdictions. On the other hand, LEA's powers are territorially defined, and this can be a challenge during cybercrime investigations. On an overall scale, the implications of data's intangibility may potentially challenge traditional international law on jurisdiction[155] as governments may be tempted to unilaterally access cross border cloud data.

b. Is unilateral access to remote cloud data an exercise of extraterritorial enforcement jurisdiction?

The unique features of cloud services and cloud data is the ability for LEA to access such evidence instantaneously. Law enforcement agents can either unilaterally access sought after data (direct access) or obtain the evidence with the assistance of service providers (indirect access).[156] What is concerning is that due to the ease with which LEA can access evidence, LEA may be lured to exceed the bounds of a search[157] or forego the process of obtaining a search warrant. The question which typically arise is whether this amounts to the exercise of territorial jurisdiction or extraterritorial jurisdiction. If the answer to this question is that LEA exercise extraterritorial jurisdiction, ideally, they would need to cooperate with relevant foreign governments to obtain the evidence. Typical processes include the mutual legal assistance treaty (MLATs) channels, data sharing agreements or assistance from internet service providers (ISPs).

To comply with international law, LEA must follow these internationally recognised procedures and respect the sovereignty of other states. Sovereignty is a fundamental principle of international law and refers to the collection of rights held by a state. A sovereign state is entitled to

[154] Chapter 13 of the ECT Act has been criticised for its failure to appropriately criminalise different forms of cybercrime. Crimes such as website defacement, non-consensual pornography, phishing and attacks on critical digital infrastructures are not criminalised by the ECT Act.
[155] Kristen E. Eichensehr 'Data extraterritoriality' (2017) 95 *Texas Law Review* 145 at 145.
[156] Jennifer Daskal 'Transnational government hacking' (2020) *Journal of National Security Law and Policy* 677 at 678.
[157] Musoni Melody 'Is cyber search and seizure under the Cybercrimes and Cybersecurity Bill consistent with the Protection of Personal Information Act?' (2016) 3 *Obiter Law Journal* 683 at 685.

exercise control over its territory and to represent that territory and its people.[158] The UN Charter[159] also prohibits the United Nations to intervene in matters which are within the domestic jurisdiction of any state. To access evidence stored in the cloud hosted on foreign territory without the authorisation of the relevant authorities in that foreign state constitutes a breach of the territorial integrity of that state and thus a wrongful act.[160] Regional legal frameworks should also reflect these international law principles. One of the concerns raised against the Malabo Convention is its lack of explicit reference to international law and failure to explicitly outline the minimum threshold that national constitutions, legal frameworks, and laws should meet and comply with.[161]

Apart from direct access, LEA can infringe the sovereignty of another state through directly approaching cloud service providers and ISPs and requesting for assistance. While there is debate around the application of the extraterritoriality principle to cloud data, consensus has been reached on jurisdiction over publicly available cloud data. It is argued that if publicly available data can be accessed from a territory, that territory exercises territorial as opposed to extraterritorial enforcement jurisdiction.[162] As will be discussed in this study,[163] arguments have also been presented that states can unilaterally access content hidden on the dark web as well as data which are meant to be accessible from a particular location. There has been criticism on this position as there is no clarity on the meaning of 'meant to be accessible' standard. Eichensehr noted that this standard can be interpreted in different ways which may result in different conflicting outcomes.[164]

[158] Gary P Corn and Robert Taylor 'Sovereignty in the age of cyber' (2017 – 2018) 111 *AJIL – Unbound* 207 at 209.

[159] 'Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII' Article 2 (7) Charter of the United Nations of 26 June 1945.

[160] The case of *USA v Gorshkov* is an example of the violation of state sovereignty by law enforcement. The FBI invited two Russian hackers, Vasiliy and Alexey Ivanov for an interview in Washington DC. The Russians had no knowledge that the company interviewing them was a bogus FBI operation. To assess their skills and capabilities, the Russians were asked to demonstrate their skills by hacking a network set up by the FBI. The FBI had installed a keystroke logger program on each laptop which recorded the usernames and passwords of Gorshkov and Ivanov and managed to download files that were on computers located in Russia. The Russians were subsequently prosecuted in the US. *USA v Gorshkov 2001 WL 1024025*. Russia did not take the news about the conviction of its citizens lightly. It opened its own criminal case against the FBI agents who were responsible for collecting evidence hosted on Russian soil. Russia argued that the FBI had violated the principle of state sovereignty and committed a crime of hacking in Russia. The USA did not comply with this extradition request.

[161] Instead, the Malabo Convention overemphasises the ACHPR despite the ACHPR not having an explicit right to privacy in relation to access to information and processing of personal data. The African Union Convention on Cybersecurity and Personal Data Protection' (2014) The Zimbabwean, Southampton 21 July 2014.

[162] Eichensehr opcit note 156 at 148.

[163] Chapter 4 of this study.

[164] Who determines the access, the account holder or the cloud service provider? Eichensehr opcit note 156 at 152 – 153.

c. *Who should exercise jurisdiction over encrypted data?*

The internet can be anonymous. This means that people can transact without having to reveal their true identities or make use of their real names. Cloud computing technologies compounds this problem of anonymity by having in place tools which allow for data to be encrypted. Encryption of cloud data presents an additional jurisdictional problem to the compounded problem of establishing jurisdiction over cloud data. Encryption techniques involves the use of mathematical algorithm which converts data from its original form into an indecipherable or scrambled form. When data are encrypted, it becomes challenging for LEA to ascertain whether they have jurisdiction over the data or not. Without knowing the location of the cloud data due to encryption techniques, LEA may not be able to exercise enforcement jurisdiction. Ordinarily, LEA under the authority of a search warrant, can break locks to any premises identified in the search warrant. In the context of cyberspace, the analogy to breaking locks is the use of encryption and decryption keys. However, breaking into computer systems is not that straightforward. Numerous anonymising services and techniques are available on the internet. When communications are anonymised using these techniques, LEA find it difficult to rely on IP addresses to track down suspects.[165] Criminals can disguise the originating IP address by sending network traffic through an intermediary computer. For example, use of Virtual Private Network (VPN) services re-routes internet traffic through an intermediary server and the originating IP address of an internet user is changed.[166]

Cloud computing enables people to log in to a web portal and make use of electronic communication services and online storage services.[167] When data are encrypted, LEA are not able to interpret the data without decryption keys. The other challenge with encrypted data is that even where the service providers have been requested to provide data, they are not always able to unencrypt the data if the cloud user has also encrypted the data. In instances where the sought after data are personal data, encryption may mean that the data ceases to be 'personal data' and may be processed free of data protection law requirements.[168] A warrant for search of evidence stored in the cloud cannot be valid when the issuing judge does not know whether it would be executed within or outside its state.[169] The anonymity of the suspect compiled with the cloud's unknown location creates a chicken and egg conundrum.[170] Where a suspect is not known, a judge cannot determine whether the warrant will be a

[165] Oerlemans Jan-Jaap *Investigating Cybercrime* (unpublished PhD thesis, Leiden University 2017) at 38.
[166] Ibid at 39.
[167] Ibid at 51.
[168] Hon and others had argued that strongly encrypted and secured data should not be considered as personal data. W Kuan Hon, Christopher Millard and Ian Walden 'The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing' (2011) *International Data Privacy Law* 211 at 213 and 228.
[169] Section 90 of the ECT Act provides that a court in the Republic trying an offence in terms of this Act (this include cybercrimes) has jurisdiction where the offence was committed in the Republic.
[170] Diana Benton 'Seeking warrants for unknown locations: The mismatch between digital pegs and territorial holes' (2018) 68 *Emory Law Journal* 183 at 193.

valid exercise of jurisdiction until the warrant has already been executed.[171] In countries like the United States of America, law enforcement agencies have jurisdiction over evidence if its location has been concealed by technological means. The US Federal Rule of Criminal Procedure 41 specifies that a Judge can issue a remote access search warrant if the location of the device or data is unknown, or if the location has been concealed via technological means. The challenge for LEA in accessing data on unknown locations is that it could lead them to inadvertently search and access data and devices on foreign territory. This risks the investigating state to violate the rule of sovereignty and the principle of comity. Coincidentally, there are dangers that the investigators involved may end up being subject to criminal prosecution under the domestic laws of the country in which the data are located.[172]

d. How should law enforcement agents lawfully search and seize cloud evidence belonging to an anonymous suspect?

The dark web presents a problem that is pertinent not only to cloud services but to all cybercrime investigations. The dark web is a private global computer network that enables users to conduct anonymous transactions without revealing their location (IP address) or identity.[173] Criminal actors increasingly rely on the dark web to mask their identities and commit crime. The famous Silk Road[174] is an example of a dark web marketplace. Mr Ross Ulbricht had been running the Silk Road for almost three years. LEA could not identify him despite them having infiltrated the marketplace. Unmasking the true identities of cybercriminals is a mammoth task for LEA. To re-iterate, the use of technologies which reroutes the IP address of a perpetrator results in LEA being unable to identify the perpetrator, the location of the perpetrator and the location of the sought-after evidence. The most common technology used on the dark web is The Onion Router (ToR).[175] ToR is common for its anonymity.[176] ToR provides a platform for users to interact and conduct transactions without knowing each other's network identity. Dark web users don't know the persons offering the site, while the site administrators also don't know who is posting to it.[177]

Without knowing the identity of a criminal, LEA are left in an unfavourable position. They are not able to determine whether they have the authority to assert jurisdiction over the anonymous criminal or whether they can lawfully conduct a search to seize any electronic evidence of the crime.

---

[171] Ibid at 193.
[172] Daskal op cit note 156 at 677.
[173] Ghappour op cit note 154 at 1086.
[174] Available at *https://en.wikipedia.org/wiki/Silk_Road_(marketplace), accessed* on 22 June 2019.
[175] The ToR system distributes a transaction over several places on the internet, so that no single point can link a person to their destination. The ToR system masks the identity of a user. Trautman op cit note 110 at 16.
[176] ToR was developed by the Naval Research Laboratory as a measure to protect the anonymity of the US government. Wayne Dalton, Joey Jansen van Vuuren and Justin Westcott 'Building cybersecurity resilience in Africa' (2017) *12th International Conference on Cyber Warfare and Security* 112 at 114. Brett van Nierkerk 'The cybersecurity dilemma: Considerations for investigations in the dark web' (2018) 13 *Acta Criminologica: Southern African Journal of Criminology* 132 at 136.
[177] Trautman op cit note 110 at 19.

Unmasking the true identities of cyber criminals is a stupendous task which calls for the utilisation of services from skilled technical experts who are already scarcely available. With most law enforcement agencies lacking in the skillset to investigate cybercrimes, most of the crimes committed will likely go unpunished and unsolved. To unmask the offender, LEA may need to hack into the offender's computers. Hacking is a form of search which requires a warrant and in the absence of such a warrant, any evidence collected cannot be used in a court of law.[178]

Under the current South African legal framework, network investigative techniques[179] (law enforcement agents hacking) are not clearly explained under the ECT Act. However, the Cybercrimes Act[180] allows for the removal of a computer data storage medium or any part of a computer system and rendering inaccessible data, a computer program, a computer data storage medium or any part of a computer system to preserve evidence.[181] Hacking is only permissible where the data are located in South Africa and not in instances where the data are situated in a cloud server in a foreign country.[182] If a court issues a warrant to search a computer at an unknown location, then the warrant may be void *ab initio* if the search reveals that the computer is physically beyond the court's jurisdiction.[183] Ghappour identified the risks involved in investigating crime on the dark web which includes the risk of attribution, vulnerability disclosure, diplomatic risks associated with unauthorised cross border operations as well as the risk of countermeasures the injured state may be entitled to take.[184]

V. WHAT IS THE HYPOTHESIS?

Jurisdictional principles applicable to cybercrime investigations must be evaluated to align with the challenges of remote cross border searches for electronic evidence. The principles of territoriality and state sovereignty are currently based on the geographical location of '*where*' the crime was committed and '*where*' the criminal is located. However, the investigation of cybercrimes questions these principles. Cybercrimes are committed not in a physical pinpointed location on a map but in

[178] Benton op cit note 171 at 186.
[179] Network investigative techniques involves access and extraction of evidence. Ghappour op cit note 151 at 1096.
[180] The Cybercrimes Act 19 of 2020.
[181] Section 32 (1) Cybercrimes Act.
[182] A police official may without a search warrant referred to in section 29 (1) (a) search any person, container, premises, vehicle, facility, ship or aircraft for the purposes pf performing the powers referred to in paragraphs (a) and (b) of the definition of "seize" in respect of a computer data storage medium or any part of a computer system referred to in the definition of "article", if the police official on reasonable grounds believes –

(a) That a search warrant will be issued to him or her under section 29 (1) (a) if he or she applies for such warrant; and
(b) That the delay in obtaining such warrant would defeat the object of the search and seizure.

Section 32 of the Cybercrimes Act.
[183] Benton op cit note 171 at 187.
[184] Ghappour op cit note 154 at 1108. Adopting the arguments submitted by Ghappour, chapter 4 of this study discusses how South Africa addresses the problematic challenge of anonymity on the deep dark web when investigating crime.

cyberspace. The ubiquitous nature of the internet and cloud computing services underscores the material differences between crimes committed in cyberspace and crimes committed in the physical world. Crime has evolved because of technological innovations. This warrants the development of new set of rules to govern cybercrimes. It has been argued that 'it is legally possible to extend jurisdictional principles such as the territorial sovereignty as such a principle was never sacrosanct but rather it's an evolving concept'.[185]

Post correctly noted that due to the volumes of information that the internet can instantaneously process, our laws need to be revised to catch up with the internet scale up.[186] During the embryonic stages of the internet, Brenner had argued that instead of creating distinct laws on cybercrime, lawmakers should apply the existing principles to define crimes that are considered as cybercrimes.[187] This study suggests that a new set of laws should be introduced which addresses criminal conduct in cyberspace and new principles on jurisdiction should be formulated when addressing conduct in cyberspace. Cloud computing techniques such as sharding and partitioning allow for data to be stored as fragments across a range of machines[188] which means that pieces of evidence may be in different countries simultaneously. To apply the same jurisdictional principles to crimes committed in cyberspace is limiting. The result of that application is that criminals would go unpunished due to the state failing to establish jurisdiction over the crimes committed.

This study commends the South African government for promulgating the Cybercrimes Act which is the principal law on cybercrime. However, the study argues that the Cybercrimes Act is not clear on whether enforcement powers can be exercised in instances were sought after electronic evidence is on data servers in another country. When applying the Cybercrimes Act to international law, it is apparent that there is jurisdictional loopholes exist. . Without addressing these shortcomings, criminals will slip through the jurisdictional loopholes and go unprosecuted. Without adequate jurisdictional principles to govern conduct in cyberspace and clarity on jurisdiction of data in the cloud, the powers of LEA would be increasingly significantly limited.

VI. LIMITATIONS OF THE RESEARCH

The study glosses over procedural and substantive issues regarding cybercrime investigations and international cooperation. These procedural and substantive issues are quite significant and merit careful analysis and study. This is outside the scope of this research. When LEA access electronic evidence, there are risks that the integrity of such evidence may be tampered with, the data may be mishandled, altered, misappropriated, or destroyed. While the study discusses the legal challenges for

[185] Jack Goldsmith 'The Internet and the Legitimacy of Remote Cross Border Searches' (2001) *Chicago Public Law and Legal Theory Working Paper* 1 at 6.
[186] Post op cit note 66 at 22.
[187] Brenner op cit note 69 at para 113.
[188] Walden op cit note 101.

LEA in accessing remote cloud data, it will not discuss risks around the electronic evidence itself. There are studies on preservation of the integrity of electronic evidence during searches and seizures and this is outside the scope of this study.[189]

VII. STRUCTURE OF THE RESEARCH

a. Chapter 1 Introduction

Chapter 1 of the study maps out the contextual background to cybercrimes and cloud computing by discussing the issues around internet regulation. It points out to the reader where the challenges around criminal jurisdiction in cyberspace originated. Importantly, it sets out a general overview of the research objectives of this study.

b. Chapter 2 The legal framework on cloud computing

This chapter introduces the topic of cloud computing law. Cloud computing law is a new area of law in South Africa and globally. Chapter 2 of this study discusses the features of cloud data. This discussion is aimed at drawing the reader to understand the challenges that could potentially arise when LEA seek to access cloud data. To appreciate the argument for reformulation of jurisdictional principles, one needs to delve into the cloud architecture to get clarity on the novelty of cloud data instead of glossing over its features.

The chapter also sets out the legal and policy framework around cloud services in South Africa. It aims to examine how the laws regulating cloud services address jurisdictional challenges posed by cloud computing. To get an understanding of the legal framework on cloud computing, one must look at different pieces of legislation such as the ECT Act, the POPIA and the RICA Act. The recently published draft National Data and Cloud Policy (NDCP) reflects the government's approach to data governance including data jurisdiction. The chapter discusses the regulatory and policy framework to get a comprehensive picture on the legal instruments around cloud computing in South Africa.

Importantly, the chapter discusses how leading cloud service providers deal with police requests for access to data. This discussion is key in highlighting the primary role of private actors in cybercrime investigations. The significance of these objectives is to provide a basis for the

[189] C. Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) *Journal of South African Law* 461. Hennie Lochner Bernadine Benson Juanida Horne 'Making the invisible visible: the presentation of electronic (cell phone) evidence as real evidence in a court of law' (2012) *Acta Criminologica: African Journal of Criminology & Victimology* 69. Lee Swales 'An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: suggestions for reform – part one' (2018) 21 *Potchefstroom Electronic Law Journal* 1. Lee Swales 'An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: suggestions for reform – part two' (2018) 21 *Potchefstroom Electronic Law Journal* 1. Annalise Kempen 'Digital forensic evidence and investigations' (2021) 114 *Servanus Community-based Safety and Security Magazine* 38. Rehema EY Uroki *Damage to data is devastating* (unpublished LLM thesis, University of Tumaini 2013).

development of legal arguments on data jurisdiction (chapter 4) and data localisation (chapter 5). It also highlights the dominance of foreign based entities in South African cloud markets and the concern of foreign governments being potentially able to access such cloud data.

The rationale behind seeking clarity on jurisdiction in the cloud stems from the antithetical legal standpoints in today's literature. Without legal certainty on which state has jurisdiction over cloud data, criminal investigations in the cloud have the potential to violate international law and may potentially infringe on state sovereignty as well as infringing on people's rights to privacy. Despite the increased prevalence of the provision of cloud services, there is surprisingly no certainty on which state has jurisdiction over data stored in the cloud. Some states have exercised jurisdiction over cloud data stored on data servers in foreign states based on the cloud service provider being established in that state. Some courts have established jurisdiction over cloud data based on the location where the data are accessible from.[190] Some scholars have suggested that jurisdiction over cloud data should stem from the nationality of the person to whom the data relates. Conversely, other scholars argue that the nationality of the owner of the data should be the determining factor in establishing jurisdiction as the owner of the data is not always the same as the person to whom the data relates.

c. Chapter 3 Introduction to cybercrime

Chapter 3 outlines one of the research questions which is 'do criminal laws in South Africa adequately address cloud jurisdictional challenges?' To address the research question, the chapter introduces the topic on cybercrimes. It starts off by discussing the opportunities that the internet and technology present in the commission of crime. It then moves to discuss criminal law in South Africa with a focus on cybercrimes. This is done by first defining what cybercrimes are and the types of offences which constitute cybercrimes. Secondly, the chapter examines the legislative framework in South Africa which criminalises cybercrimes.

Until recently, cybercrimes were not regulated by a unified piece of legislation, but different pieces of legislation dealt with various aspects of cybercrime.[191] For example, though the ECT Act criminalises cybercrimes, the procedure to gather electronic evidence of a cybercrime was subject to the Criminal Procedure Act. The exercise of enforcement jurisdiction under the ECT Act was provided for under three scenarios. First, if a crime has been committed within the territorial borders of South Africa.[192] Traditionally, this basis to exercise jurisdiction was easier to prove. Any crime committed

[190] This is the current position in terms of South African law as provided by section 83 (2) (*c*) ECT Act.
[191] Previously, the ECT Act was the primary piece of legislation which criminalised some forms of cybercrimes. However, ECT Act was very limited in scope of the cybercrimes that it criminalises; The Cybercrimes Act is a much more elaborate piece of law which has the potential to criminalise conduct that was not previously criminalised by the ECT Act. Other laws include the Criminal Procedure Act 51 of 1977; the International Cooperation in Criminal Matters Act 75 of 1996, the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, the National Cybersecurity Policy Framework 2015; the Critical Infrastructure Protection Act 8 of 2019 and the Protection of Personal Information Act 4 of 2013.
[192] Section 83 (2) (*a*) ECT Act.

on South African soil or on South African registered ship or aircraft would be investigated by local police. If the evidence of the crime is within the physical borders of South Africa, LEA could search and seize it. LEA would apply for a search warrant which is issued by a magistrate within the same jurisdiction where the crime occurred. The direct application of section 83 (2) (a) of the ECT Act is difficult to prove in case of cybercrime. Where unlawful conduct has been committed over the internet or in cyberspace, it is not clear whether a certain physical territory or 'place' can exercise territorial jurisdiction.

The question becomes how does one determine whether the cybercrime was committed within the territory of a state? Does one consider the networks used to commit the offence? If the cybercriminal uses local networks to commit a crime, the state can potentially argue that the crime was committed within its territory. Similar questions can be posed when it comes to gathering of evidence. This is the focal point of this study. LEA also have the power to investigate a crime and gather evidence if a state has personal jurisdiction over the persons involved. A citizen, resident or company carrying business in South Africa is subject to South Africa's criminal laws.[193] This may allow the LEA to gather evidence pertaining to the crime committed. As will be discussed in chapter 4 of this study, LEA may not be able to act unilaterally to access remotely based cloud evidence.

The other ground to establish jurisdiction is where the information pertinent to the investigation is accessible from within the area of jurisdiction of the court.[194] This means that if electronic evidence which can prove the commission of a crime can be accessed from South Africa, a South African court can issue a search warrant authorising a LEA or cyber inspector to search for such electronic evidence. This implies that where a person has documents or data stored on a cloud server hosted in a foreign state, South African courts can still exercise jurisdiction over that data. The extent of LEA's exercise of enforcement jurisdiction is also questionable in terms of international law.[195]

Before the promulgation of the Cybercrimes Act, cybercriminals understood that they could engage in certain unlawful conduct without being criminalised. The inadequacy of cybercrime laws in South Africa has been a concern for cybercrime scholars for decades.[196] With the enactment of the Cybercrimes Act, this study examines the adequacy of this piece of legislation in combatting cybercrime.

As part of the research methodology, the study conducts a comparative analysis between the legal framework in South Africa and mechanisms under the COE Budapest Convention and the AU

[193] Section 83 (2) (*b*) ECT Act.
[194] Section 83 (2) (*c*) ECT Act.
[195] The exercise of extraterritorial jurisdiction over cloud data is further unpacked in detail in under chapter 4 of this study.
[196] Fawzia Cassim 'Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study' (2009) 12 *Potchefstroom Electronic Law Journal* 36.

Malabo Convention, with an interest on jurisdiction over cloud evidence. Cybercrimes are global in nature and the investigation and prosecution of cybercrimes requires the existence and effective action of multiple regulators. Non-regulation of cybercrimes in other jurisdictions increases this global menace and it is expected of all countries to make concerted efforts in regulating cybercrimes through national laws and international cooperation.

d. Chapter 4 Jurisdictional challenges of cloud services

Chapter 4 of the study discusses the research questions in detail. It critically examines the challenges in gathering evidence stored in the cloud. This spans from challenges in establishing jurisdiction of the data in the cloud, establishing jurisdiction where data are in transit, establishing jurisdiction where the offender is anonymous as well as the challenge where cybercriminals operate from the dark web. There is wealth of jurisprudence on jurisdiction in relation to international crimes as well as jurisdiction in cybercrimes. One of the distinguished and leading scholars on cybercrime law has produced work which provides a foundational background on understanding jurisdictional principles applicable to cybercrimes.[197] Drawing on scholarly opinions on cybercrime jurisdiction, one could note that scholars did not challenge the principles of jurisdiction and advance the argument for a reconceptualisation of these principles. Such an argument stems from the shortcomings and inadequacies that current principles of jurisdiction pose on crimes committed in cyberspace.

The chapter goes in-depth to discuss the leading debate between two competing viewpoints. One camp argues that data are territorial and principles on territorial jurisdiction apply to data. This study refers to the supporters of this viewpoint as data territorialists. The other camp argues that data are exceptional, and territory should not be used as a determining factor to exercise jurisdiction over cloud data. This viewpoint is elaborated by data exceptionalists or non-territorialists. These debates on jurisdiction in cyberspace correctly criticise territoriality as a form of jurisdiction.[198] The purpose of this discussion is to provide the reader with different perspectives shaping data jurisdiction principles. Importantly, the discussion is aimed at exploring if data or cloud are unique to warrant the changes on jurisdictional principles.

Chapter 4 is the core of this study. It investigates the relationship between territory and jurisdiction. It explains why territory remains as the primary basis to establish jurisdiction even in cyber environments. Maillart correctly argued the limitations of subjective territoriality over cybercrimes in that it is difficult to pinpoint the actual physical location where the cybercrime was

[197] Jonathan Clough *Principles of Cybercrime* 2 ed (2015).

[198] There are two types of territoriality jurisdiction – subjective territoriality and objective territoriality. Subjective territoriality is where the crime is commenced within a foreign state and completed within a country's territory. Dugard op cit note 133 at 136-137. Bojana Tubic and Stefan Radojcic 'Jurisdictional problems in international law' (2017) *Romanian Journal of Comparative Law* 200 at 203. Objective territoriality on the other hand gives a state in which the effect or impact of the crime is felt to exercise jurisdiction.

committed.[199] The argument forwarded by Maillart is a building block in developing an argument why traditional territorial jurisdiction should have no application in cyberspace. However, this argument creates the impression that cybercrime is a crime that is committed in a physical place that can be pinpointed on the map. One could note that the debate by Koops and Goodwin on changing the language and metaphors used in describing conduct in cyberspace is of paramount importance in advancing the debate for a reconceptualisation of principles of jurisdiction.[200] In contrast to Maillart's line of argument, they argue that the language used to describe actions in cyberspace points towards an interpretation that most states conceive cyberspace as a physical place rather than a space which is an abstract area.[201]

To expand on this discussion, the chapter explores the Lotus decision on extraterritorial jurisdiction and its application in the digital world. It discusses the question of whether remote searches of data amount to the exercise of extraterritorial jurisdiction or territorial jurisdiction. With the globalisation of cloud services, the chapter explores how the rules and principles of international law apply to cloud data jurisdiction. This discussion involves exploring how different states discern data jurisdiction in terms of domestic law and international conventions.

The discussion around data exceptionalism is also an important part or section of this chapter. The importance of emphasising the novelty of data and the cloud is to advocate for new jurisdictional principles suitable for cyber environments. Applying the traditional jurisdictional principles to matters in cyberspace is not clear cut and there are major differences between territorial jurisdiction as defined by parameters of geographical borders and jurisdiction in the digital environment. The argument presented is that 'physical location can no longer be used as a criterion for conceptualising legal authority'.[202] It is impossible to cram the legal and regulatory problems of the internet into existing pigeonholes developed to handle earlier technologies.[203] What the internet demands are new rules which are better suited for the technological changes. These new rules include focusing on other grounds to establish jurisdiction instead of relying on geographical territory.[204] Other proposals include developing alternative legal account to cyberspace jurisdiction in similar ways that outer space and the high seas are regulated.[205]

e. Chapter 5 The role of data localisation in overcoming jurisdictional challenges.

The recent developments on data sovereignty and the proposed policy interventions by South Africa are timely for this study. In terms of the recent NDCP, South African government wants to own

[199] Baptiste op cit note 137 at 376.
[200] Koops & Goodwin op cit note 146 at 29.
[201] Koops & Goodwin op cit note 146 at 8.
[202] Post op cit note 66 at 22.
[203] Post op cit note 66 at 25.
[204] Benton op cit note 171 at 194.
[205] Koops and Goodwin op cit note 146 at 12.

data produced within South Africa. The policy seeks to address the challenge faced by LEA when trying to access remote cloud data. It proposes a solution of making it compulsory for copies of personal data to be locally stored. This chapter investigates how data localisation measures address the jurisdictional challenges presented by cloud computing services. Chapter 5 discusses the emerging concept of data sovereignty, what it means for data jurisdiction and the measures adopted by different states. Such a discussion is very important in shaping the solutions to the data jurisdiction challenge. Perceptions of states on jurisdiction are important in formulating legal solutions which can correspond with standard practice. Chapter 5 engages in literature and argument on data localisation and evaluate whether South Africa should adopt data localisation laws to persuade cloud service providers to retain data of South African citizens and businesses within South Africa.[206] The study relies on the current legal instruments in identifying the obligations on cloud service providers to assist LEA during cybercrime investigations. Drawing on scholarly views on why cloud services are currently not sufficiently regulated by law, chapter 5 advances the argument for data localisation as a major step in regulating cloud services.

f. *Chapter 6 Recommendations*

After a careful consideration of the jurisdictional aspects of cloud data and cybercrimes, chapter 6 provides recommendations to solve the research problem. The recommendations consider a reformulation of legal principles applicable to data jurisdiction. The recommendations offer practical approaches to address the challenges by considering the prevailing state practice and policy frameworks. One of the notable proposals involves turning to internet infrastructure or code to address the jurisdictional challenge. The solution supports the notion of code as law.

g. *Chapter 7 Conclusion*

Chapter 7 provides the concluding remarks.

[206] In March 2019, Microsoft South Africa launched two cloud data centres in Johannesburg and Cape Town. Available at *https://www.datacenterknowledge.com/microsoft/microsoft-launches-first-cloud-data-centers-south-africa*, accessed on 25 June 2019 Amazon Web Services launched its own data centres in 2020. Available at *https://aws.amazon.com/blogs/aws/now-open-aws-africa-cape-town-region/*, *accessed* on 3 May 2020. At government level, the State Information Technology Agency (SITA) has been mandated to provide cloud computing services to government departments in terms of the State Information Technology Act 88 of 1998.

CHAPTER 2: THE LAW ON CLOUD COMPUTING

I. INTRODUCTION

The UN estimate that by 2025, 49 per cent of data will be stored in the cloud and the quantity of data on a global level will amount to 175 zettabytes.[207] This is an insurmountable amount of data held by cloud service providers who include private companies or governments. Cloud service providers understand that the emerging economy and society is not only data driven but data hungry.[208] For people to use electronic devices effectively and seamlessly, they need to provide a lot of data about themselves. This results in ICTs processing a lot of personal data of users. The shortage of storage on ICT devices presents the cloud as a viable storage solution. Undeniably, when people resort to cloud storage solutions, some of the cloud data may be required by LEA as evidence during criminal investigations.[209] Recently, there has been an increase in the number of requests for electronic evidence in criminal investigations. For example, in 2014 alone, the British government sought customer data for at least 53,947 separate user accounts controlled by US based technology companies.[210] The number of cases where the sought-after data are in other jurisdictions is also becoming prevalent. A study conducted by the UN Office on Drugs and Crimes inter-governmental expert group indicated that a lot of sought-after evidence may be hosted on computer systems in other countries. The study also found that two thirds of responding states view cross border access to computer systems or data to be impermissible and (outside limited exceptional situations) requiring access to formal channels.[211]

Understanding how data in the cloud are stored, processed, or retrieved for criminal investigation purposes is crucial to addressing one of the research questions of this study. To re-iterate, this study explores the jurisdictional challenges presented by cloud computing services during cybercrime investigations. Once the reader has an informed background knowledge of how the cloud operates, it is anticipated that the reader will understand the context within which this study proposes the solutions. This study is not the first to discuss the difficult challenges presented by cloud computing in different areas of law. Previous studies considered some of the legal concerns arising from the use of

[207] United Nations *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development* (2020) 1 at 145.
[208] Microsoft 'A Cloud for Global Good: A policy road map for a trusted, responsible and inclusive cloud' (2018) at 17, last accessed from *https://news.microsoft.com/cloudforgood/* on 28 November 2020.
[209] A report by the European Union stated that electronic evidence in any form is relevant in 85 per cent of total criminal investigations. In almost two thirds (65 per cent) of the investigations where electronic evidence is relevant, a request to service providers based in another jurisdiction is needed. Internet & Jurisdiction Policy Network *Data and Jurisdiction Program: Operational Approaches, Norms, Criteria and Mechanisms* (2019) 1 at 7.
[210] Andrew Keanu Woods 'Against Data Exceptionalism' (2016) 68 *Stanford Law Review* 729 at 743.
[211] Robert J Currie 'Cross border evidence gathering in transitional criminal investigation: Is the Microsoft Ireland case the next frontier?' (2016) 54 *Canadian Yearbook of International Law* 63 at 79.

cloud services relating to intellectual property law[212], data protection and privacy[213], data security[214], competition law, private international law,[215] licensing risks[216], conflict of laws[217], civil law disputes and jurisdiction.[218] This study focuses on the legal jurisdictional challenges presented by the cloud to LEA seeking to access electronic evidence hosted cross border. O'Keeffe correctly pointed out that 'while the question of 'legal jurisdiction' is simple to pose it is in fact very difficult to answer'.[219] This study seeks to answer this question. To fight crime and protect public safety, governments must have a clear and compelling need to access digital evidence. At the same time, citizens have an expectation that due process and the rule of law, including the protection of privacy, will be upheld. When users suspect the infringement of their privacy, they are hesitant to adopt or trust any technology.[220] However, others do not see privacy, security and trust as major threats or obstacles in the adoption of the cloud.[221] It is critical to craft laws which permit LEA to access digital evidence pursuant to lawful process, while ensuring that citizens' fundamental rights and nations' sovereignty interests are protected.[222]

In this chapter, the discussion is on the cloud infrastructure and cloud services. The purpose of this discussion is to expound on the challenges that cloud services pose particularly on the investigation of cybercrime and the collection of electronic evidence in the cloud. An understanding of how the cloud functions makes it easier for the reader to appreciate the challenges relating to cloud computing as well as identify seemingly subtle differences between cloud data and device-stored data. The different features of cloud data justify why addressing the problem of jurisdiction over remote cross border data

[212] There are concerns over ownership of intellectual property developed because of the contract between the cloud customer and cloud provider. There need to be clarity on intellectual property rights in copies of cloud data for example. Sakshi Porwal, Srijith K Nair and Theo Dimitrakos 'Regulatory impact of data protection and privacy in the cloud' in Ian Wakeman et al *Trust Management V* (2011) 290 at 296.
[213] When the cloud is used to store personally identifiable information, that can raise some privacy concerns. J Gebers and J Ophoff 'Exploring cloud computing legal and privacy issues in South Africa' 2013 *15th Annual Conference on World Wide Web Applications*, Cape Town 1 at 5.
[214] S Rajesh, P Shylender Reddy and T Pavan Kumar 'Security threats in cloud computing' (2012) **GJCAT** 1043 – 1049. S Subashini and V Kavitha 'A survey on security issues in service delivery models of cloud computing' (2010) *Journal of Network and Computer Applications* 1.
[215] Allan Paul Jackson *Legal concerns arising from the use of cloud technologies* (*LLD thesis, University of Pretoria, 2017)*.
[216] Daniele Catteddu 'Cloud computing: benefits, risks and recommendations for information security' in Serrao C., Aguilera Diaz V., Cerullo F (eds) *Web Application Security IBWAS 2009 Communications in Computer and Information Science* (2009).
[217] Anthony Gray 'Conflict of laws and the cloud' (2013) 29 *Computer Law & Security Review* 58.
[218] There could be conflict on choice of law and jurisdiction between a cloud user and cloud provider especially if the relevant contracts do not clarify on applicable law and jurisdiction. Gebers and Ophoff op cit note 212 at 7.
[219] Vincent O'Keeffe 'Jurisdictional issues associated with a move to the cloud' 1 at 4.
[220] Hon, Millard and Walden op cit note 166. Ishan Rastogi, Adesh Chandra, Vivek Kumar Gupta and Abhishek Vaish 'Privacy issues and measurement in cloud computing: A review' (2013) *International Journal of Advanced Research in Computer Science* 81.
[221] A.D. Abubakar, Julian M Bass and Ian Allison 'Cloud computing: Adoption issues for sub-saharan African SMEs' (2014) 62 *EJISDC* 1 at 7.
[222] Microsoft op cit note 210 at 38.

is pertinent. The chapter argues that the unique features of cloud computing technologies justify the need for a reformulation of jurisdictional principles around cloud data.

Cloud computing law is a new discipline in South Africa. As such, legal principles specifically developed for the cloud environment are not yet developed. The gap in cloud computing regulation is not only limited to aspects of jurisdiction for criminal purposes (as per this research study) but extends to jurisdiction in other contexts. The current increase in cloud adoption positions this chapter discussion as timely. This chapter analyses different piecemeal legislation and policies in South Africa which regulate, or in certain instances, attempt to regulate cloud computing services. This chapter discussion is aimed at bringing clarity on South Africa's *lex lata* on cloud data jurisdiction. A functional legal framework on cloud computing may be important in providing clarity and clarifies the uncertainty that currently shrouds cloud data and access to cloud data.[223] This chapter argues that South African law does not provide legal certainty on how it regulates cloud computing technologies in the cybercrime context. It submits that cloud data jurisdiction is not definitively addressed in the different statutes and regulations which purport to regulate cloud computing technologies. For instance, it is unclear whether LEA can exercise their powers to conduct searches and seizures over data located on foreign territory.[224] The most limitation in the law relates to the uncertainty over cloud data governance, cloud data residency and cloud data jurisdiction. This uncertainty transcends into negatively impacting criminal procedural processes and investigations.

This chapter argues that there is a lack of legal and policy interoperability around cloud data and regulation of cloud computing. Lack of legal and policy interoperability creates legal uncertainty on different issues including uncertainty on jurisdictional principles applicable to cloud data. Whilst states are mainly involved in promulgating laws, service providers are involved in developing certain policies. Such policies have a strong bearing on cybercrime investigations and data governance. Unterritorialists have correctly noted that multinational companies are at the forefront of making key decisions as to which government's rules apply to data and how such rules are interpreted.[225] This chapter is aimed at discussing the legislative obligations and roles of private players in cybercrime investigations and gathering of cloud data. This preparatory work is particularly important as it informs the discussions of chapter 5 of this study around data localisation and data sovereignty. Cloud service providers play a very central role in either assisting or resisting LEA from accessing sought after cloud data. This chapter examines best practice adopted by cloud service providers when dealing with requests from LEA. This involves a review of terms of service for some of the global cloud service providers operating in South Africa. While most of the terms of service explain the role of the service provider in

[223] Microsoft op cit note 210 at 38.
[224] Eichensehr op cit note 156 at 145.
[225] Jennifer Daskal 'Borders and Bits' (2018) 71 *Vanderbilt Law Review* 179 at 220.

assisting LEA during the investigation of a crime, they do not explicitly set out the level of support or the extent of support to be provided. Any laws on cloud computing should promote economic development, promote sharing of data within the confines of data protection principles and international cooperation.

The absence of international frameworks for accessing digital evidence has seen governments increasingly taking unilateral approaches to seize information stored outside their borders.[226] This chapter explores how service providers navigate conflict of laws challenges when requested by LEA to disclose remote cloud data. Cross border unilateral access to data disregards the laws of other sovereigns. The potential of cloud data being subject to the jurisdiction of multiple states may present the challenge of conflict of laws for service providers who may be requested by LEA to assist in cybercrime investigations. Conflict of laws may force service providers to disregard the laws of one country to comply with the laws of another. What would work best for service providers would be a mechanism for cross border cooperation to avoid the difficulty of navigating through conflicting laws. The cross border cooperation would entail modernising outdated systems and laws and creating complementary mechanisms that operate with the efficiency required to meet today's challenges and safeguard time-honoured values including privacy and human rights.[227]

II. WHAT IS CLOUD COMPUTING?

a. What is the cloud?

It is imperative to this study to discuss how cloud computing technology works.[228] Digital transformation in both the private and public sector is heavily reliant on cloud computing. Cloud computing is 'the foundational enabler of digital transformation projects and offers the scale and speed that is needed for businesses to focus on transformation'.[229] By definition, cloud computing is 'the technology which enables network access to a scalable[230] and elastic[231] pool of shareable physical or virtual resources such as servers, operating systems, networks, software, applications and storage equipment'.[232] The National Institute of Standards and Technology (NIST) defines cloud computing as 'a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of

[226] Microsoft op cit note 210 at 38.
[227] Microsoft op cit note 210 at 39.
[228] Matthew McKenna 'Up in the cloud: Finding common ground in providing for law enforcement access to data held by cloud computing service providers' (2016) 49 *Vanderbilt Journal of Transnational Law* 1417 at 1420.
[229] State Information Technology Agency 'Digital Transformation 2020 – 2024 Strategic Plan'.
[230] Scalable means 'that the amount of computing capacity can be varied as required to meet a customer's requirements'. Simon Bradshaw, Christopher Millard and Ian Walden 'Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services' (2011) *International Journal of Law and Information Technology* 187 at 190.
[231] Elastic means the scaling can be done rapidly in response to changes in demand. Ibid.
[232] International Organisation for Standardization and the International Electrotechnical Commission ISO/IEC 17788 Information Technology – Overview and Vocabulary 2014. ISO/IEC 17788 provides an overview of cloud computing along with a set of terms and definitions.

configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[233] This technology permits one to use another person's computer and computing resources without the burden of maintaining or owning the underlying infrastructure. Use of multiple data centers in different regions ensures business continuity as cloud service providers can continue to offer services in the event of one of the data centers being destroyed.[234]

The cloud market is expected to grow and become a standard bearer in relation to the provision of IT services[235] which is beneficial to different user requirements. Examples of everyday uses of the cloud include email services like Gmail[236], software applications like Microsoft 365[237], Google Dropbox[238], and Apple iCloud.[239] Business functions relying on services such as customer relationship management offered by companies like Salesforce[240], payroll and human resources management, enterprise resource planning,[241] accounts, finance, billing, sales management, and telemedicine.[242] Cloud services also play a crucial role in the digital transformation of the public sector and in e-government.[243] It enables governments to operate infrastructure as a service, platform as a service and software as a service.[244] The model of cloud services enables a customer to only pay for actual resource consumption.[245] The International Organisation for Standardization[246] compares the consumption and payment of cloud services as similar to electricity supply which is often billed based on measured

[233] The National Institute of Standards and Technology (NIST). Available at *https://www.nist.gov/*, accessed on 3 May 2020. It should be noted that the international standards developed by the ISO/IEC and NIST are voluntary.
[234] International Organisation for Standardization and the International Electrotechnical Commission ISO/IEC TR 22678 Information Technology – Cloud Computing – Guidance for Policy Development 2019.
[235] Allison Gillwald and Mpho Moyo *Modernising the Public Sector through the Cloud: A report commissioned by the Microsoft Foundation* (2016) 1 at 12.
[236] Available at *https://www.google.com/gmail/about/*, accessed on 10 September 2021.
[237] Available at *https://www.microsoft.com/en-za/microsoft-365/what-is-microsoft-365* accessed on 10 September 2021.
[238] Available at *https://www.dropbox.com/?_hp=c&landing=dbv2*, accessed on 10 September 2021.
[239] Koops and Goodwin op cit note 146 at 22.
[240] Available at *https://www.salesforce.com/*, accessed on 11 September 2021.
[241] Rich Sauer 'Achieving trust and compliance in the cloud' (2016) 9 *International In-House Counsel Journal* 1 at 2.
[242] Porwal, Nair and Dimitrakos op cit note 214 at 293.
[243] Research conducted in the Western Cape Government in South Africa on m-government indicated that cloud computing plays an important role in m-government as it would allow for enhanced managerial efficiency and effectiveness in government. Zoran Mitrovic, Ntombovuyo Klaas and Fidel Mbhele 'Benefits of introducing the cloud computing-based m-government in the Western Cape: Policy Implications' 2013 7th International Conference on Theory and Practice of Electronic Governance "Beyond 2015 – Smart Governance, Smart Development"' Soul, Korea 22 – 25 October 2013.
[244] The government of the United Kingdom has developed its Government Cloud Computing (G-Cloud) programme which seeks to enhance e-government. Through this framework, government agencies can purchase cloud services via the cloudstore. Available at *https://advice-cloud.co.uk/ultimate-guide-gcloud/*, last accessed on 10 September 2021.
[245] Allison Gillwald and Mpho Moyo 'The cloud over Africa' 2013 Research ICT Africa Policy Paper prepared for the United Nations Conference on Trade and Development Information Economy Report 2013: The Cloud Economy and Developing Countries 1 at 2.
[246] Available at *https://www.iso.org/home.html*, accessed on 11 September 2021.

energy consumption.[247] In instances where a customer has an increased or decreased demand for resource consumption, they can easily scale up[248] or down depending on their needs.

There are three main types of cloud computing models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This study primarily focuses on Software as a Service and Infrastructure as a Service. It considers the role of data centres and data infrastructures in determining jurisdiction over electronic evidence. It also considers access to remote data storage like Dropbox or Google and remote email service such as Gmail and Microsoft Outlook. When determining which data centres to store user data, cloud service providers normally consider customer or legal requirements, a country's prevailing policy and legal landscape, availability of storage, storage costs, network capacity and availability.[249] These factors are also supported by other compelling factors such as cooler climate, political factors, and economic factors.

i. Infrastructure as a Service

IaaS is the virtual equivalent to physical hardware such as processors and hard drives.[250] IaaS model allows users to deploy their own software, applications, and operating systems.[251] The underlying cloud infrastructure is managed and controlled by a third party. Examples of the use of raw computing resources include Rackspace or Google Compute Engine.[252] While a user has control over storage, operating systems, and deployed applications, they may have limited control over networking components such as host firewalls.[253] Most cloud service providers own server farms where cloud infrastructures are built. Microsoft for example has built data centres in both Johannesburg and Cape Town.[254] The government of South Africa also runs its own data centres located within the country. When physical cloud infrastructures are built within a state, that state has jurisdiction over the infrastructure. This is territorial jurisdiction. The contention arises on whether the exercise of jurisdiction over the cloud infrastructure extends to data hosted on the infrastructure.

ii. Platform as a Service

PaaS model provides a user with a platform to develop and use software applications, such as Microsoft Azure[255] and Amazon Web Services[256]. The user can deploy its own applications including

[247] ISO/IEC TR 22678 op cit note 236.
[248] Scaling up means increasing the size of a resource and expanding the use of the cloud service.
[249] ISO/IEC TR 22678 op cit note 236.
[250] Gillwald and Moyo op cit note 247 at 4.
[251] Ibid.
[252] Koops and Goodwin op cit note 146 at 22.
[253] Gillwald and Moyo op cit note 247 at 4.
[254] Gillwald and Moyo op cit note 237 at 30.
[255] Available at *https://azure.microsoft.com/en-gb/*, accessed on 11 September 2021.
[256] Available at *https://aws.amazon.com/?nc2=h_lg*, accessed on 11 September 2021.

programming tools on the infrastructure owned and managed by the cloud provider.[257] The user does not manage or control the underlying cloud infrastructure but has control over the deployed applications and configuration settings for the application hosting environment.[258] This study will not discuss PaaS as it is mainly concerned with software development, which is not relevant for purposes of this study.

iii. Software as a Service

Consonant to this study is the SaaS model. SaaS offers software as a remote service for end users, such as webmail services or word processing software applications. SaaS also includes storage as a service in which users can manage data storage, organisation, and retrieval from any location over the internet. Good examples of SaaS are Dropbox or Rackspace's cloud files.[259] With a SaaS model, the user does not decide on where their data may be hosted. That decision is entirely up to the cloud service provider. As mentioned earlier, the location of data centres is determined by factors such as storage costs, network capacity and availability, storage performance, legal requirements, and at times customer requirements.[260]

In practice, these models may be offered by different cloud players and not by the same cloud service providers. For example, the infrastructure supporting Dropbox cloud storage may be offered by AWS.[261] The challenge with multiple cloud players is ascertaining the provider with lawful authority to disclose data. In some instances, it is difficult to determine the possible or likely place of the servers on which data are stored.[262] The lack of understanding of which cloud service provider may have actual control over cloud data relevant for an investigation compounds the problems of establishing jurisdiction in the cloud.

b. Different types of clouds

Whilst there are three cloud models, there are also four types of clouds - public, private, community and hybrid. A public cloud is a resource open to the public.[263] Usually, a cloud user does not need to pay to utilise a public cloud. Users of Dropbox and Facebook do not need to pay any fees to open accounts and store data on these platforms.[264] It should be noted that the public cloud is not

[257] App developers working on mobile applications usually use cloud-based platforms to develop and launch their services. Gillwald and Moyo op cit note 247 at 5.
[258] Ibid.
[259] W Kuan Hon & Christopher Millard 'Cloud technologies and services' in Christopher Millard (ed.) *Cloud Computing Law* (2013).
[260] ISO/IEC TR 22678 op cit note 236.
[261] Koops and Goodwin op cit note 146 at 23.
[262] Ibid.
[263] Examples of public clouds include Amazon's Elastic Compute Cloud, IBM's Blue Cloud, Microsoft's Windows Azure. Jay P Kesan and Masooda N Bashir 'Privacy in the cloud: Going beyond the contractarian paradigm' (2011) *Proceedings of the 2011 Workshop on Governance of Technology, Information and Policies* 21.
[264] Gillwald and Moyo op cit note 247 at 4.

always free and does not mean that a user's data are publicly visible.[265] Conversely, a private cloud is a dedicated resource provided by a cloud service provider for a single client or user.[266] Private cloud users usually pay a fee in order to enjoy the service offering and get better security measures when compared to public cloud users.[267] Private clouds are usually utilised by government departments or large business users or companies. A community cloud is a resource or service provided for and shared between a limited range of clients or users. As the name suggests, a hybrid cloud is a mixture of any of the deployment models.[268] The type of cloud model used may have relevance on the exercise of jurisdiction by LEA. As will be discussed in chapter 4, publicly available data are subject to the jurisdiction of any state. This would mean that data shared on the public cloud may be subject to the jurisdiction of several states. On the other hand, it may not be easy for LEA to access private cloud data. The discussion on litigation battles and court judgements in chapter 4 expands more on the jurisdictional challenges of private cloud data.

c. Features of cloud data which pose jurisdictional challenges to LEA

As will be discussed in Chapter 4 of this study, territorial borders define and limit criminal investigation and collection of evidence. The features of cloud data make it possible for evidence to be hosted on a cloud server in a foreign state. Discussing features of cloud data provides an understanding of 'how the relevant attributes of data map onto the underlying normative goals that the jurisdictional rules are trying to satisfy'.[269] When the unique key attributes of cloud data are sufficiently highlighted, it triggers an assessment of the rationale behind blithely applying traditional rules to technological developments. Such a discussion highlights the potential risk of undermining the criminal justice system by not serving the key normative interests.[270] Some of the notable reasons for low prosecution of cybercrime has been attributed to inadequate laws. If cloud data jurisdiction is still a contentious issue in cybercrime investigation and prosecution, it may be prudent to consider these arguments and the justification for new jurisdictional principles. To access this evidence would involve cross border searches or cross border transfer of data. It is debateable whether law enforcement agents' access to cross border data amounts to the exercise of extraterritorial jurisdiction or a violation of another state's sovereignty. Generally, when evidence relating to a criminal matter under investigation is in another state, LEA follow prescribed channels on mutual legal assistance or other forms of international

[265] Promise Sthembiso Mvelase, Innocentia Zamaswazi Dlamini, Happy Marumo Sithole and Nomusa Dlodlo 'Towards a government public cloud model: the case of South Africa' (2013) *Second International Conference "Cluster Computing* 149 at 150.
[266] Gillwald and Moyo op cit note 237 at 10.
[267] O'Keeffe points out that 'risk generally increases as cost decreases, with a public cloud offering being on the higher end of the spectrum from a risk point of view and the traditional client-server architecture viewed as the least risky.' O'Keeffe op cit note 221 at 2.
[268] Gillwald and Moyo op cit note 247 at 4.
[269]Daskal op cit note 227 at 220.
[270] Ibid.

cooperation to secure that evidence.[271] This is because LEA understand that they do not and cannot exercise enforcement jurisdiction in a foreign state. However, the same rules are ambiguous when dealing with cloud data as such data may easily be accessed and secured without LEA leaving their duty stations.

i. Data divisibility and fragmentation

Cloud computing services mainly focus on ensuring efficiency as well as information security. Fragmentation of data is one of the unique features of cloud services which is aimed at ensuring efficiency. Fragmentation is also called sharding or partitioning.[272] It means that 'certain sets of data are split and distributed (in pieces) among various computers and automatically relocated depending on the supply and demand of storage space in the cloud at a certain point in time'.[273] The various computers to which fragments of the data are distributed can potentially be in different countries. When a user wishes to access the data, they do not access the data in fragments. Upon entering correct credentials, the fragmented data sets are automatically reunited, and the user will be able to access the full set of data seamlessly.[274]

Koops and Goodwin argue that the distributed, dynamic, and redundant nature of cloud storage makes it difficult to say 'where' a certain file 'is' when it is stored in the cloud. This is because 'it can be in multiple places simultaneously and still not be in any single place in its entirety'.[275] If data are divided and randomly scattered on data servers around the world, the challenge becomes which states will exercise jurisdiction over the cloud data. Ordinarily, the country where the data centres are established has jurisdiction over the cloud infrastructure. However, it is unclear whether the state can exercise jurisdiction if the hosted data are for a foreign based user or owner. Where the data are hosted on servers in multiple states, the data are subjected to different laws and potential seizure by different law enforcement agencies.[276] When multiple states can potentially access data, that creates a privacy challenge for the person to whom the data relates. If one state seizes the data, it remains available and unaltered in any meaningful way for another state.[277] Due to the versatility of cloud data, the question remains whether cloud data should be subject to a different set of jurisdictional rules. Data exceptionalists are convinced that cloud data are unique to warrant new jurisdictional principles.

[271] Koops and Goodwin op cit note 146 at 24.
[272] Hon et al defines sharding as an automated procedure performed by a cloud provider's software, which automatically breaks data up into fragments for storage in different storage equipment, possibly in different locations, based on the provider's sharding policies, such as performance maximisation. Hon, Millard and Walden op cit note 166.
[273] Koops and Goodwin op cit note 146 at 22.
[274] Ibid.
[275] Ibid.
[276]Daskal op cit note 227 at 223.
[277] Ibid.

Traditionalists on the other hand, are not convinced that there should be new jurisdictional rules for cloud data. This debate is discussed in detail in chapter 4 of this study.

ii. Location independence

Location independence mean that cloud data can be accessed from an arbitrary location and not necessarily near the user.[278] This feature of cloud data presents the main challenge to jurisdictional principles on whether access to the remote data is an exercise of either territorial or extraterritorial jurisdiction. If there is an internet connection or private network, one can access cloud data. Cloud data can be accessed by using different devices such as laptops, mobile phones and personal computers.[279] Cardinal to this discussion is that IoT devices are not the same as the cloud but only act as a conduit to access cloud data. The cloud data may be hosted on a server in a different country. Before cloud computing technologies, data used to be stored on a computer's internal memory, computer hard drives, portable external hard drives, locally built server rooms or within an organisation or within a hosted environment dedicated to a single country or other jurisdiction.[280] The traditional IT infrastructure was normally done by staff and using facilities in the same jurisdiction as the customers of the service. The digital disruption of cloud computing is that location is no longer important. Customers in one country can use cloud computing resources located in another country. The resources may be managed by a cloud service provider located in yet another country. This means that cloud data can be accessed and manipulated remotely[281] and this remote location can be another country, continent, and ultimately another jurisdiction.[282]

The challenge with data location or data residency is that a foreign state may have a stronger jurisdictional basis over cloud data. The basis of jurisdiction could be because the data centres are established within that state or alternatively the cloud service provider is registered within that state. It may not always be straightforward for an investigating state to access the cloud data even in cases where the crime was committed by a citizen and within its borders. Where there are diplomatic tensions between the investigating state and the state where the cloud data resides, the investigating state may not be able to unilaterally access the cloud data.

Cloud services are remote service offerings which means that the cloud service provider does not necessarily have to establish an office in every jurisdiction. Several cloud service providers offer services in foreign states without even setting foot in these states.[283] Without legal presence, LEA may find it difficult to compel the foreign service providers for their assistance in an investigation. Due to

[278] Jennifer Daskal 'The un-territoriality of data' (2015) *The Yale Law Journal* 125 at 373.
[279] ISO/TEC 17788 op cit note 234.
[280] ISO/IEC TR 22678 op cit note 236.
[281] Daskal op cit note 227 at 227.
[282] Ibid.
[283] Ibid at 225.

location independence of cloud data, states are concerned that they will not be able to regulate cloud service providers offering services to citizens located within their territories simply because the service providers are not territorially based there.[284] As a result, states have devised ways of exercising jurisdiction over cloud data as discussed in chapter 4 of this study.

iii. 3rd party control

Multinational companies dominate the cloud services market. As mentioned earlier, cloud service providers play a significant role in electronic evidence gathering as they exercise control over the cloud data. When one compares data to money, one can note that though financial institutions are the custodians of the money, the owner of the money always has control over their money, the taxes, and interests to be paid and earned in respect of their money.[285] They know the country and the bank that is keeping their money. On the contrary, most cloud users do not have knowledge of where their data are located or hosted. Some states do not require cloud service providers to disclose the locations of their data centres. Neither is there a legal obligation to inform the data user when data are in transit. Daskal points out that third party control makes the location of the third party (and not the location of the property) potentially determinative of the rules that apply.[286] The US CLOUD Act[287] relies on this position as the United States government is able to exercise jurisdiction over any cloud data under the control of a US based entity.

iv. Multiple players

According to the NIST Reference Model, there are 5 major cloud players in the delivery process. These are the cloud consumer, cloud service provider, cloud carrier, cloud auditor and cloud broker. There are complex contractual relationships which may exist among these different cloud players. A cloud service provider usually has direct contractual relationship with a subscriber. A cloud infrastructure provider usually contracts with the cloud service provider and provides infrastructure. A communication service provider will be responsible for the transmission service enabling the cloud user to communicate with the cloud service provider.[288] Most cloud service providers adopt the principle of shared responsibility. This means that different role players like the cloud service customer[289], the cloud service user and the cloud service partner or broker[290] all have certain responsibilities in maintaining the security, privacy, confidentiality, and integrity of the service.[291] In such layered constructions, it

[284]Ibid at 227 at 225. ISO/IEC TR 22678 op cit note 236.
[285] Woods op cit note 212.
[286] Daskal op cit note 280 at 378.
[287] Clarifying Lawful Overseas Use of Data Act H.R.4943 (2018).
[288] Walden op cit note 101.
[289] A cloud service customer is a party which is in a business relationship for the purpose of using cloud services. ISO/IEC 17788 op cit note 234.
[290] A cloud service partner or broker is one who negotiates relationships between cloud service customers and cloud service providers. ISO/IEC 17788 op cit note 234.
[291] ISO/IEC TR 22678 op cit note 236.

may be more difficult to determine the scope of the different provider's rights and capacities to access customer-uploaded data. In instances where LEA are looking for access to cloud evidence, it may be difficult to timeously identify the role player responsible for the control of the cloud data. This also means that it is not clear which of the role players can lawfully provide LEA with access to cloud data.

Apart from having several actors involved in the provision of cloud services, another potential challenge is the use of multi-tenant platforms. A multi-tenant platform is a set-up which allows cloud service customers and tenants to pool storage resources and network resources. The challenge with this arrangement is that giving LEA physical access to the same pooled resource can potentially violate the confidentiality of other customers.[292] It might also be difficult to determine the possible or likely place of the servers on which data are stored.[293] To successfully establish the location of data may involve studying the terms, conditions and practices of all different cloud providers involved. Koops notes that even after such determination, it may still be difficult to pinpoint where particular data are as the different players may only see their limited part of the picture.[294] Since the cloud user has no choice in where their data are hosted, they also don't have control over the rules that potentially govern access to their data.[295] Without knowledge of where the data are located and without knowledge of who has control over the data, data owners are left in a limbo. They are not able to hold their governments accountable,[296] they are not able to know which foreign governments may have access to their data. Most importantly, they are not aware of the extent to which their data may be collected by foreign actors and the extent of their vulnerability.

Lack of proper data governance in the cloud presents a risk in governments failing to protect the privacy interests of their citizens. Improper data governance can potentially result in governments being unable to effectively investigate crime. Cross border access to cloud data by foreign governments significantly increases the risks to privacy violations. With the cloud holding insurmountable amounts of data, foreign governments' access to data might be intrusive if stringent safeguards are not put in place.[297]

An unregulated cloud environment favours the country where the cloud service providers are headquartered. By default, the country where the service provider is registered exercises personal jurisdiction over the service provider. In the event of a crime investigation, the service provider is required to cooperate and assist LEA from such a country. However, an investigating country seeking access to cloud data may find it difficult to compel the cloud service provider to cooperate. The

[292] Ibid.
[293] Koops and Goodwin op cit note 146 at 24.
[294] Ibid at 44.
[295] Daskal op cit note 227 at 225.
[296] Ibid.
[297] Koops and Goodwin op cit note 146 at 46.

investigating country's authority is very limited if there are no laws in place to compel the service provider to directly cooperate with it. For instance, if the service provider is registered in the US and the data are hosted in Europe, the investigating state may not be able to compel the service provider to cooperate.[298]

v. Encrypted data

Chapter 3 of this study discusses the issue of anonymity and encryption. Encryption is a very useful information security measure. Service providers and users both use encryption tools to protect data when stored in the cloud. When a data owner has encrypted their data, it may not be easy for the cloud provider to decrypt the data unless if they have access to the decryption key.[299] The purpose behind the tools to anonymise or pseudonymise data is to conceal or hide the data subjects' identities[300] as well as restricting who may access the data. Millard and Walden note that the security of encrypted data depends on the strength of the encryption method used, i.e., the cryptographic strength of the algorithm, and the length of the encryption key, with longer keys generally providing better security against attacks.[301] When a cloud user encrypts their data, the cloud service customer or the cloud service provider may not be able to view or control that data. At the same time, it may be potentially difficult to identify their identity or location. If LEA cannot determine the identity of the suspect or their location, a judge or magistrate may refuse to issue them a search warrant.

vi. Data mirrors and data in transit

One of the principles of information security is maintaining copies of data on replica data centres.[302] Most cloud service providers operate replica data centres. Cloud service providers build or rent out extensive pieces of land across the world to operate expansive server parks or data farms.[303] This is done so that in the event of a server park malfunction, disaster or cyberattack, data may still be retrieved from the replica data centre. Data algorithms constantly move replicated or fragmented data around different servers within or across different countries at any time.[304] The global replication of data improves the customer experience by reducing data access latency.[305] Dropbox for instance uses servers in different countries to store its users' data which is constantly being moved around to minimise costs and maximise availability.[306] At the same time, the files stored on Dropbox are accessible at any

[298] For growing economies like South Africa, it might not be possible for LEA to have the same authoritative hand over foreign cloud service providers.
[299] Koops and Goodwin op cit note 146 at 23.
[300] Hon et al op cit note 169.
[301] Ibid.
[302] ISO/IEC 17788 op cit note 234.
[303] Koops and Goodwin op cit note 146 at 22.
[304] Koops and Goodwin op cit note 146 at 42.
[305] Latency means the delay before a transfer of data begins following an instruction for its transfer.
[306] Koops and Goodwin op cit note 146 at 42.

time, but their exact location at a certain point in time is potentially indeterminable.[307] When data are in transit, its location may be difficult to ascertain. What this means for LEA is that they cannot get a search warrant from court, as the location of the evidence requirement cannot be met. This can be a constant hurdle for LEA since data are constantly moved around different servers for efficiency and improving availability.

vii. Data mobility

The mobility of data has been one of the features which justified the school of thought for a development of new jurisdictional rules for the cloud. Data moves at the speed of light, in an unpredictable fashion and generally unknown to both the data subject and the governments seeking to access sought after data. Daskal argues that data location is an unstable basis for defining territoriality or delimiting enforcement jurisdiction.[308] This stems, Daskal argues, from the understanding that jurisdictional rules that turn on the location of data fail to serve key normative and practical interests at stake.[309] Woods on the other hand, points out that data are not the only kind of property that is highly mobile to warrant a different set of rules. By comparison, money has similar mobility attributes as data. It can be instantly transferred from one location to another and there are no difficulties in determining the location of money for the purposes of asserting jurisdiction over the asset.[310] Woods submits that if intangible assets such as intellectual property or debts can be seized extraterritorially, so can cloud data.[311] Woods argues that the mobility of data mobility only creates novel market arrangements but does not present a fundamental theoretical on jurisdiction[312] to warrant the adoption on new jurisdictional principles.

Notably, data mobility and the constant change of territorial jurisdiction can be a setback for LEA relying on the location of data principle. Typically, an investigating state would need to negotiate with the country where the data are located to exercise its enforcement jurisdiction. Depending on the relationship between the two countries, such negotiations may take some time. However, if by the time the foreign state has granted permission to access the data, the data might have been moved to a server

[307] Ibid.
[308] Daskal op cit note 227 at 222.
[309] Ibid.
[310] Woods op cit note 212 at 754-6. Woods dispute the claims that data is unique and submits that the unique nature of data is overstated. Woods clarifies that these claims are not solely about the nature of data, but rather about the role of data in the cloud. If a French person writes in her diary while she is in France, her diary is in in France. If she jots down her thoughts on an iPad while in France, that digital data is in France and the situation is functionally the same. The move from a paper diary to a digital one does not raise novel jurisdictional concerns. If the same person however backs up her iPad to iCloud, her thoughts may be stored on servers in another country and here we get into potentially novel territory.
[311] Woods op cit note 212 at 735.
[312] Ibid at 759.

in another country. This can create a vicious cycle where the investigating state will have to constantly keep negotiating with different states wherever the data may be located.

viii. Loss of knowledge of location of data[313][314]

While location in cyberspace is generally difficult to determine, the cloud compounds the complexity of data location.[315] One of the most salient features of cloud services is that there is less need for storing data on IoT devices. The traditional searches and seizures of electronic devices will gradually be extended to include network searches, internet interceptions and serving production orders on cloud providers.[316] While one may access their email message, it is not always possible to tell exactly where the data representing this message might be located as such data are constantly moved around by algorithms. Even cloud providers may not know where the sought-after data are located. Svantesson submits that ascertaining the location of data may be difficult, or in some cases impossible.[317] Koops and Goodwin do not agree that it is impossible to identify the location of cloud data. They assert that reports on the impossibility of doing so were grossly exaggerated and most authors who suggest this impossibility have a legal background with no in-depth practical experience in cloud computing services.[318]

If the location of data is unknown, LEA cannot blindly conduct searches and seizures. To do so would likely threaten the sovereign interests of a foreign state, where the sought-after data happen to be located. Without knowledge of location of data, mutual legal assistance may not be feasible. The investigating state will not know which country to approach for legal assistance and cooperation. The application of the territoriality principle may also be impossible.

The above-mentioned features of cloud data make it difficult to ascertain the location of the cloud data.[319] Not knowing the location of cloud data has spawned a new legal debate on jurisdiction. The Cybercrime Convention's Cloud Evidence Group reported that a major challenge of cloud computing is that data are not stable but often distributed over and moving between different services, providers, locations, and jurisdiction, while law enforcement powers are usually defined territorially.[320] With the cloud, there is a constant challenge of not knowing 'where' a certain file is located when it is stored in

[313] The claim to loss of location was introduced by Jan Spoenle in a discussion paper for the Council of Europe's Project on Cybercrime. Spoenle points out that algorithms constantly move users' data around. He explains that while it is always possible to access a certain email message, it is not possible to tell where exactly the data representing this message might be located. Jan Spoenle 'Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?' (*Strasbourg: Council of Europe, 2010*) at 4 – 5.
[314] Halefom op cit note 22 at 20.
[315] Koops and Goodwin op cit note 146 at 44.
[316] Ibid at 23.
[317] Svantesson op cit note 104 at 104.
[318] Koops and Goodwin op cit note 146 at 44.
[319] Spoenle op cit note 315.
[320] Daskal op cit note 227 at 186.

the cloud. To date, answers to the key jurisdictional questions vary depending on the government seeking access to data, the type of data at issue and the perspective of the judges that oversee many of the requests.[321] This lack of knowledge of the location of data is a deep-rooted issue for criminal lawyers, international law experts, and academics. If data cannot be located at any point in time, which state should exercise jurisdiction over the data? In the alternative, can any law enforcement agencies access data whose location is unknown? Which of the existing jurisdictional principles is of relevance when data location is unknown? The loss of knowledge of data location raises concerns over whether people's privacy and personal data will be protected across any jurisdiction that the data may be located at any given point in time.

III. CLOUD COMPUTING LAW IN SOUTH AFRICA

South Africa is one of the leading countries in Africa steadily adopting cloud computing services. The South African government has several policies[322] and strategic documents[323] which includes initiatives towards the adoption of cloud services in the public sector. Steering the digital transformation in government is the State Information Technology Agency (SITA). SITA is a government owned company which is responsible for the provision of ICT services to government and government departments.[324] SITA recently launched a new government cloud infrastructure for South Africa, which is said to be one of the largest government clouds in the world.[325] Apart from SITA, there are other players in the provision of cloud services to the public sector. Private companies like Gijima, Huawei and IBM and Microsoft[326] have played an active role in the provision of cloud services.

South Africa's Department of Communications and Digital Technologies recently published a draft National Data and Cloud Policy for public comment. This was after increased concern over the absence of a cloud policy or cloud computing law. As an innovation, the technology of cloud computing is not yet regulated. Cloud computing law is a new area of law in South Africa. At the time of writing of this study, there is no collective academic work on cloud computing law within the South African context. This section identifies the piecemeal legislation and policy aimed at shaping cloud computing

[321] Ibid.
[322] National Development Plan 2030 – Our future, make it work; National Integrated ICT Policy White Paper 2016; South Africa Connect: Creating opportunities, ensuring inclusion – South Africa's Broadband Policy 2013.
[323] *National e-Strategy Digital Society South Africa* GN 887 in GG 41242 of 10 November 2017; *National e-Government Strategy and Roadmap* GN 886 in GG 41241 of 10 November 2017.
[324] State Information Technology Agency Act 88 of 1998.
[325] SITA Annual Report 2018/2019.
[326] Microsoft Cloud in Public Sector – South Africa cloud projects include the City of Johannesburg cloud-based consumer engagement -Find and Fix that enabled residents to be the city's eyes and ears by reporting road problems such as potholes, faulty traffic lights and damage manholes. Another example is the Government Pension Administration Agency (GPAA) migration to the Microsoft cloud which enabled it to go paperless and introduce self service facilities to access data. This enabled GPAA to address fraud and corruption and build more controls into their processes. It also moved its call centre to the cloud and within three days the new call centre was up and running. Microsoft 'Cloud in Public Sector – South Africa' available on *https://www.microsoft.com/MEA/trustedcloud/southafrica/public-sector.aspx*, accessed on 14 July 2020.

law in South Africa. It examines the existing ICT laws together with various policy developments. The aim of this discussion is to set out South Africa's position on data residency, data sovereignty and cumulatively data jurisdiction. An analysis of South Africa's corpus on cloud computing technologies may provide clarity on whether the existing laws solve the cloud data jurisdictional dilemma or if it is necessary to develop cloud computing law. A gap in the regulation of cloud computing services may warrant the development of cloud computing law.

a. A constitutional perspective on cloud computing

Participating in a digital society and enjoying the technological benefits of cloud computing services helps to improve the quality of life of all citizens and free the potential of each person.[327] The Constitution of South Africa recognises the values of human dignity, the achievement of equality and the advancement of human rights and freedoms.[328] The Bill of Rights is the cornerstone of democracy in South Africa. It enshrines the rights of all people in South Africa and affirms democratic values of human dignity, equality, and freedom. The state must respect, protect, promote, and fulfil the rights in the Bill of Rights.[329] When LEA are seeking access to cloud data, they need to respect a person's right to privacy and dignity.[330]

The international community also recognises privacy as a right which must be protected in the digital world or cyberspace and an internationally recognised human right. Article 12 of the Universal Declaration on Human Rights[331] provides that 'no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'. Similarly, Article 17 of the International Covenant on Civil and Political Rights[332] provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.

In Europe, there are several instruments to note which protects the right to privacy. The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms also protects the right to privacy.[333] In 1980, the Council of Europe adopted another treaty which protects personal data

[327] Preamble of the Constitution of the Republic of South Africa, 1996.
[328] Section 1 of the Constitution, 1996.
[329] Section 7 of the Constitution, 1996.
[330] Section 14 of the Constitution – Everyone has the right to privacy, which includes the right not to have their person or home searched, their property searched, their possessions seized, or the privacy of their communications infringed. Section 10 of the Constitution, 1996.
[331] Adopted by General Assembly Resolution 217 A(III) of 10 December 1948.
[332] Adopted by General Assembly Resolution 2200A (XXI) of 16 December 1966.
[333] 'Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law

and privacy. Convention 108[334] applies to all data processing carried out by private and public sectors including data processing by the judiciary and LEA. The changes brought about by emerging technologies such as cloud computing have also resulted in the adoption of Convention 108+.[335] The modernisation of the Convention 108 reinforces the Convention's potential use as a universal instrument on data protection while aligning with the developments on data protection within Europe. Article 7 of the EU Charter of Fundamental Human Rights affords everyone the right to respect his or her private and family life, home, and communications.[336] Prior to the adoption of the GDPR, the centrepiece of EU regulation in the field of data protection was Directive 95/46/EC.[337] This directive required EU member states to adopt data protection laws at national level. The GDPR[338], as will be discussed throughout this study, is an important legal instrument which regulates how personal data are processed and inadvertently provides some protections to the right to privacy.

The right to privacy was not previously recognised as a right under some important legal instruments in Africa. The ACHPR failed to include the right to privacy which has resulted in commentators alluding that there was no culture to privacy in Africa.[339] The ACRWC[340] was one of the earlier instruments which expressly guaranteed the right to privacy. Article 10 of the ACRWC provides that 'no child shall be subject to arbitrary or unlawful interference with his privacy, family home or

---

and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' Article 8 of The Convention for the Protection of Human Rights and Fundamental Freedoms Rome 4.XI.1950.

[334] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS 108 of 1981 (Convention 108). It came into force on 1 October 1985.

[335] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018. Part of the preamble provides that 'The member States of the Council of Europe, and the other signatories hereto,-
…
considering that it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data;
…'.

[336] Article 7 of the EU Charter of Fundamental Human Rights 2012/C 326/02.

[337] Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Directive 95/46/EC of the European Parliament and the Council of 24 October 1995.

[338] Article 1 of the GDPR set out its objectives as follows –
'This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.' Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[339] Makulilo quotes Olinger H.N. et al 'Western privacy and / or ubuntu? Some critical comments on the influences in the forthcoming data protection in South Africa' (2007) The International Information & Library Review. Alex B Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) *Computer Law & Security Review* 78 at 78.

[340] African Charter on the Rights and Welfare of the Child 1990.

correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks'. The AU eventually passed the African Union Convention on Cybersecurity and Data Protection[341] to keep up with developments on data protection and cybersecurity. The SADC Model Law on Data Protection[342] is a model law which was designed to guide SADC member states when developing their own data protection laws. The ECOWAS Supplementary Act on Personal Data Protection within ECOWAS[343] is a legal instrument on data protection applicable to countries in west Africa.[344] The EAC Cyberlaws 2008 is a legal instruments which addressing various issues including data protection for the east African community.[345] Though not a legally binding document, the African Declaration on Internet Rights and Freedoms is an important document which recognises the right to privacy and personal data protection as a key principle.[346]

When retrieving cloud data and further processing cloud evidence, LEA still need to protect the constitutional right to privacy. In the recent AmaBhungane case[347], the Constitutional Court had to decide on the constitutionality of mass surveillance and state actioned searches in terms of the RICA Act. The court applied the two-stage analysis which involved considering whether a constitutional right had been infringed and secondly whether that infringement could be justified in terms of section 36 of the Constitution (the limitation clause). This is because the right to privacy is not an absolute right and

[341] Chapter 2 of the Malabo Convention deals with the protection of personal data. Article 8 provides that 'Each state party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principles of free flow of personal data.' Malabo Convention.

[342] Establishment of Harmonised Policies for the ICT Market in the ACP Countries: Data Protection: Southern African Development Community Model Law 2013.

[343] Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS 2010 (ECOWAS Data Protection Act). Article 2 of the ECOWAS Data Protection Act provides that 'Every Member state shall establish a legal framework for the protection of the privacy of data including the collection, processing transmission, storage, and use of personal data without prejudice to the general interest of the state.'

[344] Orji notes that the ECOWAS Data Protection Act harmonises data protection laws in ECOWAS Member States (member states being sovereign states in the West Africa sub-region). Uchenna Jerome Orji 'Regionalising data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act' (2017) *International Data Privacy Law* 179 at 179.

[345] East African Community Cyber Laws 2008.

[346] Article 8 of the African Declaration on Internet Rights and Freedoms provides that 'Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim'. African Declaration on Internet Rights and Freedoms. Available at https://africaninternetrights.org/ accessed 2 December 2020.

[347] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2019] 4 All SA 343 (GP) para 157.

can be limited if there are countervailing public interests or conflicting rights of others.[348] In applying this test, the apex court held that the surveillance techniques adopted by the state infringed on the right to privacy. Upon application of the limitation clause, the Constitutional Court held that the RICA Act did not pass constitutional master because of the lack of adequate safeguards for independent judicial supervision and the notification of subjects of surveillance.

When the police are processing personal information for the purposes of crime investigation, they are excluded from complying with POPIA to the extent that adequate safeguards have been established in legislation for the protection of such personal information.[349] While discussing the right to privacy during cybercrime investigation, Musoni correctly argued that the Criminal Procedure Act permitted police officers to conduct criminal investigations within clearly defined prisms without unlawfully infringing on suspects' rights to privacy.[350] Whilst police are generally expected to respect a person's privacy when carrying out their duties in terms of the CPA and the Cybercrimes Act, it is not clear whether the safeguards put in place effectively protect privacy and personal data. Following the Amabhungane judgement, it may be prudent that in addition to national security agencies putting in place safeguards to ensure that personal information and privacy rights are protected, law enforcement agencies and departments like SAPS should adopt similar safeguards in clearly drafted frameworks. South Africa can also draw lessons from the EU framework on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters.[351] In terms of this framework, member states are required to protect the fundamental human rights and freedoms when preventing, investigating, detecting, or prosecuting criminal offences or executing criminal functions.

People may use cloud-based platforms to disseminate information and receive information or ideas. When conducting any criminal investigations and accessing cloud data, LEA should respect this right to freedom of expression.[352] The right to freedom of association[353] is also recognized in the Constitution of the Republic of South Africa. LEA should not block a user from being a member of certain online groups or platforms unless if it is justifiable to do so. Everyone who is arrested for allegedly committing an offence has the right not to be compelled to make any confession or admission

[348] Konrad Lachmayer and Normann Witzleb 'The challenge to privacy from ever increasing state surveillance: A comparative perspective' (2014) *University of New South Wales Law Journal* 748 at 751.
[349] Section 6 (1) (c) (ii) of POPIA. The Information Regulator recently served the SAPS with summons for its failure to provide sufficient details regarding the disclosure of personal information of rape victims. Information Regulator Media Statements available at https://inforegulator.org.za/media-statements/ accessed on 12 September 2022.
[350] Musoni op cit note 158 at 686.
[351] Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matter 2008/977/JHA of 27 November 2009 [2008] OJ L 350/60 (Framework Decision).
[352] Section 16 of the Constitution – everyone has the right to freedom of expression, which includes freedom of the press and other media, freedom to receive or impart information or ideas; freedom of artistic creativity, and academic freedom and freedom of scientific research. The Constitution, 1996.
[353] Everyone has the right to freedom of association. Section 18 of the Constitution, 1996.

that could be used in evidence against that person.[354] Every accused person has a right to a fair trial, which includes the right to adduce and challenge evidence and[355] the right not to be compelled to give self-incriminating evidence.[356]

b. The Electronic Communications and Transactions Act 25 of 2002

The ECT Act is one of the prominent pieces of legislation relevant to cloud computing and electronic communications in South Africa. Its objectives are to promote legal certainty and confidence in respect of electronic communications and transactions[357] and to promote technology neutrality in its application.[358] The ECT Act is technology neutral, which means it applies to cloud computing technologies and any new technologies. It also ensures compliance with accepted international technical standards in the provision and development of electronic communications and transactions. In the absence of a cloud policy or cloud specific regulations, international standards such as the ISO standards are best practice which tend to be adopted and applied to the provision of cloud services in South Africa.[359]

Cloud service providers enjoy the same protection as any other service provider who provides storage of data messages in an information system. If the cloud service provider does not have actual knowledge of the cloud contents or of the activity relating to the cloud data messages, they will not be held liable for any damage that may arise from the cloud data.[360] LEA are also permitted to access cloud data during cybercrime investigations. Section 82 of the ECT Act empowers cyber inspectors to enter any premises or access an information system that has a bearing on an investigation and search and seize evidence. For cyber inspectors to exercise their powers, a magistrate or a judge of the High Court must issue a search warrant. There must have been reasonable grounds that an article is within his area of jurisdiction or an article is being used or is involved or has been used or was involved in the commission of an offence within his area of jurisdiction or within the Republic.[361] South African courts can issue a search warrant where '*information pertinent to the investigation is accessible from within the area of jurisdiction of the court*.'[362] Chapter 4 of this study expatiates these jurisdictional clauses under the ECT Act and discusses whether search warrants can be executed where data are located

[354] Section 35 (1) (c) of the Constitution, 1996.
[355] Section 35 (3) (i) of the Constitution, 1996.
[356] Section 35 (3) (j) of the Constitution, 1996.
[357] Section 2 (*e*) of the ECT Act.
[358] Section 2 (*f*) of the ECT Act.
[359] The DPSA recently issued a directive which provides guidelines to public service departments on the use of cloud computing services and technologies. Public Service Cloud Computing Determination and Directive Awareness Circular 1 of 2022. DPSA Standards available at https://www.dpsa.gov.za/policy-updates/e-gov/e_government/standards/ accessed 18 August 2022.
[360] Section 76 of the ECT Act.
[361] Section 83 of the ECT Act.
[362] Section 83 (2) (*c*) of the ECT Act.

outside South Africa. In other words, the chapter discusses whether the ECT Act was intended to be of application extraterritorially.

c. The Electronic Communications Act 26 of 2002

The ECA seeks to promote and facilitate the convergence of telecommunications, broadcasting, information technologies and other services contemplated in the Act. The provisions of the ECA are open to wide interpretation and can be argued to include innovations such as various forms of cloud computing. Cloud computing technologies form part of information technologies envisaged by the ECA.

Cloud services could be interpreted to fall under the legal definition of electronic communications service.[363] The ECA defines electronic communications service as 'any service provided to the public, sections of the public, the state, or the subscribers to such service, which consists of wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network but excludes broadcasting services'. Cloud computing services include cloud-based communications (Communication as a Service). Apart from cloud-based communications being regulated under the ECA, cloud infrastructures are also regulated in terms of the ECA. The definition for electronic communications facility includes cloud infrastructures and data centres. Further, the objectives of the ECA indicate that cloud computing services are regulated by the ECA.

The ECA provides for the Minister of Communications and Digital Technologies to make policies in relation to the application of new technologies pertaining to the electronic communications services, broadcasting services and electronic communications network services.[364] Pursuant to the ECA, the NDCP was drafted. This chapter reviews how this draft policy seeks to address issues of cloud data jurisdiction, data residency and data governance. From this policy, one can interpret South Africa's approach to data sovereignty as well as data jurisdiction.

d. The Protection of Personal Information Act 4 of 2013

POPIA protects the processing of personal information including personal information stored in the cloud. The definition of processing is broad enough to include cloud data storage. POPIA has put in place eight minimum requirements which must be met when processing personal information. POPIA applies to the processing of personal information entered into a record either by automated or non-automated means.[365] Secondly, POPIA applies where a responsible party is domiciled in South Africa.[366] This means that a cloud service provider in South Africa must process personal information in line with POPIA conditions. Where a responsible party is not domiciled in South Africa, POPIA

[363] Gillwald and Moyo op cit note 237 at 9.
[364] Section 3 (1) (*d*) of the ECT Act.
[365] Section 3 (1) (*a*) of POPIA.
[366] Section 3 (1) (*b*) (*i*) of POPIA.

applies if the responsible party makes use of automated or non-automated means in South Africa.[367] Similarly, POPIA applies to a foreign based cloud service provider who has established data centers in South Africa.

Section 3 (1) (b) (ii) of POPIA creates challenges in respect of foreign cloud service providers processing personal information of South Africans in foreign territory. Unlike the GDPR whose scope applies to any processing of data of European Union citizens and residents by a controller or processor based in the European Union regardless of location, POPIA is found wanting. A locally based cloud service provider with data centers in other countries is not required to comply with POPIA if the personal information of South African citizens and residents is not being transferred from South Africa. Additionally, POPIA does not apply where the responsible party makes use of automated or non-automated means only to forward personal information through South Africa.[368] This would mean that where data servers in South Africa are used when data are in transit, POPIA will not be of application.

Transborder sharing of data is only permitted if certain requirements have been met.[369] A cloud service provider who may want to utilise cloud servers in other jurisdictions can rely on any one of the exceptions under section 72 of POPIA. Where the recipient third party is subject to law, binding corporate rules or binding agreement which provide an adequate level of protection like POPIA conditions, the cloud service provider may transfer the data. Consent of the data subject is another basis for transborder flow of personal information. If the transfer is necessary for the performance of a contract between the cloud service provider and the data subject, then transborder flow of data is permitted.

While POPIA permits transborder data flows, it does not address the question of data jurisdiction. It is not clear under POPIA whether South Africa exercises jurisdiction over cloud data once it has been migrated to a foreign territory. This lack of clarity on data jurisdiction can be a contributory factor to the different approaches to cloud jurisdiction discussed under chapter 4 of this study. Provisions of POPIA are extensive and studies need to be concluded to assess the level of readiness of cloud services for compliance with POPIA.[370] Gillwald suggests that potential users of cloud services need to develop a readiness plan and profile, to advancing the opportunities for innovative uses of internet and other electronic communications resources, where personal data are concerned.[371]

[367] Section 3 (1) (*b*) (*ii*) of POPIA.
[368] Section 3 (1) (*b*) (*ii*) of POPIA.
[369] Section 72 of POPIA.
[370] Gillwald and Moyo op cit note 237 at 41.
[371] Ibid.

IV. CLOUD POLICY IN SOUTH AFRICA

Understanding the current policies relating to ICTs in South Africa is equally important for a study of this nature. Policy documents set out the vision and objectives of the government. In instances where there are gaps in the law, policy helps to shape the formulation of law as well as indicating government's approach on a particular issue. It is pivotal to understand prevailing policy especially in the absence of a robust law regulating cloud computing technologies in South Africa.

Before the draft NDCP was published, scholars argued that absence of policy guidelines was one of the reasons why cloud computing use in South Africa was limited.[372] At the time of writing of this thesis, cloud computing is not covered in the current public sector ICT framework in South Africa. Gillwald and Moyo previously submitted that although there are several regulations and policies, such as the White Paper on Transforming Public Service Delivery, POPIA, ECTA and MISS which affect cloud computing services, there is a need for a dedicated cloud policy.[373] Comparative study shows that cloud first strategies have been adopted by several countries to facilitate the uptake of cloud solutions in the public sector.[374] An effective cloud policy must address issues relating to the security standards for provisioning of cloud computing, vendor compliance requirements, prioritising cloud in the national ICT agenda and recognising cloud as a preferred hosting platform for the public sector.[375]

The ISO/IEC has indicated that when developing policy on cloud computing, considerations should be made on whether policy constrain the storage location of cloud service customer or derived data to a specific jurisdiction.[376] In instances where a policy has jurisdictional constraint, a question should be asked on whether the constraint applies to all data or to an identified subset of data categories.[377] With policy constraints on data location, the question should be whether there are operational exceptions in special circumstances. For example, maintaining the cloud service in operation during a major emergency affecting the local cloud data centre. The ISO/IEC also recommends a policy which mandates a cloud service provider to explain to the cloud customer on how their data will be used.

a. National Development Plan 2030: Our future – make it work

One of the objectives set out in the NDP 2030 is achieving a seamless information infrastructure by 2030. It is expected that the information society and knowledge economy will be more inclusive, equitable and prosperous. The NDP 2030 also recognises that cloud technology has transformed human

[372] Ibid.
[373] Ibid at 48.
[374] Niamh Gleeson and Ian Walden 'Placing the state in the cloud: Issues of data governance and public procurement' (2016) 32 *Computer Law & Security Review* 683 at 684.
[375] Gillwald and Moyo op cit note 237 at 49.
[376] ISO/IEC TR 22678 op cit note 236.
[377] ISO/IEC TR 22678 op cit note 236.

experience and empowered individuals through access to knowledge and markets.[378] An ecosystem of digital networks, services, applications, content, and devices, will be firmly integrated into the economic and social fabric of the country.

b. SA Connect: Creating Opportunities, Ensuring Inclusion. South Africa's Broadband Policy 2013

The objectives of SA Connect are to improve access to broadband in South Africa. The SA Connect policy addresses issues such as cost of broadband, infrastructure sharing, principles of openness and the introduction of policy to promote broadband usage. Though the policy does not deal with cloud computing directly, it recognises that cloud solutions are critical factors for the digital transformation of the public sector. The successful implementation of SA Connect plan is key to the adoption of cloud computing services in South Africa.

c. National Integrated ICT Policy White Paper 2016

The ICT Policy White Paper outlines the overarching policy framework for the transformation of South Africa into an inclusive and innovative digital and knowledge society. It reinforces and extends existing strategies such as SA Connect, the NCPF and the National Information Society and Development Plan. The White Paper notes that it is crucial for South Africa to harness the potential of new technological developments. Any technological advances must further promote the principles of an open internet, while protecting rights to privacy and security. The White Paper submits that South Africa is committed to proactively exploring the impact of new technologies such as cloud computing and IoTs. To promote cloud services in South Africa, the White Paper promotes localisation of data centres and to position South Africa as a data centre hub. Government would monitor developments in relation to cloud computing on an ongoing basis. It would assess the need to set out specific rules, standards, regulations, and guidelines on cloud computing to ensure the objective of an open internet accessible to everyone is fulfilled. Promoting localisation of data centres evidences the approach on data localisation by South Africa. Chapter 5 of this study notes the challenges around data localisation laws and how it may potentially impact negatively on the principles of open internet. The White Paper Policy does not address the issues of data governance and data jurisdiction which is the central discussion of this study.

d. National e-Government Strategy and Roadmap 2017

In 2017, the DTPS published South Africa's e-government strategy and roadmap. The objectives of the national e-government strategy are to ensure citizens' access to quality public services, to reduce the cost of public administration, to harmonise policy environment and establish institutional mechanism that will advance the coordination and facilitation of e-government services. The strategy

[378] NDP 2030 op cit note 324 at 93.

identified that cloud computing services play an important role in e-government[379] and proposed an implementation of a common cloud ICT architecture to enable the implementation of government-to-government services.[380] In successfully achieving e-government strategy, the DTPS will be responsible for, amongst other roles, developing technology roadmaps on leveraging technological innovations such as cloud computing by government.[381]

e. National e-Strategy Digital Society South Africa

In identifying the interventions needed to grow the ICT sector, the e-Strategy proposes the introduction of innovations and support schemes to encourage the private sector to invest in cloud computing and data centres in South Africa.[382] Similar to other discussions on ICT policies, there is no mention of or discussion on data residency and jurisdiction.

f. Draft Digital Futures: South Africa's Digital Readiness for the Fourth Industrial Revolution

In 2020, the National Planning Commission published the South Africa's Digital Readiness for the 4th Industrial Revolution. In this document, the NPC proposed for SITA to come up with a cloud programme. In terms of this programme, the government would operate its private cloud with SITA as the agent responsible for certifying cloud standards for all government departments.[383] SITA would also provide a policy framework to direct cloud computing adoption by government departments.[384]

g. South Africa's Government Public Cloud Ecosystem

SITA has put in place the Government Public Cloud Ecosystem document.[385] This document creates an enabling environment where traditional IT infrastructure services can be offered to different spheres of government in a modernised way. In terms of this document, all cloud data must be hosted on servers within the South African soil. The GPCE also enables partnerships between SITA and cloud

[379] Clause 5 of the e-Government Strategy op cit note 325 at 15.
[380] Clause 10 (h) of the e-Government Strategy op cit note 325 at 24.
[381] Clause 12.2 of the e-Government Strategy op cit note 325 at 29.
[382] National e-Strategy op cit note 325 at 13.
[383] Digital Futures: South Africa's Digital Readiness for the Fourth Industrial Revolution August 2020 at 100. NPC available at https://www.nationalplanningcommission.org.za/assets/Documents/Digital%20Futures_South%20Africa's%20Digital%20Readiness%20for%20the%20Fourth%20Industrial%20Revolution.pdf accessed on 14 October 2022.
[384] Ibid.
[385] SITA Strategic Plan op cit note 228 at 27. In its Strategic Plan, SITA identifies the GPCE as an ecosystem of different clouds for exclusive access by South African government departments that will be owned by government and operated and managed by SITA. SITA launched its new government cloud infrastructure for South Africa which is said to be one of the largest government clouds in the world. The GPCE brings together private and hybrid clouds hosted either within a government data centre or at third party data centre into one single ecosystem from where cloud services can be provisioned through a single cloud suite.

operators such as Microsoft, Amazon and Google. Such partnerships are aimed at creating value for government through the unique service offerings and support provided by such cloud operators.[386]

h. The draft National Data and Cloud Policy

The draft NDCP[387] identifies the potential opportunities presented by the digital economy, the 4IR and emerging technologies in South Africa. The draft policy emphasizes the need for proper policy frameworks to harness the economic and social potential of data and cloud computing. The policy recognizes that data are a driving force for the digital economy and the driver behind 4IR and the enabler of macro-economic development. Due to the huge amounts of data being generated by government, business and academia, cloud computing plays an important role in the management and storage of this data. The NDCP seeks to ensure the implementation of effective cybersecurity, privacy and data and cloud infrastructure protection measures.[388] It also provides for institutional mechanisms for the governance of data and cloud services. The government seeks to support the development of small, medium, and micro enterprises in the provision of cloud computing technologies. Privacy and cybersecurity measures are some of the identified issues informing the NDCP.[389]

The establishment of data centres on South African soil is one of the important objectives identified by this policy. The policy provides that where data has been classified or declared as national critical information infrastructure, such data should be hosted on data centres within South Africa.[390] The policy has been heavily criticized for lack of clarity on its objectives, vague and incorrect references to data-related concepts and terminology.[391] It is not clear whether data generated by private service providers will be included within the definition of critical infrastructure. The policy notes that there is a need for South Africa to develop an open data strategy or framework for the sharing of data, informed by data for good principles, to enable access to relevant data for all South Africans. The policy appreciates the open data strategies adopted by the European Commission, the United Kingdom and Rwanda. The policy references the ICT White Paper recommendation on the development of open government data action plan and manual. The policy notes that non-sensitive government data should be made available to all citizens to enable innovation and the development of digital solutions that can solve societal problems.

The policy is also ambiguous on ownership and control of data. It provides that data generated in South Africa shall be the property of South Africa, regardless of where the technology company is

[386] SITA Strategic Plan op cit note 231 at 32.
[387] National Data and Cloud Policy GN306 GG 44389 of 1 April 2021.
[388] NDCP, section 8.
[389] NDCP, section 10.
[390] NDCP, section 10.4.1.
[391] Shanelle Van der Berg 'Data protection in South Africa: The potential impact of data localisation on South Africa's project of sustainable development' 2021 *Mandela Institute Policy Brief 02 University of Witwatersrand* 1 at 4

domiciled.[392] This objective of the Policy has been met with resistance due to its lack of clarity and failure to comply with legal principles. For instance, the form of state ownership of data has been identified as a novel proposition.[393] Others have, and correctly so, criticised the policy for misunderstanding the nature of personal data as a resource that can be owned by the state and the supply of which can be regulated.[394] Tech companies whose data may end up falling within the definition of critical infrastructure may be compelled to build data centres and build replica back-up data centres in South Africa or rent data centre space from local cloud service providers. This requirement will result in companies not being able to fully leverage the power of cloud computing and gain from the benefits of cloud computing. A requirement for duplicate data centres can also result in an increase in the cost of services as companies may need to incur additional costs in having to meet the security standards for critical infrastructure.

The policy emphasized on the importance of privacy and security in the digital economy. It notes that South Africa is vulnerable to cybercrimes. The policy notes that for South Africa to fully leverage the opportunities presented by 4IR technologies such as data and cloud computing, a fully integrated strategic approach to digital risk management is fundamental, and must be an integral part of national security, planning and response. This can be complemented by a social compact based on PPPs (such as legislators, regulators, service providers and communities) for effective policy implementation and ensuring public trust. To achieve cybersecurity, the policy proposes that the NCPF shall guide the implementation of initiatives and measures. The NCPF shall be reviewed where necessary to ensure it is responsive to the threats and risks associated with digitalization.

Importantly, the policy clarifies that government shall use private cloud for sensitive data in line with the existing government data protection frameworks including laws on access to information.[395] The policy clarifies that the public cloud may be used to store non-sensitive government data. This public cloud is subject to the existing government data protection and access to information framework and legislation, to enable universal access. As far as data generated by other government departments, the policy proposes that government departments and state agencies should develop their own sector specific data classification guidelines informed by the classification framework of the State Security Agency.

[392] NDCP, section 10.4.4.
[393] Under South African law, ownership of data can be through copyright where proprietary rights to datasets are allocated to a person or through the POPIA, where a data subject owns their personal data. State ownership of data is novel and there is no legal basis for the state to own data. Gabriella Razzano 'Data localisation in South Africa: Missteps in the valuing of data' 2021 *Mandela Institute Policy Brief 06 University of Witwatersrand* 1 at 5.
[394] Fola Adeleke 'Exploring policy trade-offs for data localisation in South Africa, Kenya and Nigeria' 2021 *Mandela Institute Policy Brief 09 University of Witwatersrand* 1 at 3.
[395] Promotion of Access to Information Act 2 of 2000 (PAIA).

The policy also recognizes the importance of data security in ensuring that data are kept safe from unauthorised access, alteration, and distribution. The policy notes that South Africa's data protection laws do not take into consideration the context of the digital economy where data are the key drivers of societal and economic development. The policy emphasized the importance of the data protection principles prescribed under POPIA. Processing metadata on personal information shall comply with privacy provisions as contained in POPIA and other data protection legislation. However, commentators have criticized the policy as being irreconcilable with POPIA as government control over data will violate the right to privacy.[396] The policy provides that data generated by government and state entities shall be stored in the High-Performance Computing and Data Processing Centre (HPCDPC). The data are to be subject to security measures as defined by the Minister of State Security to safeguard integrity and security and ensure collective rights over collective data. This policy intervention has been criticized. It is not clear whether service providers contracted by government departments and state entities are expected to use the HPCDPC. It is also not clear whether the government still considers foreign entities to provide cloud computing services or if procurement will be restricted to locally owned companies and SMMEs who will have access to use the HPCDPC.

Data localization policy interventions under the NDCP set out South Africa's position on data jurisdiction. The policy highlights the existing challenge that data centres hosting South African data are in foreign lands while locally stored data are owned by foreign technology companies. The policy notes that given that data storage is not limited to geographical location, consideration should be given to measures that ensure that cross border data transfers do not transgress the national security and privacy protection laws and other related policies and legislation of South Africa. To achieve the localization and regulated transfers of cross border data, the policy proposes that all data classified / identified as critical information infrastructure shall be processed and stored within the borders of South Africa.[397] The policy recognizes the challenges faced by law enforcement in accessing data for crime investigation. To address this challenge, the policy proposes that copies of personal data should be stored in South Africa for law enforcement purposes.[398]

The above discussion on current policies, strategies and visions for the South African government demonstrates four important things. First, cloud computing technologies play a very important role in the economy and in the public sector and there is an expected increase in the adoption and use of cloud computing services. Secondly, there is a lack of clear laws regulating cloud computing technologies and lack of clarity on how to approach the issues of data residency and data jurisdiction. Thirdly, because of the inadequate laws, different government departments have attempted to advocate for a

[396] Van der Berg op cit note 394 at 4.
[397] NDCP, section 10.4.1.
[398] NDCP, section 10.4.3.

certain position around data residency and data jurisdiction. What is important to highlight is that government departments have demonstrated the need to retain some form of control over data hosted on cloud infrastructures either by insisting on use of government cloud infrastructure or insisting on local hosting of cloud data. Fourthly, cloud data jurisdiction, whether for criminal law purposes or for commercial purposes remains unclear under South Africa's ICT related policies. This study will revert to this discussion when unpacking the concerns around data localization.

V. CLOUD SERVICE PROVIDERS AND INTERNATIONAL BEST PRACTICE

As mentioned earlier, a discussion around the terms of service of cloud service providers is important as it demonstrates the important role played by service providers in cybercrime investigations. Cloud service providers can either assist LEA by providing them with access to cloud data of their customers or resist requests from LEA making it difficult for LEA to gain access to relevant cloud evidence. This section is intended to signify the role of service providers in law making both domestically and internationally. It signifies the centrality of service providers in crime investigations and access to cross border data. This discussion provides a practical approach to how different cloud service providers interpret the law around cloud data jurisdiction and the exercise of enforcement jurisdiction over remote cloud data. This discussion will form part of the justifications discussed in chapter 6 for a multistakeholder approach to data jurisdiction. It also indicates the basis for states' fears of the increasing dominance of service providers and their quasi-sovereignty interests.

a. Microsoft

Microsoft plays a very important role in the provision of cloud services not only in South Africa but globally. Most businesses and organisations of varying sizes make use of Microsoft Office 365[399], which is a cloud-based solution. Microsoft is one of the first service providers to collaborate with the public sector in South Africa to find ways of optimising government ICT spend and maximizing the government's return on investment.[400] It has worked with a couple of government departments in providing cloud-based services. For instance, it assisted the Government Pension Administration Agency (GPAA) in migrating to the Microsoft cloud which enabled it to go paperless and introduce self-service facilities to access data.[401]

Microsoft is one of the tech companies which has had a fair share of requests, warrants and court orders issued by different law enforcement agencies to provide access to data of interest. In cases that have been brought before the courts, Microsoft has maintained its position of protecting the privacy

[399] Microsoft Office 365 is a cloud-based solution designed to assist individuals to businesses with a variety of cloud-based solutions such as storage services (OneDrive), data sharing services (SharePoint), email services (Outlook) and video services. Available at *https://www.microsoft.com/en-za/microsoft-365/what-is-microsoft-365* accessed on 12 January 2021.
[400] Microsoft op cit note 328.
[401] Ibid.

rights of its customers. In its white paper, Microsoft acknowledges the importance of digital evidence in the fight against crime. It notes that any laws should provide access to digital evidence while also protecting the fundamental privacy rights and respect the sovereignty of other nations.[402] Microsoft also cautions that unilateral steps taken by governments to access evidence may result in unresolvable jurisdictional conflicts that undermine laws or force companies to choose to disregard the laws of one country to comply with the laws of another.

b. Amazon Web Services

The above discussion has indicated that a cloud service provider may choose the location to store data based on considerations such as efficiency, economic factors, climate, or political conditions.[403] However, with AWS, it is the cloud customer which chooses the region (country) where their content and servers will be located.[404] AWS customers retain control of which regions are to be used to store and process content. The above position may still be valid in instances where an AWS customer offers cloud services to other customers or end users. AWS will not move customer content except as necessary to provide the services initiated by the customer or as necessary to comply with the law or a valid and binding order.[405]

Regarding government access to content, AWS indicates that the local laws where the content is located are important considerations. However, AWS also cautions that there could be other laws from other jurisdictions which may be of application. AWS indicated that typically government agency seeking access to the data of an entity will address any request for information directly to that entity rather than to the cloud provider.[406] As far as its policy on granting government access to data, AWS advises that it does not disclose or move data in response to requests from governments unless legally required to do so to comply with legally valid and binding order, or as is otherwise required by applicable laws.[407] AWS also indicated that their practice is to notify customers where practicable before disclosing their content so that they can seek protection from disclosure unless they are legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services.[408] Though the document is focused on South Africa, AWS does not explain its position in instances where foreign governments seek access to content data hosted within South Africa. What

[402] Microsoft op cit note 208 at 38.
[403] Primary considerations for constructing a data center are having physical space to construct the data centers, good internet connectivity, affordable and availability of energy sources to power the data centers as well as enabling laws and policies. Kesan and Bashir op cit note 262 at 4.
[404] 'Using AWS in the context of South African privacy considerations' (2019) AWS White Paper 1 at 6. Available at *https://d1.awsstatic.com/WWPS/pdf/Using_AWS_in_the_Context_of_South_African_Privacy_Considerations.pdf*, accessed on 2 June 2020.
[405] Ibid.
[406] Ibid at 8.
[407] Ibid at 9.
[408]Ibid at 9.

the document indicates is that for non-US governmental bodies seeking access to data, they must use recognised international processes such as MLATs with the US government to obtain valid and binding orders. One can allude that this might be the similar position with regards to South Africa and data located on South African data centres.

c. Facebook

Facebook's transparency report indicates that it responds to governments requests for data in accordance with applicable law and terms of service.[409] In 2020 alone, Facebook received more than 173,592 requests from LEA across the globe. In South Africa, Facebook received twelve requests and 28 requests for user accounts between the period of January to June 2020. Facebook produced some data in respect of about 58 per cent of the requests made. Apart from receiving requests for data, Facebook also receives requests for content restrictions from governments and civil society organisations. If certain content posted on Facebook does not comply with local laws, it may be restricted or deleted. Depending on the request made, some of the content may be restricted. For example, in April 2017, Facebook received a report about a post which allegedly violated Latvian law on hate speech. After reviewing the report, Facebook removed the items and restricted access in Latvia to the items and notified the responsible users.[410] In the period from January to June 2020, Facebook received over 22 000 content restriction requests.[411] Facebook never received a content restriction request in 2020 in South Africa and only one request the previous year which was a response to a case for defamation. While South Africa employs the frameworks provided by service providers, most African governments hardly do the same.[412]

d. Google

Cloud users of Google products are subject to the terms of service for either Google LLC (a US company) or Google Ireland Limited (an Irish company). Gmail users based in South Africa are subject to Google LLC terms of service.[413] Requests to Google LLC are subject to US laws such as the Electronic Communications Privacy Act (ECPA) and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Most law enforcement agencies request for subscriber information, non-content transactional information and content information from different Google services such as Gmail, YouTube, Google Voice, and Blogger.[414] Any foreign government which seeks to access data from a Google user is obligated to comply with the law. Google LLC considers US laws, the law of the requesting country, international norms, and its internal policies. First, the request for access and

[409] Available at *https://transparency.facebook.com/,* accessed on 12 January 2021.
[410] Available at *https://transparency.facebook.com/content-restrictions* accessed on 13 January 2021.
[411] Available at *https://transparency.facebook.com/content-restrictions* accessed on 13 January 2021.
[412] Halefom op cit 22 at 31.
[413] Available at *https://policies.google.com/terms* accessed on 13 January 2021.
[414] Available at *https://support.google.com/transparencyreport#topic=7294962* accessed on 13 January 2021.

disclosure must be permitted under applicable US law such as the ECPA. Secondly, the LEA must have followed due process and legal requirements if the request were to a local provider or a similar service. This means that LEA must work under the authority of a court issued warrant or a court order for preservation or disclosure of data. Thirdly, Google also considers international norms on freedom of expression and privacy. This means that if the purpose of the request from a government is to censor freedom of expression, such a request may be rejected by Google. Lastly, Google also considers its own policies and whether the request is in line with its terms of service and privacy policies.[415]

Between January to June 2019 alone, Google received a total of 192 diplomatic legal requests. These are requests from government of one country to another through a MLAT.[416] Within that same period, three diplomatic legal requests from South Africa were issued. Google's Transparency Report also shows the requests received in respect of enterprise cloud customers. It defines an enterprise cloud customer as a Google cloud platform account billed through offline invoicing or a G-Suite domain. Between the period of July 2019 to December 2019, Google received a total of 282 requests for disclosure of enterprise cloud customer information. 54 per cent of the requested information was produced.[417]

e. The Reserve Bank of South Africa

Before South Africa published its policy position on cloud and data, the private and public sector responded to cloud adoption by ensuring that it complies with existing mandates. One such sector was the financial services sector. The South African Reserve Bank prepared directives for South African banks which utilise cloud computing services or offshoring of data. In 2018, a Directive was issued by the Prudential Authority to all banks.[418] This directive is to be read together with the Guidance Note 5/2014.[419] The Guidance Note was issued by the Office of the Registrar of Banks. The Guidance Note (note 4.5.) emphasises on the importance of cloud computing initiatives. It requires banks to notify the Office before offshoring material IT business. Banks must notify the Reserve Bank of any outsourcing arrangements, like cloud contracts, which they intend entering which have a bearing on the risk profile of the bank, affects the systems and controls of the bank, is classified by the bank's management as

[415] Available at *https://policies.google.com/terms/information-requests* accessed on 13 January 2021.
[416] Available at *https://transparencyreport.google.com/user-data/overview?dlr_requests=authority:;time:Y2019H1&lu=dlr_requests* accessed on 13 January 2021.
[417] Available at *https://transparencyreport.google.com/user-data/enterprise* accessed on 13 January 2021.
[418] South African Reserve Bank 'Cloud computing and the offshoring of data' Directive D3/2018. SARB available at https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-directives/2018/8749 accessed 12 January 2020.
[419] South African Reserve Bank 'Outsourcing of functions within banks' Guidance Note 5/2014. SARB available at https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-deposit-takers/banks-guidance-notes/2014/6320 accessed 12 January 2020.

being of strategic importance and which has implications for the Reserve Bank's discharge of its supervisory responsibilities.

In terms of this Directive, banks must have in place a formally defined and board approved data strategy and data governance framework. There is a requirement for banks to have a clearly defined cloud computing and offshoring of data policy which is aligned with its business strategy and linked to its risk appetite. Importantly, the oversight of cloud computing and offshoring of data must be incorporated into the governance structures, processes, and procedures within government. Before adopting cloud computing services or offshoring data, banks are required to assess whether the risk involved is within its risk appetite. Banks must always ensure compliance with applicable legislation and regulations when using cloud computing services and before offshoring their data.

VI. CONCLUSION

Cloud computing technologies are steadily becoming mainstream in both the private sector and the public sector. As more people resort to the use of cloud services, LEA will increasingly rely on cloud evidence when investigating crime. It is important that law and policy are developed to address different legal concerns which may arise because of cloud services. One such challenge relates to cloud data jurisdiction. Properly defined laws on data jurisdiction provides clarity to LEA interested in accessing cloud data evidence, cloud service providers who may be obligated to assist in criminal investigations and cloud users whose privacy may be infringed during the investigations. To be well positioned to develop appropriate legal frameworks around cloud computing, it is important for law makers and policy makers to understand the features of the cloud, how the cloud functions and the impact of these salient features on data jurisdiction.

CHAPTER 3: CYBERCRIMES IN THE CONTEXT OF CLOUD SERVICES

I. UNDERSTANDING THE DEFINITIONAL CHALLENGES OF CYBERCRIMES

a. Introduction and objectives

As will be discussed below, this study shall strictly focus on 'true' cybercrimes. True cybercrimes are crimes that will cease to exist if we take away the internet and computer technology.[420] The objectives of this chapter are to get a grasp of the different definitions of cybercrimes and the preferred definitions to be applied and used throughout this study. It elucidates on what is 'cyber' about cybercrimes and clearly distinguishes 'true' cybercrimes from traditional crimes which are committed with the aid of computers. This background discussion adds to the broader dialogue on why traditional substantive and procedural criminal laws designed on the premise of physical territory are not compatible with addressing the challenges of cybercrime. This discussion provides clarity on whether cybercrimes are a category of crime in need of new jurisdictional principles or whether it is better understood by existing jurisdictional principles. The argument is that if the traditional criminal laws can be applied directly to cybercrime, it may not be necessary to develop different set of laws to regulate cybercrimes. This would also mean that the hypothesis for a reformulation of jurisdictional principles may be irrelevant. However, should cybercrimes be considered as a new and innovative set of criminal conduct which warrants technologically suitable criminal laws, then the adoption of new principles is justified.

This chapter 3 also provides a critical analysis of the recently promulgated South Africa's Cybercrimes Act. It discusses how the Cybercrimes Act, together with other criminal laws preceding the Act address cybercrime and unlawful conduct in cyberspace. The chapter also discusses the evolution of cybercrime laws in South Africa. It is important to note that one of the reasons why South Africa's laws on cybercrime slowly evolved was because during the time when the internet was commercialised, South Africa was going through a transition from an apartheid regime to a democratic regime. This meant that the focus of the government was on the development and implementation of a human rights culture.[421] The effect of this was that there was little regard on internet regulation in the South African legal system.[422] At the time, the Roman Dutch law and English law influenced South Africa's common law. The traditional criminal laws particularly common law and the Criminal Procedure Act 51 of 1977 did not criminalise criminal conduct we now call 'internet crimes'.[423] Even

[420] Mark N. Gasson & Bert-Jaap Koops 'Attacking Human Implants: A New Generation of Cybercrime' (2013) 5 *Law, Innovation & Technology* 248 at 250.
[421] Watney op cit note 5 at 338.
[422] Ibid.
[423] Ibid.

at the international level, the general perception was that law and government control were irrelevant to the internet and technology was perceived to regulate the internet.[424]

Whilst there were insignificant legal reforms on cybercrimes taking place in South Africa, at the international level, initiatives were already put in place to address the growing spectre of cybercrimes.[425] At the United Nations level, the General Assembly adopted a resolution which called for member states to intensify their efforts to combat computer crime by modernising their national criminal laws and procedures.[426] In 1995, the UN published the United Nations Manual on the Prevention and Control of Computer-Related Crime. With the increase in the proliferation of the internet and the dependence on the internet, there was a rise in certain internet related crimes and lawmakers noted that common law principles were inadequate to address these new forms of crime. This necessitated the South African government to promulgate the Electronic Communications and Transactions Act.[427] Chapter 13 of the ECT Act criminalised cybercrimes and was the primary legislation criminalising cybercrimes for nearly two decades. The ECT Act was promulgated due to the ineffectiveness of the South African common law to combat cybercrime. At the time when the ECT Act was promulgated, its provisions were lauded as they were responding to the technological landscape at the time. However, as is the norm, technology is not constant but rather changes rapidly. The once lauded ECT Act was no longer adequate to address the technological changes that we have experienced over nearly two decades since its inception. Due to technological changes, the ECT Act was found inadequate and wanting which has resulted in South Africa adopting the Cybercrimes Act. The Cybercrimes Act takes the centre stage as the legislative response to the shortcomings that the ECT Act had. He Cybercrimes Act also introduces harsher penalties, something that was missing in the ECT

[424] Ibid.

[425] From the period between 1983 to 1985, the Organisation for Economic Cooperation and Development (OECD) carried out a study of the possibility of an international application and harmonisation of criminal laws to address cybercrime and abuse. The study resulted in a 1986 report, Computer-related Crime: Analysis of Legal Policy, which surveyed existing laws and proposals for reform and recommended a minimum list of abuses that countries should consider prohibiting and penalizing by criminal law. This list, compiled as a result of a comparative analysis of substantive law around the world, outlined commonly recognised acts, which could constitute a shared basis for the different approaches taken by member states. The Council of Europe Select Committee of Experts on Computer-Related Crime was also involved in discussions on cybercrime issues and subsequently drafted Recommendation 89 (9) which was adopted on 13 September 1989. Goodman and Brenner op cit note 44 at 165. Recommendation 89 (9) emphasised the importance of an adequate and quick response to the newly emerging challenge of cybercrime, which is transborder in nature and therefore requires harmonisation of the law and practice and improved international legal cooperation. It further emphasised the need for international consensus in criminalising and addressing certain computer related offenses.

[426] This resolution was prepared by the 8th United Nations Congress on the Prevention of Crime and the Treatment of Offenders addressed the legal problems posed by cybercrime.

[427] Chapter 13 of the ECT Act criminalises certain conduct as cybercrime. Unauthorised access to data is a cybercrime under the ECT Act.

Act.[428] The Cybercrimes Act deletes sections 85, 86, 87 and 88 of the ECT Act in their entirety. It also substitutes section 89 of the ECT Act.[429]

b. Limitations of the research

A lot of content related crimes and computer related crimes can be categorised as cyber-enabled crimes and cyber-assisted crimes. This study argues that a distinction between cybercrimes from cyber-enabled or cyber-assisted crimes is necessary to avoid exaggerated public policy responses on the criminal justice system which may include unwarranted legislative amendments. This study only focuses on true cybercrimes as defined under part (e) and part (f) of this section. A good example of cyber-assisted or cyber-enabled crime is the crime of child pornography or Child Sexual Abuse Material (CSAM).[430] CSAM is criminalised under different cybercrime legal frameworks such as Article 29 of the African Union Convention on Cybercrime and Data Protection (the Malabo Convention)[431], Article 9 of the Budapest Convention[432], and Articles 13 and 14 of the SADC Model Law on Cybercrime[433]. In South Africa, the Criminal Law (Sexual Offences and Related Matters Amendment) Act 32 of 2007 criminalises various sexual offences including CSAM. The Films and Publications Act[434] also deals with CSAM and obligate internet service providers to monitor information to prevent access to online CSAM. In *Carolissen v Director of Public Prosecutions*, Gamble J and Donen J acknowledged that child pornography is a crime in South Africa, in cases where child pornography is shared via the internet. The study submits that regardless of child pornography or CSAM being criminalised under various legal frameworks on cybercrimes, it is not a true cybercrime.

While cyber-assisted and cyber-enabled crimes have been listed as cybercrimes in terms of various legal frameworks, this study argues that such crimes should not be labelled as true or real cybercrimes. The importance of making a distinction between true cybercrimes and cyber-enabled

[428] Cassim op cit note 41 at 132.
[429] Cybercrimes Act Schedule Laws Repealed or Amended.
[430] It has been argued that the term child pornography suggests a degree of consent on the part of the child and with 'pornography increasingly being normalised, the term may contribute to trivialising and diminishing the seriousness of sexual exploitation and abuse of children.' Equality Now 'Ending online sexual exploitation and abuse of women and girls: A call for international standards' 2021 Equality Now Report 1 at 5-6. Available at https://www.equalitynow.org/ accessed 8 March 2022.
[431] Any activities from the production of child pornography, offering or making available, disseminating or transmitting, procuring, and possessing child pornography are outlawed under the Malabo Convention. Article 29 (3) (a) – (d) of the Malabo Convention.
[432] Title 3 of the Budapest Convention. Article 9 lists several forms of child pornography. The definition of child pornography includes 'pornographic material that visually depicts a minor (a person under 18 years of age) engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct, or realistic images representing a minor engaged in sexually explicit conduct'.
[433] Article 13 of the SADC Model Law on Cybercrime provides a list of different instances which amount to child pornography. This includes the production, offering, distribution, transmitting, possession or access of child pornography. Article 14 of the SADC Model Law on Cybercrime also makes it an offence for anyone who exposes children to pornographic content. This offence is not mitigated whether the child has consented to receiving the pornographic content.
[434] Films and Publications Act 65 of 1996, as amended.

crimes is that traditional laws on criminal procedure can easily be applied to cyber-enabled crimes and cyber-assisted crimes. However, most existing criminal laws cannot apply to cybercrimes. Such a distinction will justify the hypothesis for the reformulation of criminal laws to address unique challenges presented by cybercrimes.

c. A synopsis of the cybercrimes definitions

The Constitution of the Republic of South Africa provides that an accused person has the right to a fair trial, which includes the right not to be convicted for an act or omission that was not an offence at the time it was committed.[435] The Constitution of the Republic is the supreme law of the land and any conduct which is inconsistent with it is invalid. It is important to understand and correctly define cybercrimes. It should be noted that there is no universally agreed definition of cybercrimes as different people define the term differently with some calling it online crime or internet crime. Definitions play a fundamental role in legal discourse, which can be identified in its two basic functions of avoiding ambiguity in interpretation, and warranting the application of a law to a case.[436] Definitions are used to describe the meaning of a term (for example, murder is defined as the intentional and unlawful killing of a human being by another) while others impose or establish a new meaning.[437] For an act or omission to constitute a crime, it must meet the definitional elements of a crime. Snyman provides that 'these definitional elements contain a description of the type of conduct prescribed, the way the act must be performed, the person performing the act, the person or object in respect of which the act must be performed and the place where the act must take place'.[438]

Chapter 13 of the Electronic Communications and Transactions Act did not have clear definitions on cybercrimes and neither does its successor, the Cybercrimes Act. Papadopoulos and Snail note that there is no general definition for cybercrime, but the ECT Act characterises it as 'any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems including any device or the internet or any one or more of them'.[439] Similarly, international cybercrime legal instruments such as the Malabo Convention and the Budapest Convention also omitted to define the term cybercrime. Wall warns that when there is no systematic clarification of the nature of cybercrimes, there is a danger that 'dystopian and often inapt concerns about these crimes can result in misplaced or exaggerated public demands for policy responses from criminal justice agencies'.[440] In other words, lack of clarity on cybercrimes can result in legislative changes and amendments which are

[435] Section 35 (3) (*l*) of the Constitution, 1996.
[436] Fabrizio Macagno 'Definition in law' (2010) *Swiss Bulletin of Applied Linguistics* 197 at 200.
[437] Ibid.
[438] Snyman op cit note 70 at 31. In law, there are different types of definitions that can be ascribed to an act. We can define by providing examples or showing the fundamental characteristics of the concept defined or listing the constituent parts of the denotation, see Macagno op cit note 439 at 200.
[439] Sylvia Papadopoulos and Sizwe Snail *Cyberlaw @ SA IV* 4ed (2021) chapter 13 at 477.
[440] Wall op cit note 13 at 81.

not warranted. Clarity on cybercrimes is also important for the public so that they find out with reasonable ease and in advance how to behave to avoid committing crimes.[441] This is why it is important for this chapter of the study to discuss cybercrimes at length before addressing the question of whether there should be a reformulation of jurisdictional laws applicable to cybercrime.

Different scholars have different definitions for cybercrime. Nduka and Basdeo correctly argue that having different definitions to cybercrimes impact on how different jurisdictions respond to cybercrime and this will hamper knowledge sharing, crime reporting, as well as endangering international cooperation in addressing the growing menace of cybercrime.[442] Chawki et al defines cybercrime as 'unlawful acts wherein the computer is either a tool or target or both'.[443] To understand the meaning of cybercrime involves considering these different types of definitions as well as the list of examples of cybercrimes provided in South African law. Wall argues that 'the term cybercrime in itself is fairly meaningless because it tends to be used emotively rather than scientifically, usually to signify the occurrence of a harmful behaviour that is somehow related to the misuse of computers, with more recent uses suggesting that it is used with regard to networked computers'.[444] Brenner criticises the online dictionary definition for cybercrime as a crime committed on a computer network.[445] Brenner notes that this definition needs to be modified for two reasons. The first reason is that the definition assumes every cybercrime constitutes nothing more than the commission of a traditional crime by non-traditional means.[446] Brenner submits that while most of the cybercrime we have seen to date is simply the commission of traditional crimes by new means, this will not be true of all cybercrime.[447] The second reason why the definition for cybercrime needs to change is that it links the commission of cybercrime with the use of a computer network.[448] Brenner notes that it is possible that computer technology, not network technology, can be used for illegal purposes.[449] To differentiate the two, Brenner argues that a

[441] Snyman op cit note 70 at 38.
[442] Rapuluchukwu Ernest Nduka and Vinesh Basdeo 'The need for harmonised and specialised global legislation to address the growing spectre of cybercrime' (2021) *Southern African Public Law* 1 at 2 - 3.
[443] Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan and Sapna Tyagi Cybercrime, Digital Forensics and Jurisdiction (2015) *Springer International Publishing* 1 at 3.
[444] Wall op cit note 13 at 79. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cybercrime.
[445] Brenner concludes that a better definition of cybercrime is the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order. This definition encompasses both traditional and emerging cybercrimes. It also encompasses any use of computer technology, not merely the use of networked computer technology. Susan W Brenner 'At light speed: Attribution and response to cybercrime / terrorism / warfare' (2007) 97 *The Journal of Criminal Law & Criminology* 379 at 382 and 386.
[446] Brenner ibid at 383.
[447] Ibid.
[448] Ibid.
[449] Ibid.

non-networked computer can, for example, be used to counterfeit currency or to forge documents.[450] The computer is being used to commit an old crime, but it is at least conceptually possible that a non-networked computer could be used to commit a new crime of some type.[451]

Gasson and Koops define cybercrimes as criminal acts committed using electronic communications networks and information systems or against such networks and systems.[452] From Gasson and Koops' definition, it can be identified that there are two types of cybercrimes. On the one hand, the criminals are using electronic communications networks and information systems to commit a crime (for example, using emails to send spam messages or phishing messages). On the other hand, the criminals are targeting and attacking the electronic communications and information systems (for example, distributed denial of service attacks). This definition is similar to the one provided by Baiden who defines cybercrimes as criminal activities where computers, networks or electronic information technology devices are the source, tool, target, or place of crime.[453] Baiden also submits that these cybercrimes are divided into two categories, with one category of crimes being targeted against computer networks or devices and on the other category of crimes being facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.[454]

From these definitions, one can conclude that any device that uses the internet, receives data, collects data, stores data, and sends out communication can be used either as a tool for the commission of a crime (cybercrime) or as a target of a crime (cybercrime). This study submits that such a definition for cybercrime is too broad, and its ambit can ultimately include anything and everything. As we transition into the 4IR, there will be an increase in automation and the use of IoTs. This means that every act will potentially be capable of being committed using electronic communications networks and information systems. Such a broader definition will result in every crime being considered as a cybercrime, which may further complicate the cybercrime legislative landscape and policy considerations as forewarned by Wall.[455]

Others define cybercrime as any crime carried out primarily by means of a computer on the internet.[456] Odumesi defined cybercrimes as crimes that are computer based or traditional crimes that are being committed through computer networks.[457] Murdoch defines cybercrimes as 'any unlawful

---

[450] Ibid.
[451] Ibid.
[452] The authors correctly noted that typical cybercrimes are crimes committed against computer networks and computer systems such as hacking, disseminating viruses and denial of service attacks. Gasson and Koops op cit note 427 at 249.
[453] John E Baiden 'Cyber Crimes' (2011) 1 at 3. Available at http://dx.doi.org/10.2139/ssrn.1873271.
[454] Ibid.
[455] Wall op cit note 13 at 81.
[456] Cassim op cit note 199.
[457] Olayemi John Odumesi 'Combatting the menace of cybercrime' (2014) 3 *International Journal of Computer Science and Mobile Computing* 980 – 991.

conduct involving a computer or computer system or computer network irrespective of whether it is the object of the crime or instrumental in the commission of the crime or incidental to the commission of the crime'.[458] Others have also defined cybercrime as an amorphous term, used to describe any crime that is facilitated or committed using a computer, network, or hardware device.[459] The definition of cybercrime provided by Murdoch is quite different from Gasson, Koops and Baiden's definitions. Murdoch's definition is not focused on computers or computer networks being the tool or the target of the crime. From this definition, cybercrimes could almost mean anything and every unlawful activity that relies on computers and computer networks.

As will be discussed below, common law is an important source of law in South Africa's criminal jurisprudence. Cybercrimes were not defined under common law and in many instances, the existing criminal law principles were extended to criminalise cyber-related criminal conduct. However, in most instances, the traditional definitions of crime were not sufficient to cover cybercrime. To illustrate the differences between traditional crimes and cybercrimes and why we need cybercrime laws, Watney assessed the applicability of the elements of the crime of housebreaking to the cybercrime of unauthorised access.[460] The findings of this assessment was that the definitional elements of the crime could not be met and thus they could not be applied to cybercrimes.[461] This study agrees with Watney's general submission that the definitional elements of a traditional crime cannot be artificially equated to cybercrime.[462]

Most of the definitions on cybercrimes relate to computers. Understanding the ascribed meaning for cybercrimes also includes an understanding of other terms used or associated with crimes. The ECT Act does not have a definition for a computer and neither does the Budapest Convention. The Cybercrimes Act defines a computer as 'any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set

[458] Watney op cit note 5 at 338.
[459] Fernando M Pinguelo and Bradford W Muller 'Virtual crimes, real damages: A primer on cybercrimes in the United States and efforts to combat cybercriminals' (2011) 16 *Virginia Journal of Law and Technology* 116 at 118.
[460] Under criminal law, the crime of housebreaking with intent to commit a crime comprises of the following elements - breaking open; entering of; building or structure; unlawfully; and intentionally. Watney argues that there is no actual breaking open or entering of when we are dealing with cybercrime. The author also argues that the requirement of intent to commit an offense on the premises is also problematic. Murdoch Watney 'The criminal and procedural means of combating cybercrime (part 1)' 2003 *TSAR* 56 at 59.
[461] Ibid.
[462] The element of 'breaking open' may be equivalent to the circumvention of security features on a computer, computer network or electronic data or electronic communication. If someone can access and use the victim's password or encryption key to gain access to the victim's network, then that may be equivalent to the element of 'breaking open. The second element of 'entering of' may be equated to the actual access exercised by a cybercriminal upon circumventing the security features of a computer or network system. Watney op cit note 458 at 59.

instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device'.[463] Computer system has been defined as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'.[464] Computer program means 'data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function'.[465] Gamble J has held that when interpreting the ECT Act, one must examine it within the context in which it was passed and the interrelationship of all provisions.[466]

Contextualising the time when these definitions were suggested, one can extrapolate that reference to computers meant machines that can be instructed to carry out sequences of arithmetic or logical operations automatically via computer programming. Things have changed. We now have smart devices like smart microwave ovens, smart refrigerators and smart wearables which can perform some functions that were previously only performed by traditional computers. The question then becomes whether the definitions of cybercrimes included computer-like smart things and smart devices.

Considering that earlier work on cybercrime was initiated before the extensive use of IoTs, one could argue that the definition of cybercrime was determined by the prevailing technology at that time. One could question whether the definition for computers should be interpreted to include all devices with the ability to connect to the internet or to interconnect with each other. Apart from cloud computing technologies, there is growth in use of artificial intelligence and machine learning. This may also raise additional questions around cyber criminality in instances where AI driven technology has performed an act which falls under the definition of cybercrime.[467] The key takeaway from technological changes is that it will be no surprise that as we come to the end of this new decade, the decade of 2030 might be marred with novel criminal law issues not conceptualised at the time of writing of this thesis and debating of our current criminal laws and literature.

In this light, one can argue that the definition of cybercrimes should be flexible enough to accommodate any technological developments. Incidentally, the question of how technologically

[463] Section 1 Cybercrimes Act.
[464] Article 1 (a) of the Cybercrime Convention. The Cybercrimes Act defines computer system as one computer, two or more interconnected or related computers, which allows these interconnected or related computers to exchange data or any other function with each other or exchange data or any other function with another computer or a computer system. The Malabo Convention defines a computer system as an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or devices.
[465] Section 1 Cybercrimes Act.
[466] *S v Miller & Others* [2015] 4 All SA 503 (WCC) para 42.
[467] Include a short discussion on the recent COE discussions on AI and admissibility of evidence in court proceedings. Alexa, an AI based virtual assistant suggested to a child to electrocute themselves in a game, see Sam Shead 'Amazon's Alexa assistant told a child to do a potentially lethal challenge' https://www.cnbc.com/2021/12/29/amazons-alexa-told-a-child-to-do-a-potentially-lethal-challenge.html accessed 30 December 2021.

neutral our cybercrime laws should be, remain to be answered. One of the important features of the Budapest Convention is that it is technologically neutral.[468] This can be seen in the fact that the most central of terms is computer, which is defined to mean any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. Clough correctly notes that by focusing on the underlying conduct than the technical mechanisms for its commission, the terms of the Convention have been able to keep pace with developments not foreseen or fully appreciated at the time of its drafting.[469]

d. Common law principles applicable to cybercrime

As mentioned in chapter 1, this study seeks to justify why criminal law principles relating to cross border cyber searches must be re-evaluated. The argument is that a failure to reform the jurisdictional principles may likely result in cybercriminals slipping through the jurisdictional loopholes and not being prosecuted. Without adequate jurisdictional principles to govern conduct in cyberspace and clarity on jurisdiction over data in the cloud, the powers of LEA would be significantly limited. Common law is a significant source of law in criminal law jurisprudence in South Africa. A discussion on cybercrime definitions and a re-evaluation of criminal law principles should also consider common law. Before the promulgation of the ECT Act, cyber-related offences were criminalised by relying on common law. Any criminal conduct related to the internet had to be reviewed and criminalised in line with the then existing common law principles and statutory law.

One of the prominent cases which extended principles of common law to a cybercrime offence was the case of *S v Howard.*[470] The court had to decide whether the accused committed the common law crime of malicious damage to property when malicious code loaded by him onto a computer network system belonging to his employer, Edgars Consolidated Stores Ltd caused the erasure of intangible data. The Edgars store suffered losses between nineteen million Rand to 57 million Rand. Question before the court was whether malicious injury to property could be committed where the property was not corporeal. The court held that temporary damage was done to corporeal property consisting of an integral unit of intangible software and tangible hardware. In this case, the court held that the crime of malicious damage to property was committed as the conduct by the accused caused an entire information system to break down. With the advancement in technology, the question that should be addressed is whether common law principles should be extended to prosecute true

[468] Clough op cit note 24 at 376. Paragraph 6 of the Explanatory Report by the Cybercrime Convention Committee (T-CY) on the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence provides that the concepts embodied in the Convention are technology-neutral so that the substantive criminal law may be applied to both current and future technologies involved, and the Convention remains crucial in the fight against cybercrime.
[469] Clough op cit note 24 at 376.
[470] *S v Berend Howard* unreported case no 41/258/02, Johannesburg Regional Magistrates Court.

cybercrimes. If such principles can be extended, one can argue that it may not be relevant or necessary to reformulate laws to address the new reality of cyberspace.

Common law revolves around the principle of *nullum crimen sine lege*, which means there is no crime without a law.[471] Article 7 (2) of the African Charter on Human and People's Rights provides that 'No one may be condemned for an act or omission which did not constitute a legally punishable offence at the time it was committed. No penalty may be inflicted for an offence for which no provision was made at the time it was committed.' Article 22 of the Rome Statute provides that 'a person shall not be criminally responsible under this Statute unless the conduct in question constitutes, at the time it takes place, a crime within the jurisdiction of the court'. The rationale or basis of the principle of legality are the policy considerations that the rules of criminal law ought to be as clear and precise as possible so that people may find out with reasonable ease and in advance how to behave to avoid committing crimes.[472] South Africa has no codified common law principles. Instead of a criminal code, a large collection of authoritative decisions lays down the requirements for every common law crime as well as general criminal law principles.[473] In terms of the common law principle of *ius acceptum*, a court may not find a person guilty of a crime unless the type of conduct he performed is recognised by the law as a crime.[474] At the same time, a court may not create new crimes. In South Africa, the *ius acceptum* must be understood to denote not only common law but also existing statutory law. The *ius acceptum* is anchored in South African law by virtue of section 35 (3) (l) of the Constitution.[475]

The other important common law principle for purposes of this discussion is the *ius strictum*. In terms of this principle, crime creating provisions in both acts of parliament and subordinate legislation must be interpreted strictly.[476] Snyman notes that 'this principle of legality does not mean that a court should so slavishly adhere to the letter of the old sources of the law that common law crimes are deprived of playing a meaningful role in our modern society – a society which in many respects differs fundamentally from the society of centuries ago in which our common law writers lived'.[477] In chapter 4 of this study, a similar argument is raised in the context of jurisdictional principles which are applicable to cloud data. The *ius strictum* principle implies further that a court is not authorised to extend a crime's field of application by means of analogy to the detriment of the accused.[478] This is also provided in terms of Article 22 (2) of the Rome Statute which provides that 'the definition of a crime

[471] For an accused to be found guilty of an offence and sentenced, the type of conduct with which he is charged must have been clearly recognised by the law as a crime, before the conduct took place and without the court having to stretch the meaning of the words and concepts in the definition to bring the particular conduct of the accused within the compass of the definition. Snyman op cit note 70 at 36.
[472] Ibid at 38.
[473] Ibid at 39.
[474] Ibid at 39.
[475] Every accused person has a right to a fair trial, which includes the right to adduce and challenge evidence.
[476] Snyman op cit note 70 at 44.
[477] Ibid at 45.
[478] Ibid

shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favor of the person being investigated, prosecuted, or convicted.' Snyman found it disturbing that the case of *Masiya v Director of Public Prosecutions*[479] amounts to an extension of the scope of the common law crime of rape to include situations not previously included and this undermines the principle of legality.[480]

The common law principle of legality generally does not permit for the development of common law definition of crimes to the extent of creating new crimes. The interpretation of *S v Howard* did not result in the creation of a new form of crime but rather it was a narrow extension of common law principles to the crime. *S v Howard* emphasised on the connection between information systems and the physical property (particularly the point of sales machines which could not be used). One can argue that had the virus not caused tangible harm on the physical property of Edgars, the court might not have arrived at the same conclusion. While common law principle of legality permits us to develop criminal law principles, what is not clear is the extent to which such development of principles is permitted when addressing cybercrimes. Considering the limitations placed by the *ius strictum* and *ius acceptum* principles, common law is not adequate to address novel cybercrime conduct which is not criminalised in terms of statutory law. As will be discussed below, it may be challenging to apply common law principles to criminal conduct such as DDoS attacks.

e. The cybercrime transformational test

Wall developed the transformational test which seeks to distinguish what is and what is not a cybercrime.[481] The importance of discussing this transformational test is to highlight the differences between true cybercrimes and traditional crimes which are being facilitated by computers and the internet. This distinction helps to avoid exaggerated public policy responses on the criminal justice system which may include unwarranted legislative amendments. The transformational test categorises cybercrimes into three generations or categories. The first-generation crimes are cyber assisted crimes.[482] These are the crimes that pre-date the existence of computers, the internet and cyberspace.[483] They consist of the traditional crimes or normal crimes such as murder, theft, robbery or salami fraud.[484]

[479] *Masiya v Director of Public Prosecutions* 2007 2 SACR 435 (CC). The Constitutional Court extended the meaning of rape to include sexual penetration through the anus. Prior to this judgement, penetration of the anus by a penis was considered as indecent assault.
[480] Snyman op cit note 70 at 46.
[481] Transformation test or elimination test. Wall op cit note 13 at 81. David S Wall 'Towards a conceptualisation of cloud (cyber) crime' in T. Tryfonas *Human Aspects of Information Security, Privacy and Trust*, (2017) 529 at 533.
[482] Ibid. Bert-Jaap Koops 'The internet and its opportunities for cybercrime' (2011) 9 *Tilburg Law School Legal Studies Research Paper Series* 735 at 739.
[483] Sagwadi Mabunda 'Is it cyberfraud or good ol'offline fraud: A look at section 8 of the South African Cybercrimes Bill' (2018) 2 *Journal of Anti-Corruption Law* 58 at 61.
[484] Salami fraud occurs when a tiny, unnoticeable fraction of many different bank accounts is sliced off. Clough op cit note 24 at 372.

These crimes can be classified as cybercrimes in circumstances where the use of the computer is an incidental aspect of the commission of the crime and may afford evidence of the crime.[485] Wall correctly argues that if the internet were to be removed from the equation, these activities will still persist and be conducted through alternative forms of communication such as telephone and postal services.[486]

Second generation cybercrimes have a global scope through the advent of computer networks.[487] Without the internet, these second-generation crimes or computer enabled crimes would continue to exist, but their scale would be drastically reduced.[488] These crimes include dissemination of CSAM[489], stalking, criminal copyright infringement and fraud.[490] These crimes can be committed without computers, but the computer is used as a tool to commit the crime.

The third generation consists of 'true' cybercrimes or computer dependent crimes.[491] With these crimes, the computer or computer network is the target of the criminal activity.[492] True cybercrimes includes crimes such as hacking, denial of service attacks (DoS), distributed denial of service attacks (DDoS attacks), website defacement and dissemination of malicious software.[493] These crimes emerged because of the internet and without which, they do not exist. While Wall's description for third generation cybercrime or true cybercrimes provides a better understanding of what constitutes cybercrimes, there is room for improvement on how cybercrimes are defined. For example, the transformational test does not list all the elements of a cybercrime. The proceeding section carefully considers the elements which should constitute cybercrime and proposes the adoption of this definition for cybercrime.

f. Cybercrime redefined

This study agrees with Wall, Gasson and Koops that true cybercrimes are crimes that will cease to exist if we take away the internet or any technology.[494] To provide clarity and certainty on whether certain unlawful conduct should qualify as cybercrime, there is a list of elements which should be met for conduct to qualify as a cybercrime. Providing parameters of what constitutes cybercrimes is important especially when assessing whether existing traditional laws are sufficient to address these cybercrimes or whether it is necessary to adopt new laws. A cybercrime can be defined as an unlawful,

[485] Clough op cit note 24 at 372.
[486] Wall op cit note 13 at 81.
[487] Gasson and Koops op cit note 427 at 250.
[488] Wall op cit note 13 at 82.
[489] Gasson and Koops op cit note 427 at 250.
[490] Clough op cit note 23 at 371.
[491] Wall op cit note 13 at 82 - 83.
[492] Clough op cit note 24 at 371.
[493] Brenner op cit note 452 at 385.
[494] Gasson and Koops op cit note 427 at 250.

intentional act or omission, by a person, by means of or against any technology and which ceases to exist if we take away the technology. The following criminal elements constitutes a cybercrime –

h. unlawful
i. intentional
j. act / omission
k. by a person (natural, juristic or any other)
l. by means of or against any technology, including but not limited to, computers, computer data, computer systems, computer networks, information systems and electronic communication networks
m. ceases to exist if we take away the technology used.

This proposed definition incorporates the definitional elements of a crime in terms of the existing criminal law. The inclusion of a 'juristic person' or 'any other person' in the definition of a person is very important. With artificial intelligence, it is possible for a system to be involved in criminal activities without active or direct involvement of a human being.[495] For example, if an AI based virtual assistant suggests to a child to do something dangerous[496], that can be considered as criminal conduct. Since no human being may be responsible for the conduct, it becomes interesting if the AI can be held criminally liable. This raises other potential legal challenges in wanting to prove the element of intent of an AI based system. At the time of writing of this study, use of AI based systems is on the rise and these issues are still under consideration by lawmakers and policymakers.[497] However, the proposed definition for cybercrime would potentially cover acts by AI based systems. The recent developments in granting a patent to an AI[498] as well as granting citizenship to an AI robot[499] indicate that AI will soon be recognised as a legal person in many jurisdictions. This proposed definition caters for Nduka and Basdeo's submission that the mode of classifying cybercrime should be based on the role of the

[495] A killer drone hunted down a human target without being programmed to do so. Available at *https://www.businessinsider.co.za/killer-drone-hunted-down-human-target-without-being-told-un-2021-5* accessed on 4 June 2021.
[496] Edward Segal 'A crisis is averted after Amazon's Alexa tells child about lethal viral challenge' 28 December 2021 Forbes News.
[497] The first draft of the Artificial Intelligence Convention of the COE was examined during a meeting by the COE Committee on AI held in September 2022. https://www.coe.int/en/web/artificial-intelligence/-/2nd-plenary-meeting-of-the-committee-on-artificial-intelligence accessed 10 October 2022. At the EU level, a draft EU AI Act was published in 2021 and still under consideration. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206%20 accessed 10 October 2022. The AU is also considering the impact of AI and regulation of AI. 473 Resolution on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa - ACHPR/Res. 473 (EXT.OS/ XXXI) 2021. In October 2022, the US released a Blueprint for an AI Bill of Rights. https://www.whitehouse.gov/ostp/ai-bill-of-rights/ accessed 10 October 2022.
[498] The South African Companies and Intellectual Property Commission recently granted a patent where one of the listed inventors was an AI system called Device for Autonomous Bootstrapping of Unified Sentience. Inventorship has always been granted to a natural person. 'Inventorship in the age of artificial intelligence' https://www.adams.africa/intellectual-property/inventorship-age-artificial-intelligence/ accessed 26 December 2021
[499] Saudi Arabia grants citizenship to robot Sofia. https://www.dw.com/en/saudi-arabia-grants-citizenship-to-robot-sophia/a-41150856 accessed 26 December 2021.

computer system in the commission of the offence and broad enough to cover future genres of crime.[500] With technological developments, we can envisage a future where machines and computers will increasingly be involved in criminal activity and we should be able to have such conduct criminalised by inferring liability to either a human being or the AI itself, though at this stage one cannot comprehend how that can be possibly effected. This would require further and independent research. The question that would need to be explored is who will be held criminally liable in case of a cybercrime being committed by an AI machine?

The last part of the definition is particularly important in that it differentiates cyber-assisted and cyber-enabled crimes from true cybercrimes. If the act could continue to exist if the technology used is taken out of the picture, then such a crime will not be a true cybercrime. The reference to technology includes the data that is either processed by the technology itself or the data which constitutes the technology. The Cybercrimes Act provides a good definition for data as the electronic representation of information in any form. This means that data includes, but is not limited to confidential information, sensitive and critical information, personal data and financial data. In *S v Miller,* Gamble J also confirmed that the definition of data under the ECT Act could include the information stored on a cell phone's list of contacts, any notes saved thereon, photographs taken with a cell phone and stored in its memory bank.[501] This definition sounds pretentious and magniloquent and may still require modifications. However, what is important is that it qualifies what is and what is not a true cybercrime.

It has been noted that cybercrime is growing faster in Africa than any other continent[502] and with the increase in access to broadband, there has been an increase in phishing attacks.[503] Interpol's 2023 report[504] on cybercrime trends in Africa identified cyber fraud, cyber extortion, business email compromise, phishing, and as ransomware as the most common forms of cybercrime in Africa. The large potential audience, anonymity and ease of communication facilitate a range of traditional and modern scams, including online sales, advance fee schemes, fraudulent investment opportunities and fraudulent electronic transfer of funds.[505] Advance fee fraud and the Nigerian 419 scams are some of the widely talked about crimes that take place over the internet.[506] Article 8 of the Cybercrime

[500] Nduka and Basdeo op cit note 449 at 4.
[501] Supra note 4734 at para 45.
[502] Cassim op cit note 40 at 126.
[503] Cassim op cit note 41 at 127.
[504] 'African cyberthreat assessment report' INTERPOL 2023. Available at *https://www.interpol.int/en/Search-Page?search=African+cyberthreat+assessment+report*, accessed on 13 April 2023.
[505] Clough op cit note 24 at 373.
[506] Advance fee fraud occurs when offenders send out spam email to random people and hoping someone will be foolish enough to fall for the email. With the Nigerian 419 scam, the perpetrator would claim that they have inherited a large estate in some remote African country and would need the victim to assist them in transferring that money from the country. The victim is lured in by a promise of a reciprocated benefit for the successful transfer of the money. Once the perpetrator has convinced the victim enough, they would demand that the victim

Convention requires member states to adopt legislative or other measures to prevent the loss of property by any input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer system.

In South Africa for example, there has been an increase in cyberattacks within the banking sector, particularly with the increase in SMS fraud and bank fraud.[507] These crimes are the first-generation crimes and the second-generation crimes which should not be classified as true cybercrimes. The SMS fraud scams, and bank scams are crimes which existed before the adoption of computers and internet banking. Mabunda adopts the same line of reasoning when it comes to cyber-assisted crimes. In her argument to discredit why cyberfraud should not be considered as a true cybercrime, Mabunda correctly argued that the mere presence of an internet element in the commission of a fraud, is not enough to elevate the crime to cyberfraud status.[508] Applying Wall's transformational test, if we take away computers and the internet, these scams and fraudulent activities are likely to continue to exist as they have been in existence long before the internet.

There are a fewer reported cases of successful prosecution of true cybercrimes. The factual background in *S v Myeni*[509] reflects how criminal syndicates are exploiting technology to commit crime. In this case, the cybercriminals were able to disable the firewall of some of the municipality's computers which were used to capture, verify, and release payments by using the Winspy software to record all keystrokes, including usernames and passwords. To successfully execute the mission, the criminals unlawfully obtained information required by mobile operators before a SIM swop could be processed on a particular cell phone. Once the SIM swop was processed, all bank notifications would be received by the criminal without the owner of the bank accounts being aware. The court found the accused guilty of unlawful interception of data as well as unlawful use of security measures designed to protect data. The accused were sentenced to fifteen years imprisonment.

This study submits that though scholars correctly noted that there is an increase in cybercrimes due to an increase in internet penetration and internet use, the examples of the crimes discussed are nothing more than cyber-assisted or cyber-enabled crimes and not true cybercrimes. If proponents for

---

pay for the transaction costs for the process and these costs usually keep increasing up until the victim has lost a lot of money and invested so much that they hope to see the deal through. Chawki et al op cit note 441 chapter 9. Onuora, Ogbunude and Uwazuruike op cit note 58 at 5. Tarisayi Andrea Chimuka and Lesedi Mashumba-Paki 'Understanding cyber scams: An assessment of the challenges of law enforcement in Botswana' (2016) *Journal of Sustainable Development in Africa* 111 at 114.

[507] Cassim discusses the SMS fraud case where a Vodacom employee who was working with a syndicate to intercept SMS notifications from banks to their customers. This scam resulted in R7 Million being siphoned off from customers' accounts. Another case related to a fraud that happened in the Mpumalanga Education Department in which huge amounts of money were paid into an unsuspecting woman's account from the Department's bank. Cassim op cit note 41 at 130 -2.

[508] Mabunda op cit note 4901 at 58.

[509] *S v Myeni* 2019 (1) SACR 360 (ECG) para 10.

the adoption of cybercrime specific legislation are not able to correctly identify real cybercrimes in their arguments, it diminishes the exigency and the need for adopting new laws as others can argue that existing statutes can be interpreted to address such crimes. This study submits that a discussion on cybercrime should focus on real and true cybercrimes. To include cyber-enabled and cyber-assisted crimes in the definition of cybercrime may not justify the importance of the reformulation of jurisdictional principles. To justify the importance of developing new principles starts off with understanding that the criminal activity is novel, innovative, and not previously criminalised. If cyber-enabled and cyber-assisted crimes are viewed as cybercrimes, there may not be urgency or need to develop new principles as the existing principles may be applied directly to such conduct. Application of traditional principles and laws to real cybercrimes may result in certain conduct remaining unregulated as will be discussed in the succeeding sections.

It should be noted that another reason why cyber-enabled crime should not be considered as true cybercrimes is that common law definitions can be applied to such crimes without the need to extend the meanings or definitions. Take the crime of fraud for instance. Fraud is defined as the unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another.[510] The same definitional elements of fraud can be applicable to a cyberfraud[511] and this begs the question of whether this crime should be considered as a true cybercrime and whether it should have been included in the Cybercrimes Act. Applying traditional laws to cybercrimes creates the difficulty of trying to convince the judges and magistrates how they fit into the existing laws. While the definition of property could be amended to incorporate computer data, Clough identified that the approach of amending definitions is inadequate.[512] The first problem is that it is difficult to prove the elements of appropriation and intention to permanently deprive when it comes to theft of information.[513] Also, there are other new forms of offences such as Denial of Service attacks which suppress rather than modify or delete data.[514] With these new forms of offences, one cannot rely on interpreting and developing the common law principles to accommodate these new crimes as to do so will be in sharp contrast with the principle of legality.

---

[510] Mabunda op cit note 490 at 60.

[511] Section 8 of the Cybercrimes Bill defines a cyberfraud as any misrepresentation by means of data or a computer program or through any interference with data or a computer program as contemplated in subsection 5(2) (*a*), (*b*) or (*e*) or interference with a computer data storage medium or a computer system as contemplated in section 6 (2) (*a*) which causes actual prejudice or is potentially prejudicial to another person.

[512] Jonathan Clough 'Data theft? Cybercrime and the increasing criminalization of access to data' (2011) 22 *Criminal Law Forum* 145 at 152.

[513] The UK case of *Oxford v Moss* [1978] 68 Cr App Rep 183 is a good illustration of the limitations in applying traditional laws to cybercrimes. In this case, the question was whether the accused had committed the crime of theft. A student accessed an examination paper and read it in advance of an exam. He was charged with the offence of theft. The court held that there could be no theft of information. The Supreme Court had to consider whether confidential information could be the object of the theft and whether the appropriation of the information could amount to fraud.

[514] Clough op cit note 512 at 152.

II. A CRITICAL ANALYSIS OF CYBERCRIMES IN THE CLOUD

a. Introduction

Chapter 1 of this study noted that cybercrime investigations are complex when compared to traditional crimes. With most traditional crimes, the object of the crime is mostly tangible in nature as the main perpetrator is generally physically present during the commission of the crime.[515] The chapter highlighted that traditional crimes are predominantly committed and investigated within the borders of the same country and jurisdiction and choice of law is seldom an issue of dispute.[516] This section of chapter 3 discusses unique cybercrimes which make it difficult for LEA to point out the location of the crime or the location of evidence to prove the crime. By highlighting these unique features, the study seeks to justify why it is important to develop criminal law principles to cybercrime activity.

The above discussion has demonstrated the importance of knowing which crimes qualify to be considered as cybercrimes. The discussion mainly focused on understanding the definitional elements of cybercrimes but did not go into detail explaining the different types of cybercrimes (which is the focus of this section). The study argued that merely because a crime has been committed by the assistance of the internet or computers should not qualify it as a cybercrime. It is important for both legal and policy reasons to distinguish between cyber-enabled or cyber-assisted crimes and true cybercrimes. When certain criminal conduct qualifies as true cybercrime, it requires cyber-specific legislation to regulate such conduct. This would promote the development of our laws to adequately address these cybercrimes.

From a policy perspective, making the distinction between true cybercrimes and other crimes can be beneficial. South Africa's criminal justice system is under immense pressure due to a plethora of reasons including lack of financial resources to investigate crimes. With cybercrimes, there is need to have in place specialised police force to investigate the crimes. Where necessary, forensic investigators can assist in the gathering of electronic evidence. To include any cyber-assisted crime as a cybercrime puts unnecessary pressure and burden on the already skimmed cybercrime specialised task force. The police's specialised unit should only be reserved to deal with true cybercrimes. It is therefore important to discuss these true cybercrimes. Current literature on cybercrimes mainly focuses on discussions around the importance of introducing cyber-centric criminal law statutes instead of reliance on common law and antiquated statutes. The discussion has clarified the importance of adopting new legislative framework since cybercrimes are completely unique and different from traditional crimes as well as the requirements of the principle of legality. However, very few scholars delve into and elucidate on the different types of cybercrimes to justify the need for legal reform.

[515] Watney op cit note 5 at 334.
[516] Ibid.

b. Objectives

The existing literature on cybercrime is centered around legal reform on cyber-enabled and cyber-assisted crimes instead of focusing on true cybercrimes. The preceding section has argued that there is a difference between true cybercrimes and any traditional crime facilitated by the internet and technologies. In this section of chapter 3, the study will discuss in detail the true cybercrimes. To narrow down the discussion, this section of Chapter 3 only focuses on cybercrimes committed in the cloud – these cybercrimes will be referred to as true cloud cybercrimes.[517] The overall discussion of this study relates to cybercrimes, cloud services and jurisdiction. To strategically locate cloud services within the jurisdictional debate, the focus will be on cybercrimes taking place in the cloud.

Chapter 2 of this study succinctly discussed the laws regulating cloud computing services. When people use cloud computing technologies, it is possible for a cybercrime to be committed in the cloud environment under three scenarios. First, cybercrime activity can take place against websites which are hosted in the cloud. Secondly, cybercriminals may launch attacks via emails hosted in the cloud. Thirdly, criminal activity may take place against data which are hosted in the cloud. By discussing true cybercrimes taking place within the cloud environment, the study further demonstrates how cloud computing technologies further compounds the jurisdictional challenges for LEA.

This discussion then provides the backdrop to the major research question which is on establishing jurisdiction in the cloud for gathering of electronic evidence. Knowledgeable understanding of cybercrimes in the cloud is prerogative in understanding how the internet works and the jurisdictional challenges of the internet and the cloud. This discussion ties in with chapter 2 which focused on cloud services and how they distort our understanding of jurisdictional principles. The discussion also nudges a discussion on jurisdictional challenges of the cloud and cybercrime which is the focus of chapter 4 of this study.

c. Cloud webhosting and cybercrimes

i. Website defacement

Website defacement is a type of hacking in which a website's original content is replaced by the attacker's own content.[518] Due to cloud computing technologies, most websites are increasingly being hosted in the cloud. Cloud webhosting is hosting that uses the resources supplied by a shared

[517] While commenting on the Budapest Convention Article 1, Schjolberg and Gerhaouti-Helie argued that countries should consider an appropriate approach to cover criminal activities in virtual worlds and social networks including considering new legislation covering crime through cloud computing. Stein Schjolberg and Solange Ghernaouti-Helie 'A global protocol on cybersecurity and cybercrime: An initiative for peace and security in cyberspace' (2009) *Cybercrimedata* 1 at 4.

[518] C Jordan Howell, George W Burruss, David Maimon & Shradha Sahani 'Website defacement and routine activities: considering the importance of hackers' valuations of potential targets' (2019) *Journal of Crime and Justice* 1 at 2.

server. Website defacement qualifies as a true cybercrime. Following the proposed definition for true cybercrime, when the technology is taken away, this type of criminal conduct will cease to exist.

In 2015, a dating website for individuals interested in engaging in extramarital affairs called Ashley Madison was hacked by criminals who demanded the website to terminate its operations. When the website owners refused, the hackers defaced the website and publicly released the names of its subscribers. These hackers were known as Impact Team.[519] Website defacement is commonly used to protest social and political injustice around the globe, where hacktivists often rely on website defacement to spread their ideological messages to a wider audience.[520] On 28 October 2019, a cyber attacker launched a massive web defacement attack on the nation state of Georgia.[521]

The Cybercrimes Act criminalises website defacement as the unlawful interference with data, a computer program, computer data storage medium and computer system.[522] A person interferes with data or a computer program when they delete data or a computer program or alter data or computer program. The offence also includes rendering vulnerable, damaging, or deteriorating data or a computer program. Unlawful interference extends to rendering data or a computer program meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use of data or a computer program or denying access to data or a computer program.[523] Interference with a computer data storage medium or computer system means to permanently or temporarily alter any resource or interrupt or impair the functioning of; the confidentiality of; the integrity of; or the availability of a computer data storage medium or a computer system.[524] Though the case was decided before the Cybercrimes Act, *Salzmann v S*[525] addressed the crime of intentional interference with data or computer program and the contravention of section 86 (5) of the ECT Act. Snail correctly argues that 'the tailored definition of "interference" provided for by the legislature is likely to ensure legal certainty for the courts when dealing with cyber-interferences of various natures'.[526] The unauthorised interference with computer

[519] Ibid.
[520] Ibid.
[521] More than 15 000 websites were defaced, and 2000 websites were offline for a couple of hours. The websites content was replaced with a photo of the former President of Georgia, Mikheil Saakashvili, with the words "I'll be back". 'Georgia hit by massive cyber-attack' BBC News Available at *https://www.bbc.com/news/technology-50207192* accessed on 28 December 2019.
[522] Sections 5 and 6 Cybercrimes Act.
[523] Section 5 (2) Cybercrimes Act.
[524] Section 6 (2) Cybercrimes Act.
[525] *Salzmann v S* (755/18) [2019] ZASCA 145 (13 November 2019).
[526] Sizwe Snail ka Mtuze 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) *Obiter Law Journal* 536 at 549.

data or computer systems is also addressed in terms of Article 29 of the Malabo Convention[527], Article 5 of the Budapest Convention[528] and Article 7 of the SADC Model Law on Cybercrime.[529]

ii. Denial of service and Distributed Denial of Service attacks

Denial of service and distributed denial of service attacks are true cybercrimes. From the statistics provided earlier on in this study, over half of the world population are internet users. Criminals understand the role that websites play, and they tend to exploit websites through launching denial of service attacks. With a DoS attack, a criminal targets a computer system by overwhelming it with a high volume of information requests which could include providing access to a particular website.[530] Besides a Denial of Service attack, criminals also launch Distributed Denial of Service attacks. With a DDoS attack, instead of relying on one computer system, a cybercriminal would often rely on several infected machines or botnets[531] which all send high volumes of information requests to the same target system, and they are commanded like an army.[532]

One of the first DDoS attacks happened in February 2000 against high-profile websites such as Amazon.com, eBay, and CNN.[533] Since this incident, DDoS attacks have increased in frequency and sophistication.[534] South African businesses are continuously being subjected to DDoS attacks. In

[527]Article 29 (1) of the Malabo Convention provides that 'State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to (a) gain or attempt to gain unauthorised access to part or all of a computer system or exceed authorised access; (b) gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such as offence'.

[528] Article 4 of the Budapest Convention provides that 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right'. Article 5 provides that 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data'.

[529] Article 7 of the SADC Model Law on Cybercrime provides that 'A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts:
(a) damages or deteriorates computer data; or
(b) deletes computer data; or
(c) alters computer data; or
(d) renders computer data meaningless, useless or ineffective; or
(e) obstructs, interrupts or interferes with the lawful use of computer data; or
(f) obstructs, interrupts or interferes with any person in the lawful use of computer data; or
(g) denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.'

[530] Watney op cit at 5 at 335.

[531] Botnets are hijacked computers that are used to target system with many requests at the same time. Watney op cit note 5 at 335.

[532] Available at *https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18255&view=map* accessed on 27 December 2019.

[533] Susan W Brenner 'Law in an era of pervasive technology' (2006) 15 *Widener Law Journal* 667 at 772.

[534] In 2017, an 18-year-old hacker known as Jesse S launched a DDoS attack on a Dutch bank and was convicted to 10 hours of community service. After 4 months, he launched another attack which was so severe that initially

November 2019, a massive DDoS attack was launched which targeted ISPs such as Cool Ideas, Axxess, Liquid Telecom and WebAfrica.[535] When a DDoS attack takes a commercial site offline, the company is harmed because it loses actual revenue, revenue opportunities and opportunities for advertising and public relations.[536]

Brenner argues that, while DDoS attacks inflict 'harm', they are not criminal, in a traditional sense. Her argument is that the attacker merely shuts down a website but takes nothing which means he commits neither theft nor extortion.[537] She further argues that despite the attacker interrupting the website, it is left undamaged or destroyed. As such, we cannot construe the activity of the attacker as damaging or destroying property or vandalism.[538] DDoS attacks are a good example of potential criminal conduct which cannot be criminalised in terms of South Africa's common law. Merely sending traffic to a website may not amount to criminal activity in terms of common law. While the Cybercrimes Act does not specifically mention DDoS attacks, a statutory interpretation of the act points out that such attacks are criminalised.

The Cybercrimes Act provides that any person who unlawfully and intentionally interferes with data or a computer program is guilty of an offence.[539] As mentioned earlier, the Act defines 'interferes with data or a computer program' to mean to permanently or temporarily render data or a computer program meaningless, useless or ineffective or obstruct, interrupt or interfere with the lawful use of data or computer program or deny access to data or computer program.[540]

Section 6 of the Cybercrimes Actprovides that any person who unlawfully and intentionally interferes with a computer data storage medium or a computer system is guilty of an offence. It defines 'interferes with a computer data storage medium or a computer system' to mean temporarily or permanently interrupt or impair the functioning of, the confidentiality of, the integrity of and the availability of a computer data storage medium or a computer system.[541] If a person intentionally floods website traffic of another with the intention of rendering the website inaccessible or slow, they will be

people thought the attack was from Russian hackers. 'The crime and punishment of DDoS attacks' Business World 17 December 2018.

[535] Jan Vermeulen 'Massive DDoS attacks – South African Internet providers crippled' My Broadband 25 November 2019. Available at *https://mybroadband.co.za/news/internet/329539-massive-ddos-attacks-south-african-internet-providers-crippled.html*, accessed on 27 December 2019. Admire Moyo 'Liquid Telecom, Webafrica hit by DDoS attacks' IT Web 28 October 2019 Available at *https://www.itweb.co.za/content/GxwQDM1A339MlPVo*, accessed on 27 December 2019.

[536] Brenner op cit note 536 at 773.

[537] Ibid.

[538] Ibid.

[539] Section 5 Cybercrimes Act.

[540] Section 5 (2) (*d*), (*e*) and (*f*) Cybercrimes Act.

[541] Section 6 (2) (*b*) Cybercrimes Act.

committing a crime of Denial of Service. Upon conviction, a person can be sentenced to 10 years imprisonment or to both pay a fine and be imprisoned.

iii. Ransomware attacks

Closely linked to DDoS attacks are ransomware attacks. Ransomware attacks pose a great security threat because they can incapacitate the core business functions of a system.[542] As the name suggests, a ransomware attack is an attack motivated by money as the criminals are interested in extorting money from their victims. Recently South Africa's major city of Johannesburg was subjected to a ransomware attack. The criminals managed to access public facing data which resulted in the city suspending its online services.[543] In September 2021, the DOJ was also hit by a ransomware attack.[544] Before the advent of cryptocurrencies, cyber-extortionists used to demand victims to pay the ransom via money transfer agencies or deposit the money directly into specified bank accounts. With the anonymity of cryptocurrencies[545], most criminals who launch ransomware attacks demand ransom payment in cryptocurrencies particularly Bitcoin.[546] Zimba and Chishimba submit that a successful ransomware campaign involves 3 main facets. The first one is an effective encryption technique which makes it possible to hold data files hostage. The second facet is having an effective infection vector methodology that ensures that the ransomware payload is delivered to the victim. The third one is a resilient infrastructure which is the centre of operation of the attack campaign.[547]

Ransomware attacks are criminalised under the Cybercrimes Act. Cyber extortion is a crime under South African law. Cyber extortion happens when a person commits or threatens to commit any

[542] Aaron Zimba and Mumbi Chishimba 'On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems' (2019) 4 *European Journal for Security Research* 3.
[543] Shortly after the City of Johannesburg was subjected to ransomware attacks, most South African banks were also subjected to a similar attack. South African Banking Risk Information Centre (SABRIC) report. The City of Johannesburg attacks started with a ransom note which was delivered via email to both unattended as well as staff e-mail addresses, all of which were publicly available. Malibongwe Dayimani, Soyiso Maliti and Genevieve Quintal 'SA now hostage to cyber ransom' Sunday Dispatch 26 October 2019 page 5. In July 2019, City Power came under a ransomware attack that prevented thousands of prepaid customers from buying electricity. Shaun Smillie 'Hackers hold city, banks to 'ransom'' Saturday Star 26 October 2019.
[544] 'Update on progress in restoring justice services following ransomware attack'. Department of Justice Media Statement 21 September 2021. https://www.justice.gov.za/m_statements/2021/20210921-IT-Systems-RestorationProgress.pdf accessed 19 January 2022.
[545] Cryptocurrencies are used to facilitate a variety of cybercrime as they offer the level of anonymity required by cybercriminals. Eveshnie Reddy and Anthony Minnaar 'Cryptocurrency: A tool and target for cybercrime' (2018) *Acta Criminologica: Southern African Journal of Criminology* 71 at 74 – 75.
[546] In the case of the City of Johannesburg, the criminals who went by the name Shadow Kill Hackers demanded payment of 4 Bitcoin which was equivalent to half a billion Rand at the time. Catalin Cimpanu 'City of Johannesburg held for ransom by hacker gang' NET innovation 25 October 2019. Available at https://www.zdnet.com/article/city-of-johannesburg-held-for-ransom-by-hacker-gang/ accessed on 14 October 2022. Criminals also attacked a petroleum company in Mexico. On 10 November 2019, a state-owned oil company in Mexico Petroleos Mexicanos (Pemex) was attacked by cybercriminals who were demanding 565 Bitcoin ($4.9 Million). The cybercriminals claimed to have gathered sensitive data from the Pemex network. Ionut Arghire 'Mexican oil company Pemex hit by ransomware' Security Week 12 November 2019. Available at https://www.securityweek.com/mexican-oil-company-pemex-hit-ransomware accessed on 14 October 2022.
[547] Zimba and Chishimba op cit note 539 at 12.

offence contemplated in section 3 (1), 5(1), 6(1) or 7 (1) (a) or (d) of the Cybercrimes Act for the purpose of obtaining any advantage from another person or compelling another person to perform or to abstain from performing any act.[548] Section 3 (1) of the Cybercrimes Act provides that any person who unlawfully and intentionally intercepts data is guilty of an offence. Section 5 (1) of the Cybercrimes Act provides that any person who unlawfully and intentionally interferes with data or a computer program is guilty of an offence. It is also an offence to unlawfully and intentionally interfere with a computer data storage medium or a computer system.[549]

Section 7 (1) (a) and (d) of the Cybercrimes Act criminalises the unlawful and intentional acquisition or use of a password, access code or similar data or device for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6 (1), 8 or 9 (1).[550] If a person unlawfully infiltrates a computer program or data and demand the payment of a ransom in order to restore the computer system or in order not to share the data collected from the computer system, computer storage medium or computer network, the person will be committing the offense of cyber extortion. The penalty for cyber extortion is a sentence, as provided for in section 276 of the Criminal Procedure Act, that a court considers appropriate and within that court's penal jurisdiction.[551]

d. Cloud based email hosting and cybercrimes

i. Cloud Phishing

Phishing is a social engineering scam devised by criminals with the intention of luring people into sharing personal information with a cybercriminal. The cybercriminal usually sends out the phishing email or unsolicited communication (spam) under the guise of being a reputable company or person.[552] Cybercriminals can come up with legitimate and compelling reasons which can persuade someone to open and read emails such as claiming to be from shipping companies and banks, asserting that there is a problem with the company's shipment or bank account.[553] Once the victim's personal data are disclosed or captured, they can then be used by the cybercriminal for a variety of illicit purposes, including fraud, identity theft and for gaining unauthorised access to a computer network.[554] The sending out of a phishing email is not a criminal offence *per se* in terms of the South African law. The only moment when it becomes a criminal offence is if the intention is to gain access to the passwords and access codes of the victim or other information about the victim. Section 7 of the Cybercrimes Act criminalises the acquisition, possession and use of a password, an access code or similar data or device for purposes of unlawfully accessing data, computer program, computer data storage medium and

[548] Section 10 Cybercrimes Act.
[549] Section 6 Cybercrimes Act.
[550] Section 7 Cybercrimes Act.
[551] Section 19 (4) Cybercrimes Act.
[552] Pinguelo and Muller op cit note 466 at 131.
[553] Ibid.
[554] Ibid.

computer system. The section also criminalises the unlawful interception, and interfering with data or computer program, computer data storage medium or computer system.

A person convicted of the offence of phishing can be liable to a fine or to imprisonment for a period not exceeding ten years or to both a fine and such imprisonment.[555] Phishing can also be prosecuted under the common law offences of theft and fraud. However, phishing qualifies as a true cybercrime since it is only facilitated by means of email communications. The maximum penalty would depend on which court adjudicates the case. Where the magistrates court prosecuted the offender, the penalty could be a fine or imprisonment for a period of fifteen years in terms of the penal jurisdiction.

ii. Dissemination of malicious software

Dissemination of malicious software is one of the crimes identified as true cybercrimes. The crime of dissemination of malicious software can both be discussed as a cloud crime and cloud-based email crime. To avoid repetition, this crime will be discussed in relation to cloud-based email hosting. There are several malicious software (malware) which include viruses, trojan horses and worms. The 'Love Bug Virus' incident discussed earlier is one example of dissemination of malicious software. A virus is 'a piece of programming code usually disguised as something else that causes some unexpected and undesirable event and which is often designed so that it is automatically spread to other computer users'.[556] Viruses can be disseminated or contracted by the exchange of various media or by receipt in an email.

A worm is a type of malicious software that situates itself in a computer system in a place where it can do harm. Recently, the WannaCry ransomware attack was another defining moment in cybersecurity and cybercrime history.[557] The difference between a virus and a worm is that the virus must be activated by the user (usually through clicking an email link) whereas a worm gains access to the computer and searches for other internet locations, infecting them in the process.[558] A trojan horse

[555]Section 19 (2) Cybercrimes Act.
[556] Sizwe Snail 'Cybercrime in the context of the ECT Act' (2008) *JBL* 63 at 65. Reinhardt Buys 'Love Hurts' (2000) *De Rebus* 33.
[557] The WannaCry ransomware attack was a global epidemic that took place in May 2017. This ransomware attack spread through computers operating Microsoft Windows. User's files were held hostage, and a Bitcoin ransom was demanded for their return. https://www.kaspersky.co.za/resource-center/threats/ransomware-wannacry accessed 28 December 2019. WannaCry encrypted 230 000 computers in over 150 countries within 4 hours. The attackers were demanding the payment of a ransom in Bitcoin for them to unencrypt the data. The United Kingdom National Health System (NHS) almost came to a standstill and up to 70,000 devices including computers, MRI scanners, blood-storage refrigerators and theatre equipment were affected. Organisations across the world which confirmed to have been affected by WannaCry included Boeing Commercial Airplanes; FedEx; Guilin University of Aerospace Technology; Ministry of Internal Affairs of the Russian Federation; Ministry of Foreign Affairs (Romania); Renault; and Telkom (South Africa). https://en.wikipedia.org/wiki/WannaCry_ransomware_attack accessed 28 December 2019. Norton Rose Fulbright 'WannaCry ransomware attack summary' https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/. Accessed 28 December 2019.
[558] Snail op cit note 559 at 65.

is a destructive computer programme disguised as a game, a utility or application. At face value, a trojan horse appears to be a useful application or useful computer program, while in fact, it is causing damage in the background.[559]

Before the promulgation of the Cybercrimes Act, the ECT Act was criticised for not clearly setting out the elements of dissemination of malicious software. Snail argued that as the court has an inherent power to develop the common law, the creation and or the dissemination of the dangerous codes could have been prosecuted successfully as malicious damage to property.[560] The requirements of malicious intent and fault could easily be attributed in the form of *dolus directus, dolus indirectus* or even *dolus eventualis*.[561] He further notes that conscious negligence (*luxuria*) could also be relied upon where the author of such a program failed to take precautions to make sure that it did not fall into the public domain (even if it were for research purposes).[562]

Dissemination of malware is criminalised under sections 5 and 6 (2) of the Cybercrimes Act. The Cybercrimes Act succinctly defines interference with data or computer program to include rendering vulnerable, damage or deteriorate data or a computer program or render data or a computer program meaningless, useless, or ineffective.[563]

e. Cloud data and cybercrime

i. Cloud Hacking

When the term hacking was originally introduced, it referred to the technique that was used by IT personnel who were always on the lookout to find computer shortcuts that made computing tasks quicker.[564] Hacking is defined as gaining unauthorised access to a computer system, programs or data.[565] Hackers sometimes crack into government or business networks for profit, for sport or for bragging rights.[566] Different branches of the South African government have been subjected to hacking attacks. The SAPS was hacked and criminals released details of thousands of whistle-blowers and victims. The State's Government Communication and Information System was also compromised.[567] With attack tools becoming increasingly sophisticated and user-friendly, hacking remains a major concern for systems administrators. Hacking makes use of various botnets.[568] Botnets are collections of software agents that run automatically to commandeer massive numbers of computers to allow cybercriminals

[559] Ibid at 66.
[560] Ibid.
[561] Ibid.
[562] Ibid.
[563] Section 5 (2) (*c*) and (*d*) Cybercrimes Act.
[564] The first and original computer hackers emerged in 1960 at the Massachusetts Institute of Technology (MIT). Baiden op cit note 460 at 4.
[565] Pinguelo and Muller op cit note 466 at 132.
[566] Ibid.
[567] Snail op cite note 533 at 537.
[568] Ibid.

to conduct large scale malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others.[569] The growth of botnet hacking is troublesome for both government and business as botnets are the launch pad for much of today's criminal activity on the internet and in many ways, they are the perfect base of operations for computer criminals.[570]

One of the famous hacking cases is that of the *U.S. v. Gorshkov.*[571] The facts of this case raised questions around the exercise of enforcement jurisdiction over data in a different country. Chapter 4 of this study discusses the legal issues relating to LEA unilaterally accessing electronic evidence in foreign jurisdiction as well as the justification of the use of network investigative techniques as applied by the FBI in *US v Gorshkov*. For this part of chapter 3, it suffices to note that hacking as a crime has been criminalised for over 2 decades to date. Gorshkov and Ivanov were cybercriminals who hacked into US companies. It is interesting to note that regardless of hacking having been criminalised, there are still a few convictions to date. One of the identified reasons for fewer cybercrime convictions relate to lack of enforcement jurisdiction which permits LEA to gather and access electronic evidence.

South African law criminalises hacking. Before the Cybercrimes Act, courts used to rely on the cybercrime provisions set out under the ECT Act. The repealed section 86 (3) of the ECT Act provided that the unlawful selling, producing or distribution of any device including a computer program or a component which is designed to overcome security measures for the protection of data is an offence. The repealed section 86 (4) of the ECT Act further provided that a person who utilises any device or computer program mentioned in section 86 (3) to unlawfully overcome security measures designed to protect such data or access thereto is guilty of an offence. The court in *Okundu v S*[572] found the accused guilty of contravening section 86(1), (3) and (4) of the ECT Act. The accused had intercepted data belonging to cards of lawful cardholders and encoded it on magnetic strip of a Visa debit card.[573] The court found that-

[569] Ibid.
[570] Pinguelo and Muller op cit note 466 at 133.
[571] The FBI were investigating Gorshkov and Ivanov, two Russian citizens. While in the US, the FBI managed to hack into the suspect's computers in Russia without obtaining a search warrant to do so. After being indicted for computer crime, Gorshkov approached the court and argued that the evidence collected was illegally obtained as it violated the Fourth Amendment and/or violated Russian law. The district court denied the motion. It held that the Fourth Amendment did not apply because it does not encompass extraterritorial searches directed at non-US citizens. The court considered the circumstances of the search and seizure and held that even if the Fourth Amendment did apply, actions of the FBI were justified. The court also held that the actionS of the FBI did not violate Russian law and if they did, it was no basis for suppressing evidence in a U.S. proceeding. *U.S. v. Gorshkov* 2001 WL 1024026 (W.D.W.A. May 23,2001) Russian authorities regarded the actions of the FBI as a clear violation of Russian sovereignty and subsequently charged the FBI agent primarily responsible for the intrusion with hacking and asked that he be turned over for trial. U.S. authorities did not complied. Susan Brenner and Koops op cit note 61 at 21 – 22.
[572] *Okundu v S* (CA&R117/16) [2016] ZAECGHC 131 (22 November 2016).
[573] *Okundu v S* supra 572 at para 12.

'When the appellant used the Visa credit card at Pick 'n Pay and Vodashop he unlawfully and with the intention of defrauding the banks, made a misrepresentation to the banks that he was the lawful cardholder. Such misrepresentation caused prejudice to the banks and/or the lawful cardholders. All the elements of fraud having been satisfied, the appellant was correctly convicted of fraud. The appellant must have known that the banks take security measures to protect their clients' data. The only way for him to make the purchases at Pick 'n Pay and Vodashop was for him to use the Visa credit card in order to unlawfully overcome the security measures designed by the banks to protect the lawful cardholders' data. He accordingly committed the offence envisaged in section 86 (4) of the ECTA.'[574]

The provisions of section 86 of the ECT Act were discussed in the case of *R v Douvenga.*[575] In this case, the question was whether the accused was guilty of a contravention of section 86 (1) of the ECT Act. The accused intentionally and without permission, gained entry to data which she knew was contained in confidential databases and contravened the provision by emailing this data to her fiancé. The accused was found guilty of contravening section 86 (1) of ECTA and sentenced to a fine of R1 000 or imprisonment for a period of three months. In *Mgoqi v S*, the appellant was accused of the various offences including fraud of people's credit cards. The appellant (accused) captured data encoded on the magnetic strips of bank cards using a skimming device while pretending to offer assistance to lawful cardholders effecting transactions at ATMs.[576] The charge against the accused brought before the Magistrate's Court was the contravention of section 86(1) of the ECT Act in that the accused unlawfully and intentionally gained access to or intercepted data such as client information (encoded on magnetic strips of bank cards) of various international financial institutions.[577] The appeal court found that the Magistrate's Court had erred and the evidence submitted by the expert witness was not reliable. Section 86 of the ECT Act was replaced by section 3 of the Cybercrimes Act.[578]

While interpreting section 86 of the ECT Act, the court in *S v Miller* held that the word permission as provided in section 86 (1) of the ECT Act applied in situations where the accused surrenders their cellphone to police without putting a password on the phone or in situations where the accused provides their password or PIN to the police officer. It is important to note that Gamble J failed to consider and discuss the extent of that permission. Considering that cell phones are now new portals

[574] *Okundu v S* supra 572 at para 13.
[575] *R v Douvenga District Court of the Northern Transvaal,* Pretoria, case no 111/150/2003, 19 August 2003 (unreported case).
[576] *Mgoqi v S* [2020] ZAECGHC] 33 / Case No, CA&R 46/2017 para 2.
[577] *Mgoqi v S* supra 576 at para 3.
[578] Snail op cit note 533 at 542.

to people's digital life and a lot of data accessible via cell phones are hosted in the cloud, the learned judge missed an opportunity to address the parameters of this permission.[579]

Though the matter was not before a criminal court, the judge in *Harvey v Niland*[580] acknowledged the crime of hacking. In this case, a member of a close corporation was suing a former member for breach of his fiduciary duties in the close corporation. To prove this breach, the applicant used the Facebook password of the respondent without the permission of the respondent. Upon accessing the Facebook account of the respondent, the applicant came across a lot of evidence to support his claims and this evidence was attached to his founding affidavit. The court's *obiter dictum* was that the applicant acted unlawfully in terms of the ECT Act by accessing the respondent's Facebook communications and his act probably constituted criminal conduct.[581] Since this was a civil case, the court did not go into detail in discussing the crime of hacking. What is important to note from this judgement is that our courts recognise that accessing social media accounts, computer programs and computer networks without the authorisation of the owner of the accounts and programs is a criminal offence. In *S v Myeni*[582], the criminals unlawfully used a software called Winspy to overcome security measures designed to protect computer names and passwords of accounting personnel at Koukamma Municipality. The court found the accused guilty of the crime of hacking in terms of section 86 (1) and 86 (4) of the ECT Act.

The Cybercrimes Act criminalises different types of hacking. Unlawful and intentional access to data, computer program, computer data storage medium and computer system is an offence.[583] The unlawful and intentional interception of data including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system is an offence.[584] Similar provisions on unlawful access to data are contained in the Budapest Convention. Article 2 of the Budapest Convention provides that 'Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining data

[579]This judgement entails that police officers can access any electronic evidence accessible from a mobile phone. Where the electronic evidence is held in the cloud hosted in a different country, South African police can still access the evidence as per this decision. This raises jurisdictional challenges and problems identified in chapter 1 and which will be succinctly addressed in chapter 4 of this study. *S v Miller* supra 464 at para 57.
[580] *Harvey v Niland & Others* 2016 (2) SA 436 (ECG).
[581] *Ibid* para 48.
[582] *S v Myeni* supra note 509.
[583] Section 2 Cybercrimes Act.
[584] Section 3 Cybercrimes Act.

or other dishonest intent, or in relation to a computer system that is connected to another system'. The Budapest Convention also criminalises the illegal interception of computer data under Article 3.[585]

To unlawfully access any data, criminals usually make use of hacking tools which can be software tools, hardware tools, passwords and access codes. The Cybercrimes Act criminalises the intentional use and possession of any software or hardware tools for the purposes of unlawfully accessing, intercepting, and interfering with data.[586] It also criminalises the unlawful acquisition, possession, provision, receipt or use of passwords, access code or similar data or device.[587] The Cybercrimes Act also criminalises the misuse of devices. Section 4 provides that any person who unlawfully and intentionally uses or possesses any software or hardware tool for purposes of contravening the provisions of sections 2(1) or (2), 3(1), 5(1), 6(1) and 7 (1) (a) or (d) is guilty of an offence. Most hackers either possess or use hacking tools to unlawfully gain access into computer systems and networks without authorisation. Closely related to possession of hacking tools is the offence of unlawfully and intentionally acquiring, possessing, providing to another person or using a password, an access code or similar data or device for purposes of contravening the provisions of section 2 (1) or (2), 3 (1), 5 (1), 6(1), 8 or 9 (1).[588] Password, access code or similar data or device includes a secret code or pin, an image, a security token, an access card, any device, biometric data or a word or a string of characters or numbers used for financial transactions or user authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.[589]

The Cybercrimes Act contains similar provisions as those in the Budapest Convention. Any misuse of devices is listed as a cybercrime offence in terms of Article 6 of the Budapest Convention. Making available software, hardware, or computer access codes with the intent that it be used for the purpose of committing illegal access or interception of data or system interference constitutes a cybercrime. Producers of programs creating trojan horses or hacking software can be held liable and so can their distributors, importers and other parties.[590] Polanski correctly noted that individuals or corporations behind websites that make freely available software keys, key-generators and cracks are also cyber offenders under the Convention.[591] The Convention outlaws the mere possession of such

[585] Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. Article 3 Cybercrime Convention.
[586] Section 4 Cybercrimes Act.
[587] Section 7 Cybercrimes Act.
[588] Section 7 (1) Cybercrimes Act.
[589] Section 7 (3) Cybercrimes Act.
[590] Paul Przemyslaw Polanski 'The internationalization of internet law' in Klabbers, Jan and Sellers, Mortimer *The Internationalization of Law and Legal Education* (2008) chapter 10 at 204.
[591] Ibid.

software, hardware or access codes with the intent to illegally accept, intercept data or cause data or system interference.[592]

Apart from the Cybercrimes Act, hacking is also criminalised under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA Act).[593] Section 2 of the RICA Act provides that no person may intentionally intercept or attempt to intercept or authorise, or procure any other person to intercept or to attempt, at any place in the Republic, any communication in the course of its occurrence or transmission. Snail argues that attempting to intercept or monitor a data communication unlawfully is as sanctionable as actually doing it.[594] However lawful grounds of justification do apply, such as necessity, private defence, lawful interception, consent, court order or interception directive.[595] The RICA Act only applies to communications and hacking is much wider and covers not only hacking communications but unlawful access to any form of data, computer program, computer storage medium and computer system.

ii. Online identity theft and cyber fraud

As mentioned above, phishing tactics can be adopted for purposes of gathering personal information of victims which may subsequently be used in committing the crime of identity theft. This cybercrime is discussed as a cloud-based cybercrime as many a time people's personal information is stored in the cloud. Chapter 2 discussed in detail how cloud storage works. Identity theft has been described by some as the 'fastest growing white collar crime'.[596] Identity theft is a growing and evolving problem existing in both the physical and virtual worlds, and it requires a multi-faceted and multi-disciplinary approach by LEA, businesses, consumers and collaboration between countries.[597] Statistics show that identity theft increased by 337%[598] during the Covid pandemic and the FBI reported losses of more than US$43 billion globally.[599] The spate of identity theft highlights the need for adequate laws which makes it mandatory for businesses and government organisations that store personal information to have tighter security safeguards.[600] Safeguarding the security of personal data is one of the reasons

[592] Ibid.
[593] Act 70 of 2002.
[594] Snail op cit note 570.
[595] Ibid.
[596] Fawzia Cassim 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' 2015 (18) *Potchefstroom Electronic Law Journal* 69 at 71
[597] Cassim ibid at 97.
[598] South African Insurance Crime Bureau. Available at https://www.saicb.co.za/news/2021/identity-theft-up-by-337-in-2020-fraud-summit-hears#:~:text=According%20to%20the%20SAFPS'%202020,and%20impersonation%20fraud%20by%20337%25 accessed on 1 May 2023.
[599] 'African cyberthreat assessment report: Cyberthreat trends' Interpol report March 2023 at 9.
[600] Ibid.

why POPIA was enacted.[601] In most cases, identity theft is a cyber-enabled crime and not a true cybercrime. When adopting the transformational test or this study's proposed definition for cybercrime, one may argue that identity theft is not a true cybercrime. However, the purpose of this discussion is to illustrate a different kind of identity theft which is dependent on the internet and technology without which the crime does not exist.

As discussed earlier, Mabunda argues that identity theft is not a true cybercrime as this crime had existed prior to internet when perpetrators used to 'dumpster dive and rummage through garbage in search for personal information'[602]. This study takes a different viewpoint. With the promulgation of extensive data protection laws, certain attributes of information are now qualified as personal information. The definition of personal information and subsequently, identity, has been extended. In the digital world, identity is no longer just about a person's name, address, and telephone number. It is much broader to include a person's digital footprints, their online identity and IP address. Some of these pieces of personal information did not exist before the internet. Without the internet, no one could consider their IP address as personal information. People can create a digital profile of their lives, their likes, hobbies, interests, and preferences. These digital or online profiles are a representation of people online as well as their identity. As a result of technological developments, it is now possible for perpetrators to exploit a person's digital footprints and IP addresses and assume their identity for any purpose whether criminal or not. If we take away the internet, online identity theft will also cease to exist. It remains to be seen whether the United Nations ad hoc intergovernmental committee of experts[603] tasked with drafting a UN treaty on cybercrime will include online identity theft as a cybercrime.

'Identity theft occurs when someone wrongfully obtains the personal information of another individual without their knowledge, to commit theft or fraud'.[604] An individual's personal information could be used for nefarious purposes, from economic gain, illegal immigration, terrorism and espionage, evading criminal sanctions or apprehension by posing as another person (criminal identity theft) or to fraudulently obtain medical services.[605] Section 12 of the Cybercrimes Act provides that the common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property. An argument can be made that if a person uses the identity of another individual or even just some parts of

[601] Cassim argues that the Protection of Personal Information Act 4 of 2013 may be used to address identity theft, which involves inter alia the perpetration of fraud whereby the identity thief uses the personal information of the individual to open bank accounts, to obtain credit, to purchase goods and services in the individual's name or to achieve nefarious dealings such as illegal immigration, espionage or terrorism. Cassim op cit note 599 at 79.
[602] Mabunda op cit note 490.
[603] United Nations Resolution adopted by the General Assembly on 27 December 2019 A/RES/74/247.
[604] Cassim op cit note 599 at 72.
[605] Ibid.

it, to obtain tangible property such as money, the elements of the offence of theft are usually easily made out.[606]

It should be acknowledged that identity theft can be problematic when one considers the common law definition of theft. Theft occurs when a person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.[607] With identity theft, there is no permanent deprivation of the identity but rather another person can impersonate the other. It is difficult to prove the elements of appropriation and intention to permanently deprive when it comes to theft of information. Minnaar also argues that the traditional criminal law's definition of theft may not be applicable to theft of information. He argues that the definition is based on moveable corporeal objects which are taken out of an owner's possession with the intention to permanently remove them.[608] An argument can be made out that when a person uses another's identity, the crimes of forgery and fraud are committed and not identity theft as such use of another's identity does not meet all the elements of the crime of theft. Clough asserts that while the Budapest Convention addresses traditional forms of fraud and forgery and seeks to update them to the digital environment, the issue of identity theft is not addressed.[609] This is a significant omission that was not anticipated at the time of drafting.[610] Clough is correct in recognising that identity theft is a crime. The increase in criminal conduct involving the unlawful appropriation of another's identity warrants recognising identity theft as a crime on its own. While not specifically prescribed as a crime under the Cybercrimes Act, identity theft can still be criminalised in terms of section 7 of the Cybercrimes Act. Where a person uses phishing and social reverse engineering tactics to obtain the secret code, password, biometric data, or any access code of another person to obtain access to financial transactions or user identification in order to access or use data, a computer program, a computer data storage or a computer system, they will be committing a crime of identity theft.

[606] Clare Sullivan 'Is identity theft really theft?' (2009) *23 International Review of Law, Computers & Technology* 77 at 80.
[607] Ibid.
[608] Anthony Minnaar 'You've received a greeting e-card from …': The changing face of cybercrime e-mail spam scams' (2008) *Acta Criminologica CRIMSA Conference* 92 at 96.
[609] Clough op cit note 24 at 380.
[610] Ibid.

iii. Crypto laundering

Another form of cybercrime that has grown exponentially and deserve mentioning is cyberlaundering[611] and illicit financial flows.[612] As with identity theft, money laundering[613] is usually a cyber-enabled crime and not a true cybercrime. However, the purpose of this section of the chapter is to demonstrate instances where money laundering can be a true cybercrime. There is a wealth of literature which focuses on money laundering which is facilitated through digital technologies such as use of online banking and electronic fund transfers.[614] There are three stages in the lifecycle of launded money. The first stage of money laundering is placement which is the process involving the transfer of currency derived from illegal activities into a form less suspicious to law enforcement authorities[615] and thereby disguising the true origin of the money.[616] Once the money has been moved, the next step of the process is undertaking complex transactions in such a way that the funds become indistinguishable from legitimate funds (layering stage).[617] Examples of this layering stage include electronic transactions or wire transfers with the intention to obscure the trail from authorities and to hide all possible traces from their original source.[618] The last stage of the money laundering process is integration. During integration, criminals will convert their illegal proceeds into legitimate business income, for example when investing the proceeds into normal and legitimate financial, commercial, or other business operations.[619] The focus of this chapter will be on cryptocurrencies which facilitate money laundering, illicit financial flows, and financing of terrorism. Due to the anonymous nature of cryptocurrencies and

[611] Cyberlaundering is the process of utilizing internet based electronic wire transfer methods such as internet banking or online gambling, in furtherance of disguising the source of illegally obtained money. John Hunt 'The new frontier of money laundering: how terrorist organisations use cyberlaundering to fund their activities, and how governments are trying to stop them' (2011) 20 *Information & Communications Technology Law* 133 –at 134.

[612] Cyberlaundering allows for organised crime to create illegal profits and have access to money free of interest, which is created outside the legitimate banking sector. Izelde van Jaarsveld 'Following the money across cyber highways: A herculean task or international challenge? Some thoughts on money laundering on the internet' (2004) *SA Merc LJ* 685 at 688.

[613] Money laundering is a generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. Michail G Rachavelias 'Online financial crimes and fraud committed with electronic means of payment – a general approach and case studies in Greece' (2019) 19 *ERA Forum* 339 at 342.

[614] Tropina notes that automation plays a significant role in cybercrimes as it is cheaper and faster allowing criminals to easily target multiplicity of victims and computer systems. Automation is mainly facilitated using botnets. With the fast development of digital technologies, the last decade witnessed a major transformation of cyber-related crime, which has now manifested itself into a complex and thriving digital underground economy. Information technologies provide a number of tools and platforms for criminal organisations and the online platforms for these activities are merging with cybercrime underground markets. Tatiana Tropina 'The nexus of information technologies and illicit financial flows: phenomenon and legal challenges' (2016) 17 *ERA Forum* 369 at 370, 373 – 374. It is difficult to state with any certainty how much money is laundered worldwide, but the International Monetary Fund (IMF) estimates that at least $600 Billion is laundered annually, which represents between two and five percent of the world's gross domestic product. Hunt op cit note 6147 at 134.

[615] Rachavelias op cit note 616 at 343.

[616] Van Jaarsveld op cit note 615 at 688.

[617] Ibid.

[618] Rachavelias op cit note 616 at 343.

[619] Ibid.

lack of a regulatory framework across the globe, cryptocurrencies are increasingly being used by criminals as a new conduit for money laundering.

With money laundering in cyberspace taking place beyond the tools that one generally suspects, authorities have been playing catch up in trying to prevent, disrupt and investigate them.[620] The introduction and use of the blockchain technology that gave birth to different cryptocurrencies such as Bitcoin[621] means that criminals have devised new ways for money laundering. Cryptocurrencies are increasingly being used by criminals as a way of concealing their activities or as one way of money laundering. South Africa established the Financial Intelligence Centre whose mandate is to combat money laundering activities and the financing of terrorist and related activities.[622] FICA defines money laundering as any activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which one has in such proceeds.[623] Chapter 3 of FICA puts in place mechanisms which must be complied with by accountable institutions to combat money laundering and the financing of terrorist activities.

The major challenge presented by cryptocurrencies is that transactions are anonymous. Anonymising tools such as ToR have provided significant benefits that enable secure communications. With the ToR system, a user's identity is masked by distributing a transaction over several places on the internet, so that no single point can link the sender of information to its destination.[624] The anonymity of cryptocurrencies has been raised as a consumer risk by IFWG[625] of South Africa. The Financial Task Force Action Report on Virtual Currencies also stated that 'cryptocurrencies are prone to anonymity risks because their addresses or accounts are not associated with the true names of the users or any form

[620] Ramin Farinpour 'The evolving face of European criminal justice in an ever-changing world' (2016) 17 *ERA Forum* 279 at 284.

[621] A bitcoin is a fixed-value cryptographic object represented as a chain of digital signatures over the transactions in which the coin was used. Bitcoin aims to be completely distributed, free of central authorities or points of control and at least somewhat anonymous It is a virtual currency based on a decentralised peer-to-peer (P2P) network. Bitcoin can be described as a Proof of Work (PoW) based currency that allows users to generate digital coins by performing computations. Software algorithms embedded in the online Bitcoin network protect against fraud and ensure that the files are not counterfeited. By using a peer-to-peer network to distribute a master transparent public ledger called the Blockchain, each Bitcoin transaction is registered for all to see. Bitcoin exists with "no central authority in charge of the money supply [since]. the money supply is determined by a specific type of [data] 'mining' activity. It depends on the amount of resources (electricity and CPU time) that 'miners' devote to solving specific mathematical problems." The Bitcoin mining process "involves repeatedly running a computationally intensive mathematical function (called a cryptographic hash function) on a set of randomly seeded inputs until a specific pattern pops up. Trautman op cit note 110 at 42 – 50.

[622] Financial Intelligence Centre Act 38 of 2001.

[623] Section 1 FICA.

[624]ToR prevents traffic analysis by encrypting both the header and the content and sending them both through a series of proxy servers, known as nodes, each of which knows only the identities of the adjacent proxies in the chain. Every node in the chain would have to be compromised for an attacker to discover both the originator and the recipient of a packet. This allows for a near-guarantee of anonymity if at least one node in the chain is rusted, and if there are enough other users of the Tor network that an individual's traffic is hard to identify. Trautman op cit note 109 at 16 – 17.

[625] IFWG Crypto Assets Regulatory Working Group Position Paper on Crypto Assets para 4.1.2.

of identification nor do they have a central server or service provider'. To be a participant on a virtual currency network, a user is not required to produce identification, as is the case with the banks. The cryptocurrency networks do not have central monitoring bodies and there is no anti-money laundering (AML) software to oversee and identify transactions, which have suspicious trends. Due to a lack of a centralised authority for administration of cryptocurrencies, the decentralised command and control functions of a virtual currency rely typically on an encryption algorithm.[626] Section 21A of the FICA Act provides that an accountable institution may not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name. In other words, there is no need to comply with the KYC mechanisms provided by the Financial Intelligence Centre Act. Crypto traders are not currently classified as accountable institutions. However due to the nature of their services, they should be considered as accountable institutions. The anonymous nature of cryptocurrencies means that anyone can be involved in criminal activities and get paid in virtual currencies without any traceable paper trail as with bank records. The anonymous nature of virtual currency is the reason why they are the currency of choice for criminals and terrorist organisations.

Section 4 of the Prevention of Organised Crime Act (POCA)[627] makes it an offence for a person to enter into an agreement with another for purposes of concealing the source, location or movement of any property which forms part of unlawful activities. In the case of cryptocurrency transactions, if the crypto trader has reason to believe that the cryptocurrencies are proceeds from an unlawful activity, he shall be guilty of an offence. The challenge for the state will be to prove that the crypto trader reasonably ought to have known about the unlawful transaction.

The South African Reserve Bank issued its position paper on crypto assets. After conducting research on crypto assets through project Khokha, the SARB recognised that South Africa needs to regulate cryptocurrencies. The first phase is to ensure that all crypto assets service providers are registered and licenced. The objective of the registration process is to specifically gain further insights from the market participants.[628] Following registration, in the second phase, authorities will assess whether crypto asset activities could fit into existing regulatory frameworks. Where no legal authority or mandate exists for certain crypto assets-related activities, the regulatory framework will be assessed to determine what amendments are required to bring the relevant activity into the supervisory ambit. Should it be impractical to amend existing regulations appropriately, new regulations can be drafted. The specific framework, the legislative amendments required, the supervisory approach, the services covered, and the level of protection afforded will be addressed in this phase. Insights will be drawn from the approach taken regarding AML/CFT requirements, ensuring consistency in regulatory

[626] Trautman op cit note 109 at 41.
[627] Act 121 of 1998.
[628] An update on the work by the IFWG is available at https://www.ifwg.co.za/Pages/default.aspx accessed 19 October 2022.

consideration. The final phase would be to assess the effectiveness of the regulatory actions that were implemented and if the regulatory actions meet the intended objectives.

iv. Crypto jacking

Having discussed cryptocurrencies above, it is interesting to have a brief discussion on a new form of cybercrime that emerged because of cryptocurrency mining, the crime of crypto jacking. The elements of this crime are already discussed above under the cybercrimes of hacking and dissemination of malicious software. Crypto jacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads crypto mining code on the computer, or by infecting a website or online advert (ad) with JavaScript code that auto-executes once loaded in the victim's browser.[629] Hackers have two primary ways to get a victim's computer to secretly mine cryptocurrencies. One is to trick victims into loading crypto mining code onto their computers. This is done through phishing tactics such as receiving a legitimate-looking email that encourages the victim to click on a link. The link runs code that places the crypto mining script on the computer. The script then runs in the background as the victim works.[630] The other method is to inject a script on a website or an ad that is delivered to multiple websites. Once victims visit the website or the infected ad pops up in their browsers, the script automatically executes. No code is stored on the victims' computers. Whichever method is used, the code runs complex mathematical problems on the victims' computers and sends the results to a server that the hacker controls.[631]

III. CONCLUSION

This chapter is very important for the overall understanding of the issues discussed in this research study. A discussion on true cybercrimes particularly those committed in the cloud was crucial in providing the reader with clarity on the intricate differences between traditional crime and cybercrime. Such differences are important in furthering the discussion on the legal challenges faced by LEA when investigating cybercrimes. If one can identify the true cybercrimes, then they can provide a constructive critique on cybercrimes and the challenges it poses to law enforcement. First, the definitional elements for cybercrimes should indicate that if the crime can only be committed over the internet or using technology, it is a true cybercrime. When crime is committed in cyberspace not a physical space, it becomes challenging to establish whether LEA have jurisdiction to investigate the crime and gather evidence. Secondly, with cybercrime, it is possible that other states may be involved, evidence of the

[629] Michael Nadeau 'What is crypto jacking? How to prevent, detect, and recover from it' available at *https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html* accessed on 28 December 2019.
[630] Ibid.
[631] Ibid.

commission of the crime will be in digital format, there are greater chances for cross border gathering of evidence and the crime is global or transnational. Thirdly, the crime may be committed anonymously, which means that the identity of the perpetrator might be unknown and hence difficult to establish jurisdiction. Incidentally, LEA may not apply for search warrants due to the crime having been committed in a different country or the cloud evidence being stored in another country. Cybercrime investigation may also result in infringing on other state's sovereignty or interfere with that state's investigation. An understanding of jurisdiction is very important for any state to successfully prosecute cybercrimes.

The study analysed how conduct which amounts to true cybercrime is criminalised under the Cybercrimes Act. The chapter has explained why it is important to make the distinction between true cybercrimes and cyber-assisted and cyber-enabled crimes. This is because traditional laws and common law principles cannot be interpreted in a way which adequately addresses true cybercrimes. Another notable reason is that such a distinction limits the number of true cybercrimes being investigated by specialised police forces and not diverting and wasting skilled resources to investigate cyber-assisted crimes. The distinction also avoids unwarranted legislative amendments as well as avoiding misplaced or exaggerated public policy responses from criminal justice agencies.

The study has demonstrated that while common law principles can be extended to cyber-assisted and cyber-enabled crimes, the principles cannot be squarely applied to true cybercrimes. This is because developing common law principles to accommodate true cybercrimes will be in sharp contrast to the principle of legality. The study commends the provisions of the Cybercrimes Act as they carefully define and criminalise true cybercrimes and thus addressing the loopholes left under the ECT Act and common law. South Africa has progressed from not having clearly defined cybercrime provisions under the common law and the ECT Act to a more elaborate framework under the Cybercrimes Act. The study has also pointed that the Cybercrimes Act addresses cyber-assisted and cyber-enabled crimes. However, while the Cybercrimes Act empowers the courts and law enforcement agencies to exercise jurisdiction over cybercrimes, there is no clarity on whether enforcement jurisdiction can be exercised if the relevant evidence is hosted in another country. The discussions from this chapter support the hypothesis that there should be a reformulation of jurisdictional principles to address cloud data jurisdiction as current laws are not suitable to address the challenges brought about by cybercrimes and cloud computing.

CHAPTER 4: JURISDICTIONAL CHALLENGES OF CYBERCRIMES IN THE ERA OF CLOUD SERVICES

I. INTRODUCTION

'The extent of a state's power is measured not by its ability to enact laws and pass regulations, but rather by its ability to enforce them'.[632] A state is said to exercise enforcement jurisdiction when its police or other government actors are able to investigate a matter and give effect to its laws[633] or induce compliance.[634] Generally, a state can only exercise enforcement jurisdiction within its own borders and not within the borders of another state. If a state wishes to investigate a crime and exercise enforcement jurisdiction outside its borders, it must rely on permissible grounds to do so.[635] This is usually accomplished by obtaining the consent of the relevant foreign state, relying on MLAT[636] systems, letters rogatory[637], extradition[638] treaties, or any data sharing agreements[639] concluded between the states. This is a well-established international law axiom[640] which dates to the famous PCIJ judgement in Lotus.[641]

A lot has changed since Lotus. With the rise in cloud computing and internet globalisation, a person and their data are now often separated. A person may be in one country but their data or information about them are stored in another country or possibly simultaneously stored in several countries.[642] As discussed in Chapter 2 of this study, cloud services permit people to store their data in multiple foreign jurisdictions. This study further explained that there are different anonymisation tools such as The Onion Router which allow cybercriminals to mask their location and identity. This would mean that where a state is investigating a crime, it may not always be clear on which state has

[632] Teresa Scassa and Robert J Currie 'New first principles – assessing the internet's challenges to jurisdiction' (2011) 42 *Georgetown Journal of International Law* 1017 at 1071.
[633] Scassa and Currie Ibid at 1022.
[634] Christopher L Blakesley and Dan Stigall 'Wings for talons: The case for the extraterritorial jurisdiction over sexual exploitation of children through cyberspace' (2004) *Wayne Law Review 109* at 113.
[635] DJ Harris *Cases and Materials of International Law* 6ed (2004) at 269. Ghappour op cit note 153 at 1100 – 1101.
[636] Some of the frameworks which promote mutual assistance include South Africa's International Cooperation in Criminal Matters Act 75 of 1996, Article 28 of the Malabo Convention, Chapter 3 of the Budapest Convention, and Article 18 (3) of United Nations Convention against Transnational Organised Crime and the Protocols Thereto adopted by the UN General Assembly on 15 November 2000, by resolution 55/25.
[637] Geldehuys defines letters rogatory as a formal request from the judicial authority of one State to a judicial authority of another State. They are not treaty-based but rather a matter of comity between courts. Kotie Geldenhuys 'Bilateral tools for fighting transnational organised crime' (2019) *Servamus* 32 at 34.
[638] Extradition is defined as the physical surrender by one state (the requested state) at the request of another state (the requesting state) of a person who is either accused or convicted of a crime by the requesting state. Murdoch Watney 'A South African perspective on mutual legal assistance and extradition in a globalised world' (2012) 15 *Potchefstroom Electronic Law Journal* 292 at 298. Extradition Act 67 of 1962.
[639] Executive agreements are an example of data sharing agreements, and they are a common mechanism used by the United States. Section 105 of the US CLOUD Act. Article 48 of the GDPR.
[640] Currie op cit note 214 at 77.
[641] *France v Turkey* (1927) P.C.I.J Reports, Series A, No.10.
[642] Woods op cit note 212 at 742.

jurisdiction over cloud data. The architecture of cloud computing means that the location of data may be fortuitous.[643] Woods correctly observed that oftentimes, the state where the data resides coincidentally ends up with the most regulatory power. This is regardless of whether such a state has any interest in the cloud data, the owner of the data or the crime under investigation.[644]

a. Objectives

The scope of this chapter is to discuss the main research questions of this study. To re-iterate, the study investigates the challenges presented by cloud computing technologies during cybercrime investigations. With the bulk of evidence being stored in a global cloud, there are a myriad of problems that make gathering of cloud evidence challenging. These problems range from confusion over which state has jurisdiction over cloud data, limitations imposed by a broken international system around cooperation during crime investigations and differences in measures adopted by governments to respond to these challenges. To develop appropriate and adequate jurisdictional principles over cloud data requires a comprehensive understanding of the jurisdictional challenges that cloud computing currently pose. Addressing the jurisdictional dilemma over cloud evidence involves having clarity on how states should deal with transborder cloud data. Importantly, there should be clear guidelines on whether states should be permitted to unilaterally conduct enforcement measures on data stored abroad.

It is also important to clarify on whether remote cross border search for cloud data is an indirect affront to another state's sovereignty. Study on enforcement jurisdiction has highlighted the importance played by the territoriality principle. This chapter discusses whether the territoriality principle has relevance in cyberspace and cloud data jurisdiction. To expand on this, the chapter considers the arguments around data exceptionalism which justifies the need to move away from territoriality-based jurisdictional principles. Depending on who is requesting access to cloud evidence, data jurisdiction has been subjected to a myriad of jurisdictional principles.[645] The importance of a discussion on the contemporary jurisdictional debates over cloud data is that it helps to formulate a balanced approach to data jurisdiction. Such an approach should promote the sovereign interests of states in investigating and prosecuting cybercrime as well as bringing justice to crime victims. Incidentally, the approach also protects the privacy and security interests of anyone whose data may be relevant in a cybercrime investigation.

[643] A searching state may have a stronger interest in the data than the state in which the data are stored. Patricia L Bellia 'Chasing bits across borders' (2001) *University of Chicago Legal Forum* 35 at 78.
[644] Woods op cit note 212 at 742.
[645] Some of these principles include the location of data, location of owner of data, nationality of data owner, location of data controller, headquarters of a cloud service provider, subsidiary of a cloud service provider, territory where a cloud provider is offering its services, laws of the territory where the data owner has subscribed to a service, territory of the criminal justice authority or the degree to which the provider is active in the territory.

The second part of the research question is whether South Africa's criminal law adequately address jurisdictional challenges presented by cloud services. South Africa's criminal justice system has for a long time been based on antiquated procedural laws. Most of the criminal laws precede the use of the internet. As discussed in Chapter 3, most criminal laws are problematic and inadequate to address cyberspace and cybercrimes.[646] This chapter critically discusses how South Africa's criminal laws, such as the Cybercrimes Act, address the jurisdictional debate around cloud data.

With South Africa's cybercrime legislative environment still in its nascent stages, the chapter considers how other countries have responded to the jurisdictional debate. The Constitution of the Republic of South Africa provides that when interpreting the Bill of Rights, a court, tribunal, or forum must promote the values that underlie an open and democratic society based on human dignity, equality, and freedom, must consider international law and may consider foreign law.[647] The chapter discusses the efforts to curb cybercrime at a global level. It further discusses important and watershed litigation cases on cloud data jurisdiction. By discussing landmark court judgements, the chapter seeks to highlight the role played by courts in shaping the law around data jurisdiction.

II. EXERCISE OF ENFORCEMENT JURISDICTION IN THE CLOUD

The exercise of a state's enforcement powers outside its territory was established in the *Lotus*[648] case. The Permanent Court of International Justice reasoned that a state -

'*…may not exercise its power in any form in the territory of another state. In this sense jurisdiction is certainly territorial; it cannot be exercised by a state outside its territory except by virtue of a permissive rule derived from international custom or from a convention. Accordingly, not only will states not enforce the public (particularly criminal) laws of other states, but absent exceptional circumstances no state may enforce its own laws upon the territory of a second state absent some clear legal authorisation to do so. This extends to both investigative jurisdiction (for example, the police of one state cannot investigate in another state without the latter's permission) and jurisdiction over the*

[646] Cassim op cit note 199 at 39. The problem of inadequate and outdated criminal laws in cyberspace is not unique to South Africa. Other countries like Ethiopia are experiencing similar challenges as the existing criminal code did not cover certain cybercrimes. Kinfe Micheal Yilma 'Developments in cybercrime law and practice in Ethiopia' (2014) *Computer Law & Security Review* 720 at 721.
[647] Section 39 Constitution of the Republic of South Africa, 1996.
[648] *France v Turkey* supra note 637. The question before court was whether Turkey acted in conflict with principles of international law by instituting criminal proceedings in terms of Turkish law against the captain of the Lotus at the time of collision. The French government contended Turkey had to rely on some international law to have jurisdiction. On the other hand, the Turkish government took the view that Article 15 of the Convention of Lausanne allowed Turkey to have jurisdiction whenever such jurisdiction did not come into conflict with a principle of international law.

person (for example, the police of one state cannot arrest an individual in another state, again without the latter's permission) …'[649]

The Lotus decision emphasised that extraterritorial jurisdiction to enforce is, in principle, not permissible. A state can exercise enforcement jurisdiction outside its borders if the other state agrees (by treaty or during judicial or police cooperation). Applying the principles to extraterritorial jurisdiction as set out in the Lotus case may be challenging in the cloud context. This is mainly because there is lack of legal clarity on whether LEA exercise territorial or extraterritorial jurisdiction when they access, search, or seize evidence stored in foreign based cloud servers.

Chapter 2 of this study displayed the unique features of cloud data which raises the foundational questions as to how to assess territoriality for crime investigations. A state exercises enforcement jurisdiction when its police, relying on a state's criminal laws, investigates crime and its prosecuting authorities prosecute criminals.[650] State practice, dating back to Lotus, has shown that enforcement jurisdiction is territorially bound. Currie correctly noted that 'states tend to be quite chauvinistic about their domestic criminal laws and guard their sovereignty closely in this arena'.[651] This means that in principle, LEA from one state cannot unilaterally cross the border to make arrests in another country in the absence of that other country's permission. Enforcement jurisdiction also means that an investigating state cannot go to a foreign state to gather evidence on its own to prosecute a criminal within its territory.

A question which can be posed is why does the distinction between territorial jurisdiction and extraterritorial jurisdiction matter in cyberspace? In a digital environment, should there be a distinction between the two? If the exercise of enforcement powers in the transborder cloud is viewed as territorial, it follows that a state's LEA can conduct investigations in terms of the state's own national laws. However, if the exercise of such powers is considered extraterritorial, the powers of the state's LEA are limited. To exercise enforcement jurisdiction, the LEA will have to rely on a special allocation of authority under international law or valid consent by a foreign government.[652]

The question that has been raised is the relevance of the Lotus case in the emerging transnational cyberspace. How relevant are principles developed on steam engines within the context of bits and bytes? Scholars have argued that due to the gradual shift towards cloud computing, we cannot blindly follow the Lotus decision.[653] When one considers the factual background and the setting of Lotus, *vis-*

[649] Scassa and Currie op cit note 646 at 1028 – 1029.
[650] Currie op cit note 214 at 70.
[651] Currie op cit note 214 at 71.
[652] Rule 11 of the Tallinn Manual. Michael N Schmitt *Tallinn Manual 2.0. on The International Law Applicable to Cyber Operations* (2017).
[653] Mireille Hildebrandt 'Extraterritorial jurisdiction to enforce in cyberspace: Bodin, Schimitt, Grotius' (2013) 63 *University of Toronto Law Journal* 196 at 199.

a-vis the legal and technological developments, a departure from Lotus is justifiable.[654] Some scholars seem to argue that when states unilaterally access cloud data, they exercise territorial jurisdiction. The argument is that if an investigating state does not enter the territory of the foreign state, the foreign state cannot rely on its sovereignty to object to such entry.[655] Evidently, with transnational clouds, an investigating state may not need to send its investigating officers to the foreign state to gather evidence. The investigating officers can access the cloud evidence and search a computer in another country without leaving their workstations.[656] This is achieved by deploying network investigative techniques[657] or hacking technologies. Alternatively, they may request service providers to access cloud evidence on their behalf. In such instances, the foreign state may not even be aware that locally stored data was accessed by a foreign government as there is no physical entry into the foreign state.

This study argues that the Lotus judgement is still applicable in the internet age. It submits that the judgement itself did not prohibit the exercise of extraterritorial enforcement jurisdiction. Lotus did not impose an absolute ban on the exercise of extraterritorial jurisdiction by states. The PCIJ ruling in Lotus is very clear. It held that '…*absent exceptional circumstances no state may enforce its own laws upon the territory of a second state*…' The rise in cyberspace, the internet and cloud computing technologies qualify as 'exceptional circumstances' as envisioned in Lotus. As such, formulating cyber-centric law which may divert from the traditional understanding of extraterritorial enforcement jurisdiction is not a drastic departure from the Lotus decision. When LEA access a suspect's computer in another state, they will be exercising extraterritorial enforcement jurisdiction.[658] When a search warrant has been issued over data stored in another country, the state exercises extraterritorial jurisdiction in the sovereign territory of another state. This is what Currie described as an electronic rather than kinetic intrusion.[659]

Since a state is sovereign within its borders, it can exert jurisdiction over individuals or entities located on its territory as prescribed under the territoriality principle.[660] When a service provider conducts its business and hosts its data within a forum state, it is subject to the laws of that state and can be tried in its courts.[661] The corollary to the territorial principle is that a state's legal authority to regulate conduct on its own territory precludes it from regulating conduct taking place outside its

[654] Svantesson op cit note 104.
[655] Bellia op cit note 637 at 64.
[656] Benton op cit note 171 at 206.
[657] Network Investigative Techniques (NIT) are hacking techniques used by law enforcement to 'hack back' or access evidence held by cybercriminals. Steven David Brown 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2019) *ERA Forum* 423.
[658] Eichensehr op cit note 155 at 148.
[659] Currie op cit note 214 at 88.
[660] Walter C. Jnr Dauterman 'Internet Regulation: Foreign Actors and Local Harms – at the Crossroads of Pornography, Hate Speech and Freedom of Expression' (2002) 28 *North Carolina Journal of International Law and Commercial Regulation* 177 at 183.
[661] Ibid.

territory.[662] As Ghappour correctly notes, states do not directly exercise law enforcement functions in other countries without first obtaining consent.[663] Such consent can be obtained by means of Mutual Legal Assistance Treaties. These MLATs also rely on territorial jurisdiction. This means territorial jurisdiction remains the foundational background for establishing jurisdiction including jurisdiction over cloud data. Arguably, it is important to consider diverting from relying on territorial jurisdiction when dealing with transborder cloud data. Instead, states need to reformulate jurisdictional principles which disregards the role of territory and considers other competing interests. This discussion will be explored further below.

b. A primer on South Africa's position on extraterritorial data

South Africa's criminal law jurisprudence seem to permit the exercise of extraterritorial jurisdiction. The South African Police Service Act authorises police to exercise their police powers and duties with due regard to the Constitution and fundamental human rights. The police are permitted to seize any article which may prove the commission of a crime, or which was intended to be used in the commission of a crime when they stop individuals at roadblocks or checkpoints.[664] From a legislative interpretation of the SAPS Act, the legislature did not intend for police to search electronic evidence at roadblocks. However, due to the current wording of the SAPS Act, there is nothing prohibiting the police to seize any cloud-based devices. The SAPS Act does not directly authorise or permit police to seize cloud data. However, it permits police to seize any article which may provide evidence of a crime. That would seem to suggest that under the SAPS Act, police have jurisdiction over cloud data. Since the Act is silent on cloud evidence, one can arguably infer that the police can exercise extraterritorial enforcement jurisdiction over cloud data.

The National Prosecuting Authority Act[665] empowers the Investigating Director to enter any premises on or in which anything connected with an investigation is or is suspected to be and may inspect and search those premises, examine any object found on or in the premises which has a bearing or might have a bearing on the investigation in question and make copies of a document or seize anything that has a bearing on an investigation.[666] The NPA does not prohibit an Investigating Director from searching and seizing cross border cloud data.

The ECT Act also seem to permit the exercise of extraterritorial enforcement jurisdiction over cloud data. When investigating crime, the ECT Act gives cyber inspectors the power to enter '*any*' (own emphasis) premises and information systems to make copies of any documents or recordings.[667] If

[662] Ibid.
[663] Ghappour op cit note 153 at 1083.
[664] Section 13 (8) (d) (v) of the SAPS Act 68 of 1995.
[665] National Prosecuting Authority Act 32 of 1998.
[666] Section 29 of the NPA.
[667] Section 82 (1) (c) of the ECT Act.

electronic evidence is stored in the cloud, LEA have jurisdiction to access the evidence. The ECT Act does not distinguish between cloud evidence hosted within South Africa and cloud evidence hosted in foreign territory. One can note that when the ECT Act was enacted, most information systems and internet-based services relied on the use of internal hard drives in computers, external hard drives, and on-site servers. Considering that it was only recent that cloud service providers started building data centers in South Africa[668], it stands to reason that LEA always exercised extraterritorial jurisdiction over cloud data. It is crucial to have laws specifically applicable to electronic data.[669] Instead of applying antiquated laws on seizures and searches of electronic evidence.

As mentioned earlier, section 24 of the Cybercrimes Act provides that a South African court has jurisdiction to try any offence referred to in the Act. Section 24 (1) (e), (f) and (g) of the Cybercrimes Act specifically deals with offences committed outside South Africa. If a cybercrime affects any person, a restricted computer system, a public body, or any business in South Africa[670], a South African court can exercise jurisdiction over the offence. A South African court can also exercise jurisdiction if an offence was committed outside South Africa against a South African citizen or resident, against a restricted computer system in South Africa, against a registered company or body of persons in South Africa or a government facility in the country.[671] By providing protection to restricted computer system or government facility, the Cybercrimes Act is applying the protective principle.[672] It should also be noted that such restricted computer system and government facility can fall under the definition of critical infrastructure under the Critical Infrastructure Protection Act.[673] Chen Wei also notes that the protective principle is likely to be confined to cyberterrorism targeting critical state infrastructure.[674] The court can also exercise jurisdiction if the evidence reveals any other basis recognised by law in terms of which the court may assert jurisdiction to try the offence.[675] In instances where an offence has been committed outside South Africa, regardless of whether or not the act constitutes an offence at the

[668]Yevgeniy Sverdlik 'Microsoft Launches First Cloud Data Centers in South Africa'https://www.datacenterknowledge.com/microsoft/microsoft-launches-first-cloud-data-centers-south-africa accessed 05 February 2022. 'Amazon launches data centre operations in South Africa' Reuters 22 April 2020 https://www.reuters.com/article/us-safrica-amazon-com-cloud-idUSKCN2241X3 accessed 05 February 2022. 'Huawei Cloud Africa launch due for March 2019' https://www.huawei.com/za/news/za/2019/huawei-cloud-africa-launch-due-for-march-2019 accessed 05 February 2022.

[669] Vinesh Basdeo 'The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' (2012) *South African Journal of Criminal Justice* 195 at 207.

[670] Section 24 (1) (e) of the Cybercrimes Act.

[671] Section 24 (1) (f) of the Cybercrimes Act.

[672] This principle seeks to protect the security interests of a state. Du Toit Commentary on the Criminal Procedure Act Chapter 16. Blakesley and Stigall define the protective principle as a principle which provides jurisdiction over offenses committed wholly outside a state but have an adverse effect on a state's security, integrity, sovereignty or important governmental function. Blakesley and Stigall op cit note 630 at 127. Harris op cit note 649 at 266.

[673] Chapter 3 of the Critical Infrastructure Protection Act 8 of 2019.

[674] Chia Chen Wei 'Sketching the margins of a borderless world' (2018) 30 *Singapore Academy of Law Journal* 833 at 845.

[675] Section 24 (1) (g) of the Cybercrimes Act.

place of its commission, the offence will be deemed to have been committed in South Africa if the person is extradited to South Africa or is found in the country or is for one or other reason not extradited by South Africa or if there is no application to extradite the person.[676]

While the courts are permitted to adjudicate over offences committed outside South Africa in terms of section 24 of the Cybercrimes Act, it remains unclear whether South African LEA can exercise enforcement jurisdiction by unilaterally accessing cloud data hosted on foreign servers. Kohl correctly pointed out that enforcement jurisdiction is a state's Achilles heel which can put a stop to adjudicative and prescriptive jurisdiction.[677] To get a better understanding on enforcement jurisdiction, one needs to analyse Chapter 4 of the Cybercrimes Act which deals with enforcement powers to investigate, search, seize or access. Section 28 of the Cybercrimes Act provides that 'a police official may in accordance with the provisions of this chapter, search for, access or seize any article, within the Republic'. By including the words 'within the Republic', one can argue that section 28 of the Cybercrimes Act only permits LEA to exercise their enforcement powers when evidence is in South Africa and not when evidence is outside South Africa. The definition for article includes computer data storage medium. It should be noted that cloud services and storage as a service offering is covered under the definition for computer data storage medium.[678] If an article is hosted on a data centre in another country, the police may not exercise their powers as prescribed under section 28 of the Cybercrimes Act.

Section 24 (4) of the Cybercrimes Act provides clarity on how to go about prosecuting an offence committed outside South Africa. The prosecution may only be instituted against a person with the written permission of the National Director of Public Prosecutions and must commence before a court designated by the NDPP.[679] It is also required of the National Commissioner and the National Head of the Directorate, in consultation with the NDPP to issue directives with which all police officials must comply in the execution of their functions in terms of the Cybercrimes Act, regarding the investigation of offences committed outside the Republic.[680] At the time of writing of this study, the directives have not been issued yet. It is hoped that this study can provide guidance in preparation of these directives. The above discussion illustrates that South Africa's criminal laws do not prohibit the exercise of unilateral enforcement jurisdiction over remote cloud data. The main concern with exercising unilateral enforcement jurisdiction is that such action infringes on principles of international law and the sovereign interests of another state. The succeeding section of this study explores this discussion further.

[676] Section 24 (2) of the Cybercrimes Act.
[677] Uta Kohl *Jurisdiction and the Internet* (2007) chapter 1 at 18 and 26.
[678] The Cybercrimes Act defines computer data storage medium as any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, *irrespective of whether the device is physically attached to or connected with a computer system.*
[679] Section 24 (4) of the Cybercrimes Act.
[680] Section 24 (4) of the Cybercrimes Act.

III. REMOTE CROSS BORDER ACCESS TO CLOUD DATA AND STATE SOVEREIGNTY

One of the main reasons why understanding jurisdiction over cloud data is important is the preservation of sovereignty interests. It has been argued that unilateral access to remote cloud data infringe on the sovereignty of a foreign state.[681] This section briefly discusses the role of sovereignty in the cloud. This discussion shall be explored further in chapter 5 under data localisation and the role of data sovereignty and digital sovereignty. Sovereignty is the authority vested in a state over its subjects or operations taking place within its territorial borders. States' sovereign interests include preventing and prosecuting crime, protecting their citizens and residents by limiting the ability of foreign governments to unilaterally access citizens' and residents' data.[682] It also includes setting baseline substantive and procedural protections to govern access to data globally and protecting the economic interests of local companies.[683] One should note that there could potentially be conflicting sovereign interests where the same sovereign interests enjoyed by a state where data are located may be the same sovereign interests relied on by a foreign state investigating a cybercrime.

In a cyber environment, states enjoy sovereignty by exercising authority over cyber infrastructure located within their territory and activities associated with that cyber infrastructure.[684] When a state enjoys sovereignty over cyber infrastructure, it has the authority to pass domestic laws, regulations, and policies over the infrastructure. This also extends to being able to protect cyber infrastructure and safeguard cyber activity that is in or takes place within its territory.[685] In practice, a state has sovereign authority over cloud infrastructure established within its physical borders. To reduce conflict between sovereigns and preserve comity, a state should coordinate with a foreign state where data are hosted before conducting any searches.[686] To unilaterally cross digital borders and remotely access cloud data potentially infringes on principles of state sovereignty, equality of states and violation of human rights.[687] Incidentally, the data hosted on the cloud infrastructure are also subject to the sovereignty of the state. Data protection laws like the POPIA and to a broader extent, the GDPR seem to follow this line of approach to cloud data.

Some scholars view access to cloud data as less evasive than a physical search[688] and not infringing on the sovereign interests of the foreign state. This study submits that such an argument is

---

[681] Velascos notes that states still differ in opinion over whether access to cross border data should be permissible. Cristos Velasco 'Cybercrime jurisdiction: past, present and future' (2015) 16 *ERA Forum* 331 at 344.
[682] Daskal op cit note 227 at 226.
[683] Ibid at 227.
[684] Rule 1 of the Tallinn Manual op cit note 666.
[685] Rule 2 part 2 of the Tallinn Manual op cit note 666.
[686] Benton op cit note 171 at 206.
[687] Rule 11 part 1 of the Tallinn Manual op cite note 666.
[688] Bellia op cit note 657 at 77.

becoming less viable as more data are increasingly available online than offline. The rapid digitalisation of economies, the digital transformation of governments, use of big data analytics and artificial intelligence mean that insurmountable amounts of information are being stored electronically than physically.

The question of territorial sovereignty in cyberspace is not clear in terms of international law. There are different views on whether territorial sovereignty is a binding international law rule or a principle upon which other specific rules are based. The Tallinn Manual recognizes territorial sovereignty as a binding rule of international law. Rule 4 of the Tallinn Manual provides that states can determine whether a particular cyber action violates sovereignty interests of another by considering if a threshold level of intrusiveness or interfering with or usurping on an inherently governmental function has been crossed. The challenge with this threshold is that there are no guiding principles explaining at which point access to remote cross border data violates international law rules.[689]

In the absence of a clear position on whether international law recognizes territorial sovereignty as a binding rule or as a principle, one should also consider how customary international law addresses the issue of jurisdiction. Usually, a customary rule develops with the passage of time.[690] However, certain instances can result in a rule coming into existence quite rapidly.[691] A notable example is the 1963 unanimous approval of a resolution declaring the legal principles governing activities in outer space by the UN General Assembly.[692] Dugard correctly points out that a settled practice (*usus*)[693] on its own is insufficient to create a customary rule[694], but there must be a sense of obligation on the part of the states that they are bound by the rule in question.[695] Proof of *opinio juris* is difficult to produce. *Opinio juris* will be presumed when there is evidence of a general practice in support of a particular rule.[696] Dugard clarified that to prove *opinio juris*, a state must feel bound or entitled to act in a particular way, not just for political or policy reasons but because of the existence of a rule of customary international law.[697]

With the lack of scholarship on enforcement jurisdiction in which a state can effect compliance with its laws in the territory of another state[698], one can argue that it would seemingly take a while

[689] Daskal op cit note 147 at 686.
[690] John Dugard *Dugard's International Law: A South African Perspective* (2018) 5ed chapter 3 at 34.
[691] Ibid.
[692] Ibid.
[693] Usus of a state can be identified through its policy statements, its commentary on certain international reports, its courts' decisions, international treaties it enters into, opinions of national law advisers, and resolutions of international organisations. Dugard op cit note 693 at 31.
[694] Dugard op cit note 693 at 36.
[695] Ibid.
[696] Dugard op cit note 693 at 37.
[697] Ibid.
[698] Ghappour op cit note 153 at 1083.

before customary international law in this regard is developed. Currie observes that opinion juris might have been established as states view access to cross border data by investigative officials as unlawful exercise of enforcement jurisdiction.[699] However, Bellia argues that customary international law cannot impose limitations on unilateral access to cross border data because of lack of consistent state practice.[700] This study submits that when one considers the recent developments in cybercrime investigations, one can note that these developments can potentially trigger the development of customary law without the need for the passage of extended periods of time. For instance, the recently signed 2nd Additional Protocol to the Cybercrime Convention on transborder access to data will likely play a major role in the development of *opinio juris*.

Whilst it is possible to develop *opinio juris* over data jurisdiction, one should be mindful that this may be resisted by inconsistent state practice.[701] In practice, what states say is in discord with what they do.[702] Currie observes that there is an uncertain, but significant amount of unilateral cross border electronic evidence gathering, or other enforcement activity, by police and security personnel.[703] For example, police officials may unilaterally access data without even documenting it.[704] Police may cooperate directly with foreign based police officers without the involvement of judicial authorities or other government apparatus of the territorial state.[705] In some occasions, the authorities of the territorial state are notified after the fact.[706] For example, during an investigation of child pornography, Dutch authorities accessed data on US servers without the permission of the US government.[707] Due to the urgency of the case, the Dutch authorities reasoned that they had no time to seek for permission from the US. The US authorities were later notified and provided with copies of the images seized and did not object to the searches which were conducted.[708] Currie concludes by stating that despite overall state insistence that unauthorised cross border evidence gathering breaches the bar on extraterritorial enforcement jurisdiction, when it comes to electronic data, state practice does not match up evenly with *opinio juris*.[709]

If there is no agreement on whether sovereignty is a principle or a binding rule and if customary international law is not yet established, the next important question to ask is how should international law address remote cross border access to data? An answer to this question calls for a discussion on

[699] Currie op cite note 214 at 80.
[700] Bellia op cit note 657 at 63.
[701] Currie op cit note 214 at 80.
[702] Ibid.
[703] Ibid.
[704] Currie op cit note 214 at 81.
[705] Ibid.
[706] Ibid.
[707] Ibid.
[708] Ibid.
[709] Currie op cit note 214 at 84.

current status quo on data jurisdiction. This chapter gives insights into how international law should be developed by discussing the different approaches to cloud data jurisdiction and analysing the developments in international law. It also discusses the important sovereignty interests and key interests at stake.

IV. APPROACHES TO CLOUD DATA JURISDICTION

Despite the proliferation and exponential growth in the use of cloud-based services, it is interesting to note that cloud data jurisdiction is not yet settled in many legal systems.[710] Different states and courts have adopted different positions regarding the reach of the state's jurisdiction over cloud data.[711] There are about four different approaches that are applied by different states when establishing jurisdiction over remote cloud data. Some states exercise jurisdiction based on where the data or infrastructure hosting the data are located. Others have exercised jurisdiction by relying on their ability to access the data from within their territory. Some also approach data jurisdiction by relying on the jurisdictional power they have over the service providers in control of the sought-after data while others apply any of these approaches depending on the circumstances.

Technology companies, service providers, legal scholars and legal practitioners also have diverging views on data jurisdiction. Technology companies like Google and Facebook, for instance, seem to adopt the view that states have authority to compel data if the service provider is domiciled in that state's territory.[712] On the other hand, companies like Microsoft have adopted the approach that the state where the data are located has jurisdiction.[713] Categorically, scholarly opinion on data jurisdiction either falls within data exceptionalism discourse or alternatively the data territoriality discourse. When there are diverging principles, it makes it difficult for consensus to be reached particularly in the space of a global internet. This creates unnecessary hurdles for LEA who are investigating crime. Service providers who are meant to assist LEA may end up being subject to conflict of laws. Overall, a state will not be able to protect its sovereign interests and the rights and interests of its citizens and residents.

Chapter 2 argued that the unique features of data in the era of cloud services warrant the destabilisation of the territoriality doctrine of jurisdiction. The objective of this section of Chapter 4 is to discuss the various approaches adopted in determining data jurisdiction and cloud data jurisdiction. This discussion will expose the challenges that we currently have in South African law as it relates to cloud data and jurisdiction. The expected outcomes of this discussion and research are to define the limits of government or law enforcement in accessing data stored in the cloud. Considering that the

[710] Woods op cit note 212 at 732. Though Woods was commenting on the US legal landscape, this position is similarly true for South Africa's context. South Africa has not yet settled the issue of cloud data jurisdiction.
[711] Woods op cit note 212 at 732.
[712] Woods op cit note 212 at 736.
[713] Ibid.

bulk of sought-after cloud evidence constitutes personal data or personal information, this study adopts or recommends an approach which promotes, protects, and upholds human rights, particularly the right to privacy. Throughout the discussion on the different approaches to jurisdiction, this chapter also interrogates the approaches adopted by South Africa and whether the approach or approaches address the jurisdictional challenges of cloud data.

a. The importance of the territoriality principle

Territory still plays a significant role in data and internet jurisdiction. It remains as the primary basis for the exercise of jurisdiction in a state. The drafters of the Tallinn Manual consider territory as a fundamental attribute of the principle of sovereignty.[714] When one considers international law on jurisdiction as discussed earlier, territoriality principle is still significantly relevant.[715] A government's power to conduct searches and seizures emanate from the territoriality principle.[716] If an object under consideration is located within a territory, it becomes easier for a state to use location as the basis to extend jurisdiction. Location can be used to determine the rules which are applicable to an activity.[717] A review of the history of the internet and the history prior to the internet, shows that territory has been the backbone for determining jurisdiction.

As the use of the internet grew in the 1990s, there was an active debate between the unterritorialists, such as David Post and the territorialists, such as Jack Goldsmith and Tim Wu. The unterritorialists argued that the internet would defy territorial regulations while the territorialists argued that the internet would increasingly succumb to longstanding jurisdictional rules and territorial based controls.[718] Contributions from territorialists have supported the broader view of territorial sovereignty and the relevance of geographical location in defining the extent of a state's powers. Territorialists argue that geographical borders still play a role on the internet in marking off differences in culture, currency, climate, consumer norms and language.[719] An internet user's geographical location has a massive contribution on the type of online content they have access to. First, the laws in the area where the internet user is based influences the type of content that can be accessible by a user. If a country does not permit certain content, such content is filtered by location-based filtering mechanisms[720] and internet users may not be able to access it unless if they deploy certain techniques like VPN. Secondly, an internet user's location matters as service providers can tailor content such as weather updates and news

[714] Rule 9 part 1 of the Tallinn Manual op cit note 666.
[715] Tubic and Radojcic op cit note 201 at 200.
[716] Daskal op cit note 281 at 326.
[717] Ibid at 329.
[718] Daskal op cit note 227 at 181.
[719] Jack Goldsmith and Tim Wu *Who Controls the Internet? Illusions of Borderless World* (2006) at 51.
[720] Daskal op cit note 227 at 181.

updates specific to the location.[721] The debate between territorialists and unterritorialists is still not resolved today.

When one considers the sharp differences in opinion between territorialists and data exceptionalists, one can note that this signifies or indicates the challenge of cloud data jurisdiction and extreme difficulty in finding common ground. Chapter 2 of this study discussed in detail the different features of cloud data which disregards geography and thus warranting to be regulated by different set of laws. In response to these unique features of data, territorialists argue that though data are intangible, territory can still be used to determine data jurisdiction. The argument is that cloud data resides on servers and wherever those servers sit, they are subject to territorial assertions of jurisdiction.[722] Territorialists emphasise that data jurisdiction has everything to do with territoriality. This could be the location of data itself, the location of the data controller, the location of the crime or the citizenship of the victim or perpetrator.[723]

When comparing data to other forms of intangible property, territorialists argue that there is nothing novel about data as courts still exercise jurisdiction over intangible assets like stock, debt, intellectual property, and money. The argument presented by territorialists is that if courts can exercise jurisdiction over intangible assets like money, regardless of its location, the same jurisdictional provisions can be applied to cloud data. Data exceptionalists do not agree. Data exceptionalists argue that simply applying the rules governing other tangible and intangible assets is both unsatisfying and unworkable.[724] When one considers intangible assets like money and debt, one can note that they are rivalrous assets and can only be held in a single location at any given time.[725] Unlike data, not more than one person can be in possession of money simultaneously. Once money has been accessed and retrieved, it is no longer available.[726] Similarly, with new forms of currencies such as cryptocurrencies and non-fungible tokens (NFTs), once a person possesses the decryption key, no one else can access the assets. This is because the underlying blockchain technology is designed to be immutable. Data on the other hand can be divided, distributed, multiplied, or manipulated by multiple parties without interfering with the data owner's ability to use or access it. Wherever copies of the same data are located, people can still access them or manipulate them.[727]

Territorialists also argue that mobility is not an entire phenomenon unique to data. In the digital era, people and intangible property can be mobile. People can transact at the click of a button and send

[721] Goldsmith and Wu op cit not 733 at 51.
[722] Woods op cit note 212.
[723] Ibid.
[724] Daskal op cit note 227 at 220.
[725] Ibid at 223.
[726] Ibid.
[727] Ibid.

money and make payments instantly. While recognising the mobility of intangible property, data exceptionalists point out some unique features of cloud data. Data can travel across borders in seemingly arbitrary paths and can be stored in a country different to where the user or owner of the data is residing.[728] The mobility of data is not predictable or known.[729] For example, one is not able to tell the location of data while it is in transit or to tell the exact way that data moves from one server to the next. Unterritorialists conclude that due to the distinctive nature of data, territory should be rejected as a basis for exercising enforcement jurisdiction to search and seize data and there should be a reconsideration of jurisdictional principles.[730]

Technology has resisted territorial boundaries. Even during the early days of the internet, unterritorialists like John Perry Barlow[731] have argued for a cyberspace which is not under the control of states. However, states found ways to exercise jurisdiction over activities in the digital environment. Johnson and Post[732] also argued that cyberspace is a distinct, separate space where geographical borders and territorial jurisdiction make no sense. States generally should not attempt to apply geographically based regulations to internet transactions as such regulations will be ineffective.[733] History has sided with the territorialists.[734] What can be noted is that, despite a myriad of jurisdictional principles and despite the advancement in technology, territory remains to be the determinative factor when applying any jurisdictional principles to data. Most principles on jurisdiction place emphasis on territory. States have increasingly found ways to regulate and compel production of data that passes through their borders and to use new technology (such as location-based filtering mechanisms) and new mandates (such as data location requirements) to increase territorial based controls.[735]

The preceding discussion highlights how the territoriality principle continues to take centre stage in cloud data jurisdiction. Political will on data sovereignty, digital sovereignty, and data localisation centers around the territoriality principle. While cloud data are exceptional and the arguments presented by data exceptionalists are sound, it is unfortunate to note that states continue to hold on tightly to the territoriality principle. Jurisdiction is and likely always will be rooted in territoriality.[736]

[728] Daskal op cit note 281 at 326.
[729] Daskal op cit note 227 at 222.
[730] Daskal op cit note 281 at 332.
[731] Barlow op cit note 3.
[732] David R Johnson and David Post 'Laws and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367.
[733] Hildebrandt op cit note 667 at 201.
[734] Daskal op cit note 227 at 181.
[735] Ibid.
[736] Woods op cit note 212 at 764.

b. Location of cloud evidence approach

As mentioned above, state practice seems to suggest that territory and location of data matters when determining state jurisdiction over cloud data. This is because when states prescribe laws, the intention is to regulate conduct within their geographical borders as well as conduct they can prosecute. When a search warrant has been issued, it empowers LEA to access and search for evidence outlined in that search warrant. The question which arises is whether a state can authorise a search where the sought-after data are hosted in another country. In other words, is the location of cloud data important when determining if a state has jurisdiction to access the electronic evidence? Can a state issue a search warrant over data located outside its territory? To address this question, this study will analyse a US landmark case of *Microsoft Ireland v United States*[737] which discussed the question of data jurisdiction and the extent of a search warrant. This analysis will be used to draw a comparison on how South African law addresses the same question.

Despite the case being made moot by the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), the arguments presented by legal counsel for Microsoft and the US government are very important and relevant in understanding data jurisdiction.[738] In *Microsoft Ireland* case, the search warrant was issued pursuant to the US 1986 Stored Communications Act (SCA). The FBI wanted Microsoft US to disclose emails and other communications content which it had access to. The problem was that the sought-after data was stored on a data server located in Ireland.[739] When the matter was brought before the Second Circuit, the Second Circuit adopted the location of data approach and upheld the sovereign interests of Ireland. The court held that an issued warrant could only be executed where data are located within the United States. The court ruled that –

> 'Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United

[737] *Microsoft Corporation v United States of America* Docket Number 14-2985 (United States Court of Appeals for the Second Circuit). Daskal summarised the facts leading to this appeal quite succinctly - In December 2013, the US government under the authority of a warrant issued by Magistrate Judge James C. Francis IV obtained in terms of the Electronic Communications Privacy Act, compelled Microsoft to disclose certain data. The data that was requested by the US government was located on a server in Dublin, Ireland but could be accessed by Microsoft employees located in Redmond, Washington. Microsoft objected to disclose the data on the basis that the US government had no authority to demand the production of data located outside its borders. It argued that the exercise of such power by the US government was impermissible extraterritorial exercise of the government's warrant authority. On the other hand, the US government argued that since the data could be accessible from within the US its powers were not extraterritorial. When the matter was brought before the lower courts, both the magistrates court and the district court Chief Judge Loretta A. Preska sided with the US government. Microsoft appealed the decision of the lower courts to the Second Circuit which reversed the judgement of the lower courts. Jennifer Daskal 'Access to data across borders: The critical role for Congress to play now' (2017) *Advance: The Journal of the ACS Issue Briefs'* 45 at 45.

[738] Section 83 (2) (c) of the ECT Act.

[739] Jennifer Daskal 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0.' (2018-2019) 71 *Stanford Law Review Online* 9 at 9.

States, regardless of the customer's location and regardless of Microsoft's home in the United States…'.[740]

The Second Circuit went on to disagree with the lower courts and held that the issued warrant was an exercise of extraterritorial jurisdiction. To arrive at this judgement, the court reasons that –

> the magistrate judge's 'narrative affords inadequate weight to the facts that the data is stored in Dublin, that Microsoft will necessarily interact with the Dublin datacenter in order to retrieve the information for the government's benefit, and that the data lies within the jurisdiction of a foreign sovereign. Second, the magistrate judge's observations overlook the SCA's formal recognition of the special role of the service provider vis-à-vis the content that its customers entrust to it…'.[741]

The Second Circuit emphasised on the importance of following MLAT channels in instances where data are located outside the United States. It was the view of the Second Circuit that after submitting a MLAT request to the relevant government, the FBI must wait for the foreign government to respond.[742] Three important points can be made out from the *Microsoft Ireland* case. First, establishing the location of data is important before exercising enforcement jurisdiction even if the crime, victim, and target of the investigation are all located within the investigating state. Secondly, location of data is important even if the data is only held in that foreign jurisdiction for other reasons like tax or lower energy costs. Thirdly, location of data remains important even if the data is encrypted and the investigating state is unable to ascertain the specific location of the data, and thus no clarity about where to direct the request for mutual legal assistance.

Apart from the decision in *Microsoft Ireland* case, there are others who support the extraterritoriality of data and the location of data approach. Scholars argue that from a factual point of view, stored data are a physical thing that is quantitatively present in the foreign state.[743] Cloud-based data resides on servers, and wherever those servers sit, they are subject to territorial assertions of jurisdiction.[744] Currie reasons that when LEA request a cloud service provider to obtain stored data, it is the same as asking a private person to obtain paper documents or any physical property from a foreign state.[745] Requesting stored data in foreign states is an extension of enforcement jurisdiction and if it is done without the foreign state's consent, this violates the foreign state's laws.[746] When LEA unilaterally access remote cloud data without permission, they violate the sovereign interests of the foreign state where the data are hosted.

[740] *Microsoft Corporation v US* at 39.
[741] *Microsoft Corporation v US* at 40.
[742] *Microsoft Corporation v US* at 41.
[743] Currie op cit note 214 at 93.
[744] Woods op cit note 212 at 734.
[745] Currie op cit note 214 at 93.
[746] Ibid at 94.

The question of cloud jurisdiction was addressed by the drafters of the Tallinn Manual. The Tallinn Manual is a flagship research initiative of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) which addresses issues on cyber operations (first edition), rules of international law governing cyber incidents (Tallinn Manual 2.0.). According to the Tallinn Manual 2.0, where a cloud service provider establishes data centres within a state, that state has sovereign authority over the infrastructure regardless of whose data are being hosted on the data centres.[747] The state also has sovereign authority over the data hosted on the data centres and any cyber activities taking place on the data centres, such as the processing of any data. The Tallinn Manual also adopts the location of data approach as it is a very convincing and effective basis to exercise jurisdiction over cloud data. The state where the cyberinfrastructure such as data centers or server farms are located should exercise jurisdiction over cloud data. State sovereignty over cyber infrastructure and activities within its territory has two international legal consequences. The cyberinfrastructure is subject to domestic legal and regulatory control by the state and the state has the right to protect cyber infrastructure and safeguard cyber activity that is in or takes place within its territory.[748]

The location of data approach has been heavily criticised by academic scholars. Daskal argues that this data location driven approach leads to a range of concerning policy[749] as it fails to consider the underlying interests the law is meant to serve.[750] This approach is criticised for undermining law enforcement agents' ability to access sought after evidence in situations where there is probable cause to do so.[751] This stymies LEA's access to data in legitimate investigations.[752] The approach does not consider competing interests in instances where a citizen or resident has committed a crime, the crime was committed locally and the target of the crime is also local. It does not matter even where LEA have the means to access the evidence. Daskal does not see the reasonableness of states going through diplomatic processes to access cloud data simply because the data of interest happens to be stored in a foreign state.[753]

An analysis of the location based approach also shows that it fails to consider normative considerations such as interests of a state in protecting its own citizens from crime.[754] Instead, crime

[747] Rule 1 and 2 of the Tallinn Manual op cit note 666.
[748] Rule 2 part 2 of the Tallinn Manual op cit note 6666.
[749] Daskal op cit note 227 at 189. Pecoraro also argues that the location of data is a problematic factor to rely upon. Commenting on the Stored Communications Act of the United States, he submits that the Stored Communications Act should be interpreted to reach data stored overseas held by electronic service providers that are subject to the US jurisdiction. Andrew Pecoraro 'Drawing lines in the cloud: Implications of extraterritorial limits to the Stored Communications Act' (2017) 51 *Creghton Law Review* 75 at 82.
[750] Daskal op cit note 227 at 197.
[751] Ibid at 189.
[752] Ibid at 227.
[753] Ibid at 197.
[754] A crime of hacking and denial of service attack may have resulted in citizens being unable to access services such as water, electricity, and internet. A state may be investigating a crime linked to child pornography or child online grooming or even human trafficking.

investigations are put on hold merely because of a service provider's decision to store data in a particular location to maximise efficiency and reduce costs.[755] One can note that this argument, though relying on the protection of human rights can potentially lead to a violation of human rights. The argument creates the assumption that investigating states only aim to protect the legitimate interests of their citizens and residents or national security interests. The argument fails to acknowledge that a drift from a location-based approach may justify actions of despotic governments who may access data of any persons of interest based on national security interests. This poses a serious and great threat to human rights as mentioned earlier. The lessons from the Snowden revelations are that massive surveillance of ordinary citizens is on an unprecedented scale by different law enforcement and national security agencies.[756] As such, governments can hide behind national security interests in accessing citizens data while subjecting citizens to unwarranted surveillance.

While the criticism against data location may be convincing, one can note that scholars tend to confuse jurisdictional principles. It should be made clear that enforcement jurisdiction over a person is different from enforcement jurisdiction over data relating to that person. In certain situations, a state may not be able to exercise enforcement jurisdiction over the data of interest. A LEA may have arrested a suspect but not have enforcement jurisdiction over the evidence of the crime. A state automatically has jurisdiction over a cybercrime committed within its territory or a cybercrime committed against its citizens or residents. This is part of the exercise of adjudicative jurisdiction[757] as well as prescriptive jurisdiction. A state cannot, however, automatically have enforcement jurisdiction over data on the basis that it is electronic evidence and can be accessible within that state. Take the crime of murder as an example, if both the perpetrator and victim of the crime are within the same state, the state has jurisdiction over the crime. If the perpetrator hides the murder weapon or CCTV footage of the crime in another country, the investigating state cannot unilaterally cross borders to retrieve the evidence in a foreign state. The investigating state would have to follow the proper MLAT channels to access such evidence. Adopting the Daskal argument would mean that the investigating state can gather evidence on foreign state's cyberspace without informing the foreign state. This interpretation of data jurisdiction violates international law and infringes on the sovereignty of a foreign state.

Arguments have also been presented that the location of data approach can yield bizarre results and subject to manipulation by nefarious players. Some organized cybercriminals are experts in their craft. They take time to study the legal and policy frameworks in different countries and identify gaps and loopholes in legal frameworks. If data location is the basis for exercising jurisdiction, cybercriminals may take every precaution to ensure they store data in states that are unwilling, or

[755] Daskal op cite note 227 at 227.
[756] Lachmayer and Witzleb op cit note 355 at 749.
[757] Chapter 3 of the Cybercrimes Act.

perhaps technologically unable, to cooperate with official government to government requests for electronic evidence.[758] This creates significant barriers for LEA investigating crimes.[759]

As will be discussed in chapter 5 of this study, one of the unintended consequences of this approach is that governments may resort to data localisation and demand that ISPs store their citizens' data within their jurisdiction.[760] Daskal pointed that efforts on data localisation and blocking provisions have been criticised on the basis that they are misguiding as they create the presumption that sovereign interests in data are coterminous with their location.[761] Since the location of data is fluid, changeable and changing, location of data should not be used as a jurisdictional basis. While Daskal may be correct in her argument that data are fluid and this cannot be coterminous with location, the scholar seems to overlook important aspects. Data jurisdiction and internet jurisdiction principles emanate from the traditional principles of jurisdiction which focuses on territory. This study submits that to arrive at a different conclusion and adopt a different approach to transborder cloud data, the starting point should be a reconsideration and reformulation of current statutory mechanisms on jurisdiction. Current cybercrime legislation revolves around territorial jurisdiction. Adopting distinct jurisdictional principles ideal for cyberspace and internet governance can only be possible if the underlying legislative instruments shift the focus from territorial jurisdiction.

c. Data location approach within South Africa's legislative framework

Section 27 of the Cybercrimes Act provides that the Criminal Procedure Act applies in addition to the provisions of chapter 4 of the Cybercrimes Act in so far that it is not inconsistent with the provisions of this chapter. This section will consider the enforcement provisions of the Cybercrimes Act, the CPA and the ECT Act. Generally, South Africa's criminal law and cybercrime laws empower LEA to exercise enforcement jurisdiction in the cloud. There are certain instances where South African law adopts the location of data approach. For instance, sections 28 – 33 of the Cybercrimes Act permit LEA to conduct certain searches and seizures of articles. For LEA to search or seize an item or object, it must fall within the definition of an 'article'[762]. The Cybercrimes Act defines an article as

'...any data, computer program, computer data storage medium or computer system which –

i. is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;

ii. may afford evidence of the commission or suspected commission; or

[758] Daskal op cit note 281 at 390.
[759] Ibid.
[760] Ibid.
[761] Daskal op cit note 227 at 197.
[762] The definition for 'an article' was first set out in Section 20 of the CPA. This is where the term 'section 20 article' is derived from.

iii. is intended to be used or is on, reasonable grounds, believed to be intended to be used in the commission,

of

(i) an offence in terms of Part I and Part II of Chapter 2;

(ii) any other offence; or

(iii) *an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic;'*

Section 28 of the Cybercrimes Act empowers LEA to search for, access or seize a section 20 article if it is 'within South Africa' (own emphasis). [763] This provision of the Cybercrimes Act applies the location of data approach. Section 29 of the Cybercrimes Act clarifies instances where an article may be searched, accessed, or seized. First, if the article is within the area of jurisdiction of the court.[764] This means that data, computer program or computer storage program which is found within the territorial jurisdiction of a court may be searched, seized, or accessed. Secondly, if an article was used or involved in the commission of an offence within the jurisdiction of the court or within South Africa.[765] This territorial jurisdiction refers to the geographical area within South Africa. Thirdly, enforcement jurisdiction can be exercised if the article is required in evidence at criminal proceedings presided over by a magistrate or judge of the High Court.[766] It is not clear whether section 29 (1) (b) of the Cybercrimes Act would apply if the article, like cloud data, is not physically in South Africa. Similar provisions on search and seizure are contained in section 21 of the CPA[767] and section 83 of the ECT Act. The courts need to be careful and ensure they have jurisdiction over an offence. If a court does not have jurisdiction over the offence, an accused can rely on a plea of no jurisdiction.[768] In *Mandela & Others*, Streicher J applied section 21 of the CPA and held that the magistrate had no reasonable grounds for believing that an offence had been committed, that the documents required were involved in the commission of offences and that the documents were on the premises of the applicants.[769]

[763] A police official may, in accordance with the provisions of this Chapter, search for, access or seizure any article, within the Republic. Section 28 of the Cybercrimes Act.
[764] Section 29 (1) (a) (i) of the Cybercrimes Act.
[765] Section 29 (1) (a) (ii) of the Cybercrimes Act.
[766] Section 29 (1) (b) of the Cybercrimes Act.
[767] A section 20 article shall be seized under a search warrant issued by a magistrate or justice, if it appears to such magistrate or justice from information on oath that there are reasonable grounds for believing that any such article is in possession or under the control of or upon any person or upon or at any premises within his area of jurisdiction. Section 21 (1) (a) of the Criminal Procedure Act.
[768] Section 106 (1) (f) of the Criminal Procedure Act. In *S v Dersley*, the accused argued plead that the court had no jurisdiction over the offence as it was committed in a different province. *S v Dersley* 1997 (2) SACR 253 (Ck).
[769] *Mandela and Others v Minister of Safety and Security and Another* 1995 (2) SACR 397 (W).

The powers enjoyed by police officials include searching any person who may be of assistance in providing the sought-after evidence. The searched person may be able to furnish any information of material importance concerning the matter under investigation. Section 29 (2) of the Cybercrimes Act permits the police, under the authority of a search warrant, to search any person who is able to furnish any information relevant to an investigation and who is nearby, uses or is in possession or direct control of any data, computer program, computer data storage medium or computer system identified in the warrant to the extent set out in the warrant.[770] Warrantless searches are also permitted if the police obtains consent from the person with lawful authority.[771] Section 29 of the Cybercrimes Act seem to focus on the location of the person who may be able to provide access to sought after electronic evidence. If the person is located within South Africa, police officials can exercise enforcement jurisdiction. While this provision makes it easier for LEA in South Africa to search a person and computer systems in South Africa, it is vague when it comes to dealing with data hosted in another country. It is not clear whether the provisions of the Act would apply to instances where a person is in South Africa while in control of a computer data storage medium or computer system situated in another country.

The Cybercrimes Act also permits a police official to use or obtain and use any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent set out in the warrant.[772] It is not clear whether the legislature also intended for LEA to use this provision to exercise their enforcement powers if the data, computer data storage medium are hosted in another country.

Section 30 of the Cybercrimes Act permits LEA to make an oral application for a search warrant. Section 30 (4) of the Cybercrimes Act provides for conditions when a warrant can be issued upon oral application provided the police official submits a written application within 48 hours after the issuing of the warrant. First, the warrant may only be issued if the magistrate or judge of the High Court is satisfied that there are reasonable grounds to believe that a warrant applied for could be issued.[773] Secondly, the is necessary in order to immediately search for, access or seize an article within their area of jurisdiction or within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence.[774] Thirdly, if it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional

[770] Section 29 (2) (d) Cybercrimes Act.
[771] Section 31 of the Cybercrimes Act.
[772] Section 29 (2) (h) Cybercrimes Act.
[773] Section 30 (4) (a) (i) of the Cybercrimes Act.
[774] Section 30 (4) (a) (ii) of the Cybercrimes Act.

circumstances, to make a written application for the issuing of a warrant or to amend a warrant.[775] Section 30 of the Cybercrimes Act also signify the location of data approach. If the article is located within the geographical borders of South Africa, then a search warrant can be applied. However, it is also not clear whether the police can rely on this provision to seize an article if the sought-after data is hosted in another country.

Warrantless searches are also permitted under section 32 of the Cybercrimes Act. To carry out a warrantless search, the police official must have reasonable belief that a search warrant will be issued if they apply for such a warrant and that the delay in obtaining such warrant would defeat the object of the search and seizure.[776] The police official may only remove or render inaccessible computer data storage, data, computer program, computer data storage medium or any part of a computer system if the official believes that a search warrant will be issued and that the delay in obtaining such warrant would defeat the object of the search and seizure.[777] When a person has been arrested by a police official, section 33 (2) of the Cybercrimes Act permits the LEA to search for a computer data storage medium or a computer system found in the possession of or in custody or under the control of the person.[778] A police official is permitted to remove or render inaccessible a computer data storage medium or a computer system. Upon the arrest of a person, a police official may only make copies or retain a copy of data or computer program or make and retain a printout of the output of data or a computer program if they believe that a search warrant will be issued, and it is not reasonably practicable to make a written or oral application for a search warrant.[779]

An analysis of the Cybercrimes Act, the CPA and the ECT Act on search warrant provisions show that enforcement jurisdiction can be exercised where the electronic evidence is within the territorial borders of South Africa. However, there is no clarity when it comes to the enforcement powers of LEA to access transborder cloud data. For instance, the wording of Sections 28 and 29 of the Cybercrimes Act are not clear whether the search of the article will be limited to locally stored data or includes data hosted on servers in another country, but which can be accessed through the seized article. The provisions do not clarify whether the enforcement powers extend to the search or seizure of data which may be hosted on data centres outside South Africa. It is not clear whether a search warrant issued in terms of the provisions of section 29 of the Cybercrimes Act or section 83 of the ECT Act can apply extraterritorially and have such expansive application. The provisions of the Cybercrimes Act are lacking in that they do not make a distinction between the device (article 20) and the data (the actual

[775] Section 30 (4) (a) (iii) of the Cybercrimes Act.
[776] Section 32 (1) of the Cybercrimes Act.
[777] Section 32 (1) (a) of the Cybercrimes Act.
[778] Section 33 (2) of the Cybercrimes Act.
[779] Section 33 (3) of the Cybercrimes Act.

evidence). In fact, the provisions of the Cybercrimes Act confuse the location of a device and location of data which can be two different things.

The search or seizure of an ICT device or IoT device, as provided for by the wording of the Cybercrimes Act does not always amount to securing the evidence accessible through the device. While an article providing access to the cloud data may be in South Africa, the evidence might still be hosted in another state where the LEA may not have jurisdiction. The lack of clarity in sections 28 – 33 of the Cybercrimes Act mean that LEA may end up accessing data which are located beyond the geographical borders of South Africa. Before the Cybercrimes Act was enacted, LEA used to interpret the CPA very widely when seizing digital evidence.[780] Based on the wording of the Cybercrimes Act, it is highly unlikely that LEA will restrict their enforcement powers to data hosted within the borders of South Africa.

Unlike in *Microsoft Ireland* case where Microsoft contested the validity of the warrants, South African courts did not adjudicate a matter where the extent of search warrants under the CPA or the ECT Act were contested.[781] This includes instances where the relevant evidence is transborder data. The Cybercrimes Act is a relatively new law, and it remains to be seen whether its jurisdictional provisions will be challenged where sought-after data is in remote cloud servers. Usually, court cases are initiated by service providers who may resist to disclose customer data on the basis that LEA do not have jurisdiction over remote cloud data. If service providers do not contest search warrants to protect the privacy of their customers, there is a risk that LEA will continue to exercise their enforcement powers over data outside South Africa. The drawback in not having service providers challenging production orders or search warrants is that this may set bad precedent on how South African laws are interpreted. This is very dangerous. It should be noted though that service providers do not have a legal obligation to resist lawful production orders or disclosure orders. With the newly enacted Cybercrimes Act failing to address the cloud data environment, it is likely that the current *status quo* will persist. Law enforcement agents will continue to access cloud data including data held outside South Africa. This study is important as it points out the loopholes in South Africa's legal system and provides recommendations to address these loopholes.

Courts play a very significant role in interpreting laws particularly in instances where there is a lack of clarity. Unfortunately, some South African courts were presented with the opportunity to address cloud data jurisdiction during criminal investigations and missed it. In *S v Miller,* police officials were able to seize article 20 devices which included cell phones and SIM cards. Though the issue of cloud services was not raised by the criminal defence, the decision of the learned Judge failed to develop

[780] Jacobus GJ Nortje and Daniel C Myburgh 'The search and seizure of digital evidence by forensic investigators in South Africa' (2019) 22 *Potchefstroom Electronic Law Journal* 1 at 13.
[781] Ibid.

search and seizure laws in line with technological developments.[782] Gamble J held that section 20 of the CPA gave the police the general power to seize anything for the purpose set out in that section. This allowed them to have access to the contents of the articles seized in the same way that the seizure of a diary or photograph album would. This study submits that the learned Judge erred in the reasoning for the decision. The Judge failed to consider the differences between physical evidence and electronic evidence. The learned Judge downplayed and underrated the amount of data and personal information that a cell phone can store or access. The court was presented with an opportunity to address the extent of police powers in cyberspace, yet it failed to consider that a cell phone can be a device used to connect and access information that may not be within the physical possession of the suspect. There is a serious infringement of privacy rights particularly when it comes to searches and seizures of electronic evidence. The learned Judge did not uphold the constitutional value of privacy and the legitimate need for avoiding abuse of police powers of searches and seizures. This study submits that the Judge failed to develop the search and seizure principles in line with the changes brought about by technological innovations.

It has been noted by some that a section 20 article must mean a physical and tangible thing and that the provisions made in the CPA should be restructured to alleviate the restrictive interpretation that articles are only physical items.[783] Bouwer seem to argue that although the CPA authorises the search of a premises for and seizure of a computer itself, it does not apply to the search of a computer and the seizure of information located on that computer.[784] Bouwer's argument that the CPA does not apply to search of information located on a computer does not address the full scope of the problem. Electronic searches and seizures are permitted under the CPA if the information is located on a computer's hard drive or internal memory. At the same time, when LEA are searching and seizing electronic evidence, they rely on the CPA, the Cybercrimes Act, and where applicable, the ECT Act. The criminal laws collectively permit LEA to seize any information (electronic seizure) stored on the hard drives or internal memory storage. The interpretation of section 20 of the CPA seem to suggest that the article must be a physical, tangible object. This may be because when the provisions of the CPA were drafted, cloud computing technologies and cloud storage were not invented yet.

While Bouwer is correct in arguing that searches and seizures do not always include information located on a computer, there are certain clarifications to be made. Bouwer's reasoning only relates to information that is remotely stored in cloud servers and does not apply to information that is stored on the internal hard drive of an IoT device. If a cell phone's internal memory contains videos and photos,

[782] Du Toit op cit note 686.
[783] Nortje and Myburgh op cit note 794 at 13.
[784] Gideon Petrus Bouwer 'Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) *South African Journal of Criminal Justice* 156 at 158.

such data may be seized as evidence. The cell phone is within the jurisdiction of the police and the data contained in the cell phone are within the jurisdiction of the police. In that regard, the location of data approach does not result in complex legal challenges. However, if the sought-after electronic evidence is stored on a cloud based storage system like OneDrive, there must be clarity on whether the police have jurisdiction over such evidence. Though the cell phone or IoT device might be within the jurisdiction of the police, the actual evidence relevant to the crime might not be within the jurisdiction of the police. This differentiation is particularly important because most IoTs no longer keep any data internally and are mere portals or gateways to access data in the cloud. For the location of data approach to be more effective, it is important to clearly stipulate the main differences between location of a device and location of data.

Bouwer correctly argued that understanding the meaning of seizure of electronic evidence is important as it dictates when and where constitutional protection will apply to the information seized.[785] This is different to the *Powell No v Van der Merwe No* case whose decision has two significant effects. First, the seizure of electronic components and the information located on such components is treated as one and the same.[786] Secondly, the legality of the seized evidence located on the computer components is explicitly connected to the seized components itself. Bouwer submitted that an inference can be made that if the computer components are illegally seized, the information found on the components has also been seized illegally.[787] What happens when an article has been seized and only used as a portal to access the cloud data? Following Bouwer's argument, it can be submitted that unlawfully accessing cloud data using devices which were unlawfully accessed results in the inadmissibility of any evidence collected.[788]

In *S v Miller*[789], the police were able to seize cell phones and SIM cards of the suspects by relying on section 20 of the CPA. As mentioned earlier, section 20 articles are not only limited to cell phones and computers, but they can also include any IoT devices. For example, wearables like a fitbit wristwatch (smart watch) can be seized as an article 20 if its geo-location data can provide evidence such as providing the geolocation of a suspect's device during the commission of a crime. *Ntoyakhe v Minister of Safety and Security* held that seize means not only to take possession of articles but also to retain them.[790] The right of retention is not unlimited and does not authorise the state to deprive persons

[785] Ibid at 167.
[786] *Powell NO and Others v Van der Merwe and Others* (503/2002) [2004] ZASCA 25; [2005] 1 All SA 149 (SCA) (1 April 2004).
[787] Bouwer op cit note 798 at 168.
[788] Ibid.
[789] *S v Miller* supra note 464.
[790] *Ntoyakhe v Minister of Safety and Security* 2000 1 SA 257 (E).

of their lawful possession of articles indefinitely. A scrutiny of the CPA suggest that the seizure of the article takes place within the territory of South Africa.

To re-iterate, criminal law in South Africa permits the exercise of jurisdiction over cloud data. Law enforcement agents have jurisdiction over electronic evidence stored on computers, computer devices and networks within their jurisdiction. Law enforcement agents have jurisdiction over cloud data hosted on cloud servers within South Africa. However, where cloud data are hosted on foreign servers, the law does not provide clarity on whether LEA can unilaterally access remote cloud data. Additionally, there is a misunderstanding that the access or seizure of an article is the equivalent to accessing data which may be accessible via the device. The current wording of sections 28 – 33 of the Cybercrimes Act seem to suggest that if the LEA has access to the device, they can access the data regardless of whether the data is hosted outside South Africa. This study submits that this approach to data jurisdiction is problematic.

d. Solutions to the data location approach under the Cybercrimes Act

This study carefully submits that a location-based approach to data jurisdiction protects human rights. The study proposes that the provisions of the Cybercrimes Act need to be revised to make a clear distinction between locally based data and cloud data hosted on foreign servers. For instance, section 29 (2) (d) of the Cybercrimes Act should clarify that the police can conduct a search if the data and stored data are locally hosted. This would involve confirming with the person in possession or under the control of such data whether the data are locally hosted or not. The provisions of chapter 5 of the Cybercrimes Act shall be complied with in instances where the data are not locally hosted. Similarly, section 29 (2) (h) of the Cybercrimes Act should also provide clear guidelines on the extent to which the police can access or seize an article. If the LEA obtains a decryption key or password, it should be made clear that they cannot remotely access data or computer data storage located in another country. By making these distinctions, the law becomes very clear and certain. With legal certainty comes the assurance that people know the laws which are applicable to their conduct and the consequences for non-compliance with that law.[791] With this knowledge, people can choose the countries where they prefer their cloud data to be hosted from. In instances where the data are not locally hosted, Chapter 5 of the Cybercrimes Act shall be applied.

Since enforcement jurisdiction is mainly exercised by LEA, the study proposes that any solutions to the limitations of chapter 4 of the Cybercrimes Act can be included in the Standard Operating Procedures. Alternatively, the regulations applicable to the Cybercrimes Act can address these challenges and provide clarity on the enforcement powers of the South African LEA. Both the SPOs

[791] Andrew D Murray 'Mapping the rule of law for the internet' in David Mangan and Lorna E Gillies *The Legal Challenges of Social Media* (2017) at 27.

and regulations should make it clear that when data are hosted on servers outside South Africa, it is outside the enforcement powers of South African LEA. South African LEA should not exercise enforcement jurisdiction over such evidence.

To sum up, this study advocates for a data location approach. Most of the sections under the Cybercrimes Act follow the data location approach, with the exception of a few provisions which have been highlighted above. Law should be promulgated to protect the legitimate interests of people, to promote business and trade. Criminals generally find new ways of committing crime. Restrictive provisions in law to circumvent criminal activity should be the exception and not the rule. If jurisdiction over cloud data is based on location of cloud servers, there is legal certainty. People know the state that has jurisdiction over their data. This would mean that people can negotiate with cloud service providers where they wish their data to be stored. Human rights activists, journalists, whistle blowers, political opposition parties and citizens from tyrant states may store evidence of human rights violations in the cloud. A data location approach protects the privacy interests of these groups. If the cloud is hosted in foreign states, their governments cannot unilaterally access this information. Any state which may want to access cloud data will be obligated to request for mutual legal assistance. This can limit the unreasonable exercise of state power over citizens data. This places the location of cloud data approach at an advantage as it promotes the protection of human rights.

e. The Belgian Approach – Give Us Everything

Chapter 2 of this study discussed that one of the intrinsic features of the cloud is the ability of data to be accessed from anywhere in the world. Digital transformation and cloud computing technologies enable people to work, study or transact remotely. The COVID-19 pandemic has also accelerated this digital transformation. Lockdown regulations passed by governments forced people to spend more time online. The question that needs more attention is whether it is necessary for LEA to burden themselves with bureaucratic processes of seeking foreign assistance when they can easily access remotely stored data. This is usually referred to as direct access to data or government hacking. Daskal justifies transnational government hacking by pointing out that LEA should be permitted to access data unilaterally if they have physical access to the device and merely accessing data via that device.[792] This question is not only for academic debate but is a growing concern in criminal procedure and law of evidence. In practice, what is the likelihood of police officers investigating a crime in a remote village in Limpopo province of South Africa to consider the potential jurisdictional challenges in accessing a suspect's iCloud files or DropBox files? Considering that investigation of cybercrime is usually carried out by specialised units within the police force, there is a high probability for these

[792] Daskal op cit note 156 at 679.

special units to know more about the challenges regarding cloud data. The same cannot be said for an ordinary police officer carrying out an investigation relating to a traditional crime.

Courts in Belgium have shed some light on the issue of cloud data jurisdiction. They interpreted cloud data jurisdiction to include the place from where the data are accessible from.[793] The courts outright rejected the location of data approach as the primary basis of exercising jurisdiction over cloud data. In the *Belgium Yahoo!* case, the court held that territoriality is determined based on where the data are accessed and received and not where they are located.[794] The court noted that the act of accessing the data did not require the Belgian police officers or magistrates or any persons acting on their behalf to be physically present abroad or require any material action to be taken abroad.[795] The court went on to hold that this coercive measure was of a limited scope and the implementation required no intervention outside of the Belgian territory.[796] Daskal views this type of government access to remote data as a minimum coercive measure with limited extent, the execution of which does not require any intervention outside the investigating state's territory.[797]

Similarly, in *Belgium Skype* case[798], the court disregarded the absence of the cloud service provider in the country. The Belgian LEA were investigating a crime and sought for both non-content and content data regarding communications between two Belgian residents. Since the Belgian residents were communicating via Skype, the authorities approached Skype to disclose the data as well as provide technical assistance to prosecutors in obtaining these communications.[799] Skype partially complied with the order and provided basic registration information. However, Skype refused to disclose content data.

---

[793] *Belgium v Yahoo!* Case No. Nr. P.13.2082.N (Court of Cassation of Belgium) 1 December 2015. The judgement was handed down in Belgian language and the writer relied on the translated version of the judgement as published in the Digital Evidence and Electronic Signature Law Review 12 (2016) 156. In November 2007, Belgian authorities were investigating a case of fraud. They sought for IP and email addresses as well as other information that would assist in identifying the suspects. In terms of article 46bis of the Belgian Code of Criminal Procedure, the Belgian authorities ordered Yahoo! To disclose the requested information. Yahoo! refused to comply and was prosecuted, convicted, and fined 55 000 Euros in damages plus an additional 10 000 Euros for each day it failed to provide the sought-after data. Yahoo! appealed making 3 arguments. First, it argued that Yahoo! was neither an electronic communication network nor a provider of electronic communication services and thus it was outside the scope of the applicable Belgian statute. Second, it argued that U.S. company that lacked any presence in Belgium, the applicable Belgian statute did not apply. Third, it argued that the production order constituted an impermissible extraterritorial application of Belgian enforcement jurisdiction. The Supreme Court of Belgium rejected Yahoo!'s arguments and upheld the conviction of the lower court. It held that Yahoo! was a provider of electronic communication services that fell within the relevant statute. The statutory disclosure obligations cover any operator or provider that actively aims its economic activities on Belgian consumers even if the company does not have a physical presence in Belgium.

[794] Daskal op cit note 227 at 193.

[795] *Belgium v Yahoo!* supra note 804 at para 6.

[796] Ibid.

[797] Daskal op cit note 227 at 193.

[798] *Skype Communications Sàrl v Belgian Institute of Postal Services and Telecommunications* Case C-142/18. English version of the judgement available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=214741&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1 accessed 19 September 2019.

[799] Belgium Skype supra note 804 para 12.

It argued that the content of communications was retained at its headquarters in Luxembourg and any request for access to the data was to be directed to the Luxembourg government.[800] After considering the parties' arguments, the court reasoned that Skype had subjected itself to Belgian jurisdiction by actively participating in the economic life in Belgium and offering services in Belgium. The court ruled that there were no Belgian investigators entering another country, and the sought-after information was turned over in Belgium.

One can note that the major differences between *Microsoft Ireland* case and the *Belgium Skype and Belgium Yahoo!* cases was that in *Microsoft Ireland*, the US government sought to access transborder data by relying on its personal jurisdiction over Microsoft who had control over the remote based data. Contrariwise, Yahoo! and Skype were not domiciled in Belgium. Belgium had to exert its jurisdiction over the companies since they offered services in and participated in the economic life in Belgium.[801] Belgium exercise jurisdiction on two grounds. First, if the service provider, regardless of where they are located, offers services such as cloud services to people in Belgium, then Belgium can exercise enforcement jurisdiction over the service provider including the data under the control of the service provider. Secondly, if the cloud data can be accessed from within the country, then Belgium can still exercise jurisdiction over the cloud data.

A similar approach was adopted by the US government in the earlier mentioned case of the *US v Gorshkov*[802] *and US v Ivanov*[803]. In these cases, the FBI were investigating various crimes committed by Russian hackers. To gather evidence against the Russian hackers, the FBI used software to obtain login credentials and access the suspects' computer servers in Russia. The hacking operation was conducted remotely by the FBI who were in Washington, US. The court in *Gorshkov* held that since there was no interference with one's possessory interest, there had not technically been a search.[804] Such an interpretation of data jurisdiction is flawed. If law officers access cloud data regardless of the location, that amounts to a search. The nature of data is that it can be accessed by various parties without affecting the possessory interests of the data owner. This makes the issue of possessory interests irrelevant when assessing jurisdictional claims over data. This study submits that if the known suspects in a crime investigation are outside the territory of the investigating state and if the sought-after data

[800] Ibid para 13 – 15.
[801] Daskal op cit note 227 at 194.
[802] *U.S. v. Gorshkov*, 2001 WL 1024026.
[803] *United States v Ivanov* No. 300CR00183AWT. 2001.
[804] Available at https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/usa/2001/united_states_v._ivanov.html?lng=en&tmpl=sherloc accessed 23 September 2019.

are outside the territory, the deployment of network investigative techniques is an exercise of extraterritorial enforcement jurisdiction.[805]

Apart from Belgium, countries like Canada have also adopted this approach to cloud data jurisdiction. In *eBay Canada Ltd v Minister of National Revenue,*[806] Justice Evans emphasised on the importance of developing law to catch up with technological changes and developments.[807] The question before the Canadian court was whether eBay Canada should disclose records of its customers to the Canada Revenue Agency where the records were hosted on servers in the United States. eBay Canada argued for the location of data approach which meant that the Revenue Agency had to follow the normal legal processes and contact the relevant authorities in the United States before the data could be disclosed. However, the court ruled in favour of Canada Revenue Agency. The court reasoned that if data can be viewed on screens in Canada and downloaded in Canada (accessible from Canada), Canada exercised enforcement jurisdiction over the cloud.[808]

The eBay judgement implies that if data are accessible and downloadable from computer screens in Canada, Canada is not exercising extraterritorial enforcement jurisdiction. The court also emphasised that even if a search for cloud data has any extraterritorial effect, such an effect would be minimal. Courts in the United Kingdom have also adopted similar approaches. In *R v Waddon*[809], the defendant was being charged of publication of pornographic content. These images were stored on servers in the United States but could be viewed by people in the United Kingdom. The court held that the publication on the website occurred both where the content was uploaded and downloaded. While this study commends this interpretation to cloud data jurisdiction particularly in instances where heinous crimes have been committed, this approach should be adopted with strict reservations as discussed further below.

f. Locating the Belgian approach within South Africa's legislative framework

The above discussion has explored how different countries apply the Belgian approach. This section considers whether South Africa's cybercrime laws have similar provisions. In the earlier discussion on location of data approach, it was mentioned that when interpreting South Africa's cybercrime laws, one can note that location of data is synonymous to location of a device. By not making a clear distinction between locally hosted data and remotely located data, chapter 4 of the Cybercrimes Act can be interpreted to mean that LEA are permitted to access remotely located data. Specific provisions such as section 29 (2) (h) of the Cybercrimes Act empowers LEA to use network

[805] Brown correctly argues that the unilateral practice of NIT undermines diplomatic relations and this can potentially trigger other states to retaliate. Brown op cit note 653.
[806] *eBay Canada Ltd v Minister of National Revenue* 2008 FCA 348, [2010] 1 F.C.R. 145 (Can.C.A).
[807] Ibid at para 42.
[808] Ibid at para 52.
[809] *R v Waddon* [2000] WL491456 (No 99/5233/Z3 CA).

investigative techniques and access data located in other jurisdictions. To reiterate, the Cybercrimes Act and the ECT Act permit LEA to access, search and seize any computer data storage medium or any information or computer system within their jurisdiction. The law does not make a distinction between remote cloud data evidence and cloud data hosted on South African soil. The law permits the exercise of unilateral access to cross border cloud data without having to go through the MLA channels.

The Belgian approach can also be identified in the RICA Act. Law enforcement agents in South Africa are permitted to intercept communications at the authority of an interception direction[810] or an archived communication-related direction.[811] When an interception direction is issued, it is served on the telecommunications service provider to intercept the communication. Most telecommunications service providers are now operating in the cloud. Cloud based communication services such as instant messaging and VOIP are increasingly becoming the norm. The challenge with cloud-based Communication as a Service is that the service provider may not be registered in South Africa or hold any licenses in terms of the Electronic Communications Act. If registered in South Africa, the telecommunications service provider could be hosting the data on foreign servers. The RICA Act is silent on whether the interception direction or the archived communication-related direction can be served in relation to cloud data hosted on foreign servers. There is nothing in the RICA Act to suggest otherwise. This means that cloud service providers may be compelled to intercept cloud data of its customers despite the data being hosted on foreign servers.

g. The Belgian approach and potential human rights violations

While the Belgian approach to data jurisdiction makes it easier for LEA to timely access electronic evidence, this approach poses serious threats to human rights. This study argues that the exercise of jurisdiction over remote cloud data as adopted by the Belgian courts is problematic. Foreign governments may end up infringing on the privacy rights of individuals. The approach is a threat to a states' sovereignty. This can potentially lead to strained diplomatic relations. When foreign law enforcement officers apply network investigative techniques to gain access of cloud data, they breach international law and established traditional norms of jurisdiction.[812] Conflict of laws is one of the dominating problematic challenges with the global data. Each state has its own laws, standards and procedures that must be complied with by LEA when investigating a crime. These laws differ from one state to the other. If foreign LEA unilaterally access cloud evidence, they may disregard laws, standards and procedures of a foreign state.[813] This includes failing to protect the interests of the nation or state

[810] Section 3 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.
[811] Section 19 of RICA Act.
[812] Brown op cit note 671.
[813] Daskal op cit note 281 at 390.

hosting the data.[814] Instead, the investigating state imposes its own baseline standards without considering the applicable privacy protections and rules governing law enforcement's access to data in the state where the data are stored.[815] Such an approach results in states not taking the necessary steps to consider any countervailing interests of other states or the interests of the data owners.[816] Such an approach would mean that certain baseline procedural or substantive protections can potentially be disregarded.

The Belgian approach is also flawed in that there is no consideration of the rights to privacy, rights to fair trial and due process of either the suspect or owners of the accessed data. If the investigating state adopts the Belgian approach, they do not need to comply with privacy laws of the place where the data are located. Despotic governments and states with poor track records on human rights protection can use this approach to repress freedoms and rights of their citizens.[817] If an investigating state is non-democratic, there is a risk of violation of rights of both the data owner and the criminal suspect. Due to the arbitrariness of cloud data, states can access data from within their territories. If any state can access cloud data, the data owners might not know the state accessing their data, the legal basis for access and the rights they can exercise against this state. If data owners have no knowledge of which governments are accessing their data, there is no democratic accountability.[818] People will not be able to know the legal basis relied on by investigating states or the reasons for accessing the data.

The Belgian approach may subject service providers to conflicting laws. Cloud service providers may be ordered to disclose cloud data by foreign governments on the basis that such cloud data are accessible from the foreign state's jurisdiction. On the other hand, the state where the data are hosted may have blocking statutes which impose restrictions on cross border transfer of data for criminal investigation purposes. For example, the GDPR does not permit cloud service providers to disclose or transfer personal data to foreign governments without the required executive orders or court orders in place. Similarly, the ECPA[819] has been criticised for being a blocking statute which acts as a shield and a sword. It prevents foreign governments from compelling data controlled by US companies (shield) and forces companies to hand over data to the US government in accordance with certain procedures (sword).[820]

There is extensive discussion around the exercise of jurisdiction over service providers who are usually private actors. The existing debate does not address the applicability of the Belgian approach in

[814] Benton op cit note 171 at 207.
[815] Daskal op cit note 281 at 390.
[816] Daskal op cit note 227 at 195.
[817] Ibid.
[818] Ibid.
[819] Electronic Communications Privacy Act of 1986 (codified as amended at 18 U.S.C. 2701-12, 3121 – 27).
[820] Woods op cit note 212 at 779.

instances where government or government owned companies are acting as service providers. In *Microsoft Ireland, Belgium Skype* and *Belgium Yahoo!* cases, the governments were dealing with private companies as cloud service providers. What is interesting to consider are instances where the cloud service provider is a foreign state-owned company. Most governments are undergoing digital transformation and there is a steady increase in the use of cloud computing services in government. The government of South Africa for example, owns a company called the State Information Technology Agency[821] (SITA) which is responsible for the provision of ICT services to government departments and public bodies. SITA has partnered with government and the private sector to migrate government service delivery to the cloud and replace traditional business models to create new ways of meeting citizens' needs in a digital world.[822] In addition, SITA has put in place the Government Public Cloud Ecosystem document (GPCE).[823] This document creates an enabling environment where traditional IT infrastructure services can be offered to different spheres of government in a modernised way. The GPCE also enables partnerships between SITA and cloud operators such as Microsoft, Amazon AWS, and Google. Such partnerships are aimed at creating value for government through the unique service offerings and support provided by such cloud operators.[824] SITA hosts most of the South African government's critical databases such as the Department of Home Affairs population databases, the financial systems, logistics and government employee databases.[825]

Apart from sought-after data being hosted by state-owned entities, the data may be hosted by private entities on behalf of governments. For instance, the South African government has concluded PPPs[826] with ICT infrastructure providers such as AWS, Microsoft, Huawei, and Google. While the

[821] SITA is an agency of ICT for government. It was created in terms of the State Information Technology Act 88 of 1998. The mandate of SITA is to improve service delivery to the public through the provision of ICTs to government departments and public bodies and to promote the efficiency of departments and public bodies through the use of information technology. SITA is responsible for creating an enabling ICT environment for government departments to provide electronic services (e-services) to the citizens of South Africa. The government is the sole shareholder of SITA with the Minister of Communications and Digital Technologies (previously Telecommunications and Postal Services) exercising the custodian rights attached to the shareholder on behalf of the state.

[822] SITA Strategic Plan op cit note 232. SITA has partnered with cloud providers like Gijima, Huawei and IBM.

[823] SITA Strategic Plan op cit note 232. In its Strategic Plan, SITA identifies the GPCE as an ecosystem of different clouds for exclusive access by South African government departments that will be owned by government and operated and managed by SITA. SITA launched its new government cloud infrastructure for South Africa. The GPCE brings together private and hybrid clouds hosted either within a government data centre or at third party data centre into one single ecosystem from where cloud services can be provisioned through a single cloud suite.

[824] SITA Strategic Plan op cit 232 at 32.

[825] SITA Strategic Plan op cit note 232 at 36. Other South African government departments using e-services include SARS, SAPS, DoJ, NPA, DCS, DSD, SANDF and DHS. Mvelase, Dlamini, Sithole and Dlodlo op cit note 266 at 153.

[826] The Public Finance Management Act, 56 of 2003 defines a PPP as "…*a commercial transaction between an institution and a private party in terms of which the private party –*
(a) performs an institutional function on behalf of the institution; and/or
(b) acquires the use of state property for its own commercial purposes; and

service provider has access to the data, it is the government that still has control over the data. If an investigating state relies on the Belgian approach and unilaterally access the data, it will be violating the sovereign interests of the government controlling the data. To access such data requires strict compliance with the internationally recognised MLA processes. As such, the Belgian approach cannot be the ideal approach to exercise enforcement jurisdiction. If there is a compelling reason to adopt the Belgian approach, such an approach should not be taken lightly.

h. Location of service provider approach

The above discussion has elaborated the two competing approaches to jurisdiction over cross border data. Apart from exercising investigative jurisdiction based on the data being located within the territory of a state or being accessible from the state, other states rely on personal jurisdiction over the service provider. The recent development in the United States elaborates more on this approach to cross border data. The United States congress recently passed the Clarifying Lawful Overseas Use of Data Act. This law was passed as a direct response to the question in *US v Microsoft Ireland* of whether a search warrant issued by a judge in a US court had extraterritorial application. The CLOUD Act addressed the issue of jurisdiction over remote cloud data. The United States recognises the importance of timely access to electronic data to combat serious crime and protect public safety. A definition for serious crimes of concern to the international community can be found in Article 5 of the Rome Statute of the ICC. These serious crimes include crimes of genocide, crimes against humanity, war crimes and crimes of aggression.[827] By law, every country can prosecute these serious crimes as they are considered as core international crimes. States can exercise universal jurisdiction where certain *jus cogens* international crimes are concerned.[828] This sought-after data relating to serious crime may be under the control or possession of US based service providers.[829] The CLOUD Act recognises that access to data outside the United States may be a challenge. One of the challenges is conflict of laws where the service provider is not permitted to disclose data by a foreign state while the US is demanding access to data.[830]

(c) assumes substantial financial, technical and operational risks in connection with the performance of the institutional function and/or use of state property; and
(d) receives a benefit for performing the institutional function or from utilising the state property, either by way of:
(i) consideration to be paid by the institution which derives from a revenue fund or, where the institution is a national government business enterprise or a provincial government business enterprise, from the revenues of such institution; or
(ii) charges or fees to be collected by the private party from users or customers of a service provided to them; or
(iii) a combination of such consideration and such charges or fee."

[827] Article 5 of the Rome Statute of the International Criminal Court adopted and entered into force on 1 July 2002.

[828] Joke Ruelens *Universal jurisdiction: an analysis from a comparative and international law perspective*. *A future for universal jurisdiction over serious crimes under international law?* (unpublished LLM thesis, University of Gent 2016) 1 at 7.

[829] Section 102 (2) CLOUD Act.

[830] Section 102 (4) and (5) CLOUD Act.

In terms of the CLOUD Act, US service providers are required to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the location of the data.[831] The application of the CLOUD Act extends not only to US-based service providers but also to any foreign electronic communications service provider and foreign remote computing service provider.[832] A service provider is permitted to refuse to disclose data by filing a motion to quash the legal process if it reasonably believes that the customer or subscriber is not a US citizen or resident.[833] A motion to quash the legal process may also be filed if the required disclosure would create a material risk that the service provider would violate the laws of the qualifying foreign government.[834] In other words, US LEA cannot use the provisions of the CLOUD Act to access data of non-US citizens and residents.

The CLOUD Act permits the United States to enter into executive agreements with a qualifying state.[835] The first CLOUD Act agreement was concluded between the UK government and the US.[836] If there is an executive agreement in place, LEA can directly approach the service provider to disclose data. An executive agreement is only concluded if the US Attorney General and Secretary of State have determined and submitted a certification to the US Congress. The submission must show that the domestic law of the foreign government affords robust substantive and procedural protections for privacy and civil liberties considering the data collection and activities of the foreign government that will be subject to the agreement.[837] The submission must also show that the foreign government has adequate substantive and procedural laws on cybercrime and electronic evidence as demonstrated by being a party to the Cybercrime Convention.[838] Swire and Daskal correctly noted that the CLOUD Act 'sets the stage for ongoing public debates about privacy and human rights standards for government access to data'.[839]

The CLOUD Act has a different interpretation to data jurisdiction from the Second Circuit decision in *Microsoft Ireland* case. Instead of a blanket ban to jurisdiction over cloud data abroad, the CLOUD Act makes it clear that the United States government can access data if it belongs to citizens of the United States. Daskal correctly notes that the CLOUD Act implicitly accepts target location and nationality as grounds for asserting sovereign control, while rejecting data location, in and of itself, as

[831] Section 103 CLOUD Act.
[832] Section 103 CLOUD Act – subparagraph (h) (2) (A).
[833] Section 103 CLOUD Act – subparagraph (h) (2) (A) (i).
[834] Section 103 CLOUD Act – subparagraph (h) (2) (A) (ii).
[835] Section 105 CLOUD Act.
[836] Agreement between the Government of the USA and the Government of the UK of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (2019).
[837] Section 105 CLOUD Act amends Chapter 119 of title 18, United States Code by adding section 2523.
[838] Ibid.
[839] Peter Swire and Jennifer Daskal 'What the CLOUD Act means for privacy pros' (2018) IAPP blog 26 March 2018. Available at https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/ accessed on 12 May 2021.

sufficient grounds for delimiting access.[840] Daskal also points out that the CLOUD Act preserves the availability of the common law comity claims in terms of which service providers can refuse to disclose data if compliance with the warrant would generate a conflict with foreign law and the new-statute based motion to quash is not available.[841] If a foreign government has an executive agreement with the United States, the foreign government can bypass the MLAT system in their investigation of serious crime on non-US citizens and residents and directly request sought after communications from US based providers. However, if the sought-after evidence belongs to US persons or the communications content is physically located in the US, those requests will still need to go through MLA system.[842]

The CLOUD Act seems to be a promising piece of legislation in place to assist in addressing the slow process on MLATs. However, with the recent *Schrems II* judgement[843], it is highly improbable that countries with strict data protection laws, like members of the EU, will be forthcoming in entering into executive agreements with the United States. South Africa's data protection law is similar to the Data Protection Directive, a predecessor of the GDPR. There is a likelihood that the South African government may be reluctant to enter into any agreements with the United States due to the international effects of the decision in *Schrems II*.

The European Union have a framework similar to the CLOUD Act, the EU e-Evidence Regulation and Directive[844]. Some of the objectives of the e-Evidence Regulation and Directive include speeding up the process for securing and obtaining evidence stored by service providers in other jurisdictions.[845] The proposal also seeks to provide complimentary mechanisms to the European Investigative Order Directive.[846] In terms of the EIO Directive, judicial authorities of one state may communicate with those of another state during criminal investigations and there are standardised forms to be used with prescribed time frames for deadlines.[847] This EU e-Evidence Directive shifts the focus away from the location of data as the key determinant of jurisdiction. It enables the requesting government to directly compel production of data from providers located in another member state, and thereby bypass the otherwise applicable requirement that it first gain the assistance and cooperation of the host government to access sought-after data.[848]

---

[840]Daskal op cit note 147 at 1036.
[841] Ibid at 1037.
[842] Ibid 145 at 1039.
[843] *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties*, Case C-311/18.
[844] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD).
[845] Ibid at 2.
[846] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters.
[847] Laviero Buono 'The genesis of the European Union's new proposed legal instrument (s) on e-evidence: Towards the EU Production and Preservation Orders' (2019) 19 *ERA Forum* 307 at 308.
[848] Daskal op cit note 147 at 1040.

At the African Union level, the Malabo Convention also contains a similar provision. Article 31 (3) (a) of the Malabo Convention provides that –

'State parties shall take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system'.[849] One of the weaknesses with the Malabo Convention is that it failed to include a 'requirement for judicial oversight to strengthen the protection of the right to privacy and restrain political influence on data management, specifically data in transit, storage, cloud or at rest.'[850]

i. Location of service provider approach in the South African context

In terms of South African law, an electronic communications service provider is required to aid police officials investigating a crime. The type of support that police officials receive from a service provider depend on a case-by-case basis. Section 34 of the Cybercrimes Act explains the role of a service provider in a cybercrime investigation. If a service provider has control over data, computer program, computer data storage medium or computer system, LEA can request for technical assistance or any other assistance as may be reasonably necessary in order for police officials to search for, access or seize an article.[851] The type of technical assistance may include providing the LEA with passwords, decryption keys, or access codes to the sought after information. However, this provision does not clarify whether the assistance is limited to data or computer program, computer system and computer data storage medium physically located in South Africa.

A service provider may also provide real-time communication related information in respect of a customer in compliance with the requirements set out under the RICA Act.[852] A service provider may also respond to requests for preservation of data or preservation of an article. In cases of emergency, a specially designated police official may issue an expedited preservation of data direction to a service provider.[853] To comply with this direction, the service provider must preserve the current status of data,

[849] Article 31 of the Malabo Convention.
[850] The Zimbabwean, op cit note 161.
[851] Section 34 of the Cybercrimes Act provides that an ECSP, financial institution or person other than the person who is suspected of having committed the offence which is being investigated, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer program, computer data storage medium or computer system that is subject to a search authorised in terms of section 29 (1), if required, provide technical assistance and such other assistance as may be reasonably necessary to a police official or investigator in order to search for, access or seize an article.
[852] Section 40 Cybercrimes Act.
[853] Section 41 of the Cybercrimes Act provides that a specifically designated police official may issue an expedited preservation of data direction to a person, ECSP or financial institution. The person could be an ECSP or financial institution must be in control of data, which is relevant to, which was used or may be used in, for the purposes of or in connection with, which has facilitated or may facilitate, or which may afford evidence of the commission of a cybercrime.

not to deal in any manner with data, or to deal in a certain manner with data in order to preserve its integrity.[854] In any other situation, the police official may approach a court for a preservation of evidence direction.[855] The preservation of evidence direction must direct the person or electronic communications service provider (ECSP) to preserve the status of an article, not to deal in any manner with an article, or to deal in a certain manner with an article to preserve its availability or integrity.[856] The provisions of section 42 of the Cybercrimes Act are quite useful in limiting the enforcement powers of LEA. The order authorises a service provider to only preserve the data and not to do anything else with the data. This means that the LEA are not able to exercise some of their enforcement powers such as removing the data, rendering it inaccessible, making copies of the data or retaining copies or printouts of the data.

Once data or an article has been preserved, the Cybercrimes Act allows for a magistrate or judge on written application by a police official to issue a disclosure of data direction.[857] Section 44 (5) provides that the disclosure of the data direction must direct the person, ECSP or financial institution to provide data identified. The direction must also set out the period within which the data identified must be provided and may specify conditions or restrictions relating to the provision of authorised data.

Section 31 of the Cybercrimes Act provides that any police official may execute a search warrant if the person who has lawful authority to consent to the search for, access to, or seizure of the article in question consents, in writing, to such search, access or seizure. However, the Cybercrimes Act does not clarify on what is meant by lawful authority over data. This lack of clarity may be challenging in the case of cloud data where there are multiple players providing a service. As mentioned in chapter 2 of this study, there could be different players offering cloud services from IaaS, PaaS, and SaaS. The complexities of cloud data are that at times the cloud service provider does not have control over cloud data. If a cloud service provider does not have control over cloud data, they are not able to provide meaningful assistance to LEA.

Several foreign companies are offering services to South African citizens and residents but do not have offices within South Africa. A lot of technology companies have mobile applications (Apps) which are used by South Africans despite the company not having any legal presence in South Africa. It is not clear whether the provisions of the Cybercrimes Act on data preservation and data disclosure

[854] Section 41 (4) of the Cybercrimes Act provides that an expedited preservation of data direction must direct the person, ECSP or financial institution affected thereby, from time to time of service of the direction and for a period of 21 days to preserve the current status of, not to deal in any certain manner with the data referred to in the direction in order to preserve the availability and integrity of the data.
[855] Section 42 of the Cybercrimes Act provide that the magistrate or judge must on reasonable grounds believe that any person, ECSP or financial institution may receive, is in possession of or is in control of an article relevant to, which was used or may be used in, for the purpose of or in connection with, which has facilitated or may facilitate, or which may afford evidence of the commission of the cybercrime.
[856] Section 42 (3) Cybercrimes Act.
[857] Section 44 (1) Cybercrimes Act.

directions can be applied to foreign based service providers. Unlike the CLOUD Act which clarifies that it applies to U.S. based companies, the Cybercrimes Act is silent on this matter.

One challenge with the location of service provider approach is that it can potentially infringe on foreign states' enforcement jurisdiction or police activity on behalf of the investigating state. Currie notes that the question of whether it is a breach of international law for the courts of one state to compel private parties to disclose documents located in another state is one that predates the popular use of electronic data storage or the internet.[858] Currie notes that such orders have always been viewed as intrusive upon domestic sovereignty of a targeted jurisdiction. The result was jurisdictions enacting blocking statutes to prevent the companies from complying with the foreign orders.[859] Currie observes that the issue still persists even outside cybercrime setting.[860] Cloud storage has made it more difficult to disclose the contents of companies cloud storage (or easier to refuse to comply, depending upon one's perspective), due to concerns about infringing the laws or sovereignty of the state in which the cloud storage facility resides.[861]

The location of a service provider seems to have been part of the deciding factors that a Canadian court considered before passing its judgement in *eBay v Canada*. Since eBay (the service provider which possessed and controlled the data) was within the Canadian territory, the Canadian government exerted its authority. Currie laments over Canada's position that jurisdiction over individuals who possessed or controlled the data is sufficient jurisdiction to order production or disclosure of data. He argues that this measure was taken seemingly without much consideration of whether it was consistent with international law or without recognition that Canada itself had opposed such measures before the US Courts.[862]

A location of service provider approach may not yield intended outcomes for developing states like South Africa. As will be discussed in chapter 5 of this study, a lot of cloud service providers are foreign entities operating in South Africa and other African countries. These companies may not have any physical or legal presence in South Africa. Most tech companies are American owned entities. Woods notes that since most internet and technology companies have offices in America as well as other foreign countries, America automatically has personal jurisdiction over these companies.[863] The United States is thus placed at an unfair advantage in that it can at any time order the disclosure of data of interest from these service providers. While the CLOUD Act seeks to provide clarity on how the United States government will exercise jurisdiction over cloud data, one cannot overlook the Snowden

[858] Currie op cite note 214 at 84.
[859] Ibid at 85.
[860] Ibid.
[861] Yamri Taddese 'Focus: Cloud Services Create Challenges fore-discovery' Law Times (7 December 2015).
[862] Currie op cit note 214 at 86.
[863] Woods op cite note 212 at 748.

revelations. There remains a possibility that the US government can still access any data hosted or controlled by US service providers. The views by Svantesson challenge the dominance of countries like the US and its unfair advantage in exercising jurisdiction over service providers. Svantesson recommends that lawmakers in countries that commonly influence policy and law developments globally should conduct a global south impact assessment. This assessment is aimed at assessing the impact of certain approaches on the global south and what happens when the global south adopts such approaches.[864] Such an assessment is highly to indicate that global south countries will not be able to exercise jurisdiction over most service providers as they may not have any physical or legal presence in these countries. This makes the location of service provider approach a weak basis to exercise jurisdiction over cloud data.

Whilst this approach may not be the best approach for most countries[865], it should be noted that requests for data submitted to service providers provide an additional layer of protection. Service providers usually assess the extent of a request, the lawfulness of the request and the relevance of the data before disclosing the data. Such additional steps help to protect customer data or resist government overreach.[866] The cases such as *Microsoft Ireland* or *Belgian Yahoo!* are good examples of the extent companies take to protect customer data from unreasonable disclosure to LEA. As will be discussed in chapter 5 of this study, most governments blame service providers for resisting to disclose evidence during crime investigations. By contrast, when government actors are doing the searches directly, there is no additional third party to resist or raise concerns regarding a conflict of laws.[867]

j. The hybrid approach to data jurisdiction

The above discussion has shown that while states may have a dominant approach on data jurisdiction, they also tend to blend different approaches depending on the circumstances. Certain provisions in a piece of legislation may relate to the location of data approach and other sections of the same law may relate to the Belgian approach or the location of service provider approach. This study considers this hybrid approach. The Cybercrime Convention is a useful example to demonstrate how this hybrid approach apply to remote access to transborder data. As mentioned in chapter 3 of this study, the Cybercrime Convention is the leading global treaty on cybercrimes. The use and implementation of the Convention are facilitated by the Cybercrime Convention Committee (T-CY) established under Article 46 of the Budapest Convention. In 2012, the T-CY set up the Ad hoc Subgroup on Jurisdiction and Transborder Access to Data. In December 2014, the T-CY also completed an assessment of the mutual assistance provisions of the Convention on Cybercrime and adopted a set of recommendations,

[864] Svantesson op cit note 104 at 64.
[865] As will be discussed in chapter 5, a lot of technology companies are from the United States. Very few companies are from European countries or African countries.
[866] Daskal op cit note 156 at 697.
[867] Ibid.

including recommendations to establish the 2nd Additional Protocol to the Cybercrime Convention.[868] Subsequently, a Working Group on Criminal Justice Access to Evidence Stored in the Cloud, including through Mutual Legal Assistance (the Cloud Evidence Group) was established in 2015. One of the main challenges identified by the Cloud Evidence Group were related to cloud computing, territoriality, and jurisdiction. The 2nd Additional Protocol was signed in November 2021 and was opened for signature from May 2022. Chapter 6 of this study discusses in detail the solutions to data jurisdiction as envisaged by this new law.

Prior to the 2nd Additional Protocol, cross border access to data was one of the main issues that the Convention sought to address. Article 18 and Article 32 of the Cybercrime Convention deals with some aspects of enforcement jurisdiction in the cloud. The Budapest Convention permits unilateral access to cross border cloud data under strict circumstances. There are two grounds that a party may exercise extraterritorial enforcement jurisdiction without the need of consent of the other state party. First, if data are publicly available regardless of where the data are geographically located.[869] This qualification can fall within the Belgian approach to jurisdiction. States have jurisdiction over publicly available cloud data. If a cybercriminal commits a crime and the evidence of the crime is publicly available, there is no need for state parties to follow mutual legal assistance to access and seize the evidence.

As mentioned earlier, South Africa's Cybercrimes Act is silent on whether LEA have jurisdiction over cross border cloud data in general. Yet, section 45 of the Cybercrimes Act carefully considered cloud jurisdiction in respect of publicly available data. Section 45 of the Cybercrimes Act authorises LEA to receive, obtain or use publicly available data regardless of where the data are geographically located. This provision recognises that data may be located outside South Africa, unlike other provisions which are silent on this matter. It allows for the police to access the evidence if it is publicly available. It is not clear why the law permits for extraterritorial jurisdiction for publicly available data. It could be that by posting the data on a public platform, the data owner may have inadvertently consented to the use of such data by anyone, including LEA.

Secondly, a party can also access or receive stored computer data located in another party if the party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the party.[870] The phrase *'located in another party'* means that the cross-border access to

[868] The 2nd Additional Protocol relates to the disclosure of subscriber information. It provides that Each Party shall adopt legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the information is needed for the issuing Party's specific criminal investigations or proceedings.
[869] Article 32a Cybercrime Convention.
[870] Article 32b Cybercrime Convention.

cloud data is permissible if the foreign state where the data are located is a signatory to the Budapest Convention. Article 32 (b) does not permit states to compel service providers to disclose cloud data they host in foreign jurisdictions which are not signatories of the Convention. Article 32 (b) seem to favour the location of data approach and to some extent, the location of service provider approach. If the sought-after data are located within the territory of a state party, then the investigating state party can unilaterally access the data. This also means that LEA in the state parties cannot unilaterally access cloud data hosted on servers in non-signatory countries. For example, France as a signatory to the Budapest Convention can rely on Article 32 (b) to unilaterally approach a service provider for assistance in obtaining data hosted in the Netherlands, also a signatory to the Budapest Convention. However, France cannot rely on the same article to approach a service provider in France to disclose data hosted in China as China is not a party to the Cybercrime Convention.

What is also clear is that Article 32 (b) indirectly rejects the Belgian approach to cloud jurisdiction in respect of any data apart from publicly available data. The mere fact that cloud data are accessible from a state party does not permit the state party to exercise jurisdiction over the cloud data. For a state party to exercise jurisdiction over cloud data located in another state party, it must obtain voluntary consent from the service provider or person with lawful authority to disclose the data. This means that government hacking or covert searches by government are not covered under this Article 32 (b). The article also signifies that location of data is still very important when deciding on which state has jurisdiction over cloud data.

Commenting on Article 32, the T-CY, in its Guidance Note on transborder access to data, noted that Article 32 (b) is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances.[871] The T-CY Guidance Note also helped to shape the 2nd Additional Protocol. Chapter 6 of this study shall discuss the 2nd Additional Protocol in detail and how it will change our understanding of remote data jurisdiction for criminal investigations and prosecutions. Article 32 (b) by implication may be used if it is known where the data are located.[872] Article 32 (b) would not however, cover situations where the data are not stored in the territory of a state party or where it is uncertain where the data are located.[873] A party may not use Article 32 (b) to obtain disclosure of data that is stored within its territory.[874] Instead, a party would have to rely on its domestic laws to access locally hosted data. Article 32 (b) neither authorises nor precludes other situations.[875] Thus, in situations where it is unknown whether certain data are stored in

[871] October 2014 T-CY Guidance Note on Transborder Access to Data at 16.
[872] Ibid at 19.
[873] Ibid.
[874] Ibid.
[875] Ibid.

another party, parties may need to evaluate the legitimacy of a search in the light of domestic law, relevancy of international law principles or considerations of international relations.[876]

It should be noted that some of the signatories to the Budapest Convention still have reservations on Article 32. For example, Slovakia has stated that notwithstanding the article, it considers that its domestic courts must still approve any request for data.[877] Russia, though a member state has not ratified the Budapest Convention and cited Article 32 and the potential for damage to the sovereignty and security of member states and their citizens.[878] The reservations that states have in the application of Article 32 (b) are reasonably justified as discussed earlier. Most states view foreign governments' unilateral cross border access to data within their territory as a potential intrusion.[879] Territorial sovereignty and control is always key in any discussion of inter-state interaction and the criminal law is where states are at their most guarded.[880]

From an international law perspective, it is justifiable for a state to have concerns over unilateral access to data. Chapter 3 of this study discussed that the reason why the perpetrator of the 'I love you' virus was not extradited to the United States was because the Philippines had not criminalised the dissemination of malicious software. For an investigating state to be able to rely on Article 32 (b), the unlawful conduct must be criminalised in both the investigating state and the foreign state. Otherwise, the foreign state may not be interested in being unwittingly implicated in a prosecution of conduct that it does not view as criminal.[881] Currie also observes that because of sovereignty interests, a state may want to retain the capacity to refuse to cooperate or allow its territory to be used for enforcement activity. This concern usually arises in instances where a state views foreign prosecution (or some aspect of it) as contrary to its *ordre public.* For example, the pursuit of a political dissident under the guise of a criminal prosecution or the suppression of forms of speech that the target state views as being legitimate.[882] As discussed earlier, individual human rights are at risk of being violated in cases where foreign states can exercise jurisdiction of cloud data. Some states prefer that their own judiciaries or other authorities approve any evidence gathering on their territories instead of leaving the process in the hands of foreign LEA.[883]

The person who is lawfully authorised to disclose the data may vary depending on the circumstances, laws, and regulations applicable.[884] It may be an individual person providing access to

[876] Ibid.
[877] Currie op cit note 214 at 78.
[878] Clough op cit note 57 at 719.
[879] Currie op cit note 214 at 78.
[880] Ibid.
[881] Ibid.
[882] Ibid.
[883] Ibid.
[884] October 2014 T-CY Guidance Note on Transborder Access to Data at 20.

his or her email account or other data that he or she stored.[885] It may also be a legal or juristic person. Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their user's data under Article 32. The Guidance Note submits that service providers may be holders of the data but not having control over the data which means they will not be able to consent.[886]

The Guidance Note also shed some light on the location of the person consenting to provide access to or disclose data. It notes that the standard hypothesis is that the person providing access is physically located in the territory of the requesting party.[887] However, multiple situations are possible, the person could be in the territory of the requesting state, the disclosing state or a third country. It is conceivable that the person is in the territory of the requesting law enforcement authority when agreeing to disclose or providing access. The person may also be located in the country where the data are stored when agreeing to disclose and providing access.[888] The person may also be physically located in a third country when agreeing to cooperate or when actually providing access.[889] If the person is a legal person, this entity may be represented in the territory of the requesting law enforcement authority, the territory hosting the data or even a third country at the same time.[890] The committee pointed out that it should be taken into account that many parties would object and some even consider it a criminal offence if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation.[891]

Article 18 of the Cybercrime Convention deals with jurisdiction over subscriber information. State parties can issue a production order to a person (this could be a cloud service provider) to submit specified computer data. The provision further qualifies that the person must be in its territory and be in possession or control of the computer data.[892] Where a cloud service provider is in the territory of a state party, the state party can exercise jurisdiction over the service provider. Secondly, the service provider must be in possession or control of the cloud data. This means that a production order is only effective if the cloud provider has control over the cloud data. Article 18 (1) (b) also provides that the production order may be against a service provider offering services in the territory. This means that even in cases where the service provider has no physical presence within the state, they can still be ordered to produce the requested information if they offer services in the territory.

[885] Ibid.
[886] Ibid.
[887] Ibid.
[888] Ibid.
[889] Ibid.
[890] Ibid.
[891] Ibid.
[892] Article 18 (1) (a) Budapest Convention.

Part one of Article 18 requires state parties to establish mechanisms by which LEA can order a person in their territory to submit specified computer data in that person's possession or control.[893] This applies to both content and non-content data. Part two of Article 18 requires that state parties establish mechanisms by which LEA can order a service provider offering its services in the territory of the party to turn over subscriber information in that service provider's possession or control. The provision itself is silent as to whether there are any territorial limits on what can be produced.[894] Article 18 Guidance Note rejects a data location-driven approach to disclose obligations as it makes it explicit that providers who have control or are in possession of subscriber information should disclose it regardless of where the subscriber information is hosted from.[895] The note clarifies that any provider that enables persons in the territory to use its service and orients its activities towards those persons is subject to the state party's jurisdiction.[896] Daskal submits that this is akin to the broad jurisdictional hook adopted by the Belgian courts in the *Belgium Yahoo!* and *Belgium Skype* cases, although limited to situation in which the government is seeking subscriber information only.[897]

Daskal submits that Article 18 Guidance Note endorses the authority of state parties to compel the production of subscriber information from extraterritorially located service providers, it also supports the continued right of states to block such requests.[898] In other words, Article 18 Guidance Note endorses states' authority to reach service providers beyond their borders, yet refuses to disclaim government efforts to block such foreign government reach.[899] Daskal points out that the Cybercrime Committee was both unwilling and unable to endorse authority of foreign governments to compel the production of communications content held by a subscriber outside their borders.[900] This position adopted by the Cybercrime Committee signified that communications content is often deemed more sensitive and thus deserving of stronger protections than subscriber information.[901] The position also signifies the stickiness of the linkage between sovereignty and territory, irrespective of other normative and practical considerations.[902]

V. CONCLUSION

At this stage, one may wonder which of the discussed approaches yields a balanced outcome. One should admit that deciding on the right approach to jurisdiction over cloud data is a mammoth task. At

[893] Daskal op cit note 227 at 199.
[894] Ibid.
[895] Ibid.
[896] Ibid at 200.
[897] Ibid.
[898] Ibid.
[899] Ibid.
[900] Ibid at 201.
[901] Ibid.
[902] Ibid.

the outset of this project, the hypothesis was very clear – jurisdictional principles must be reformulated to accommodate the technological changes and developments particularly cloud computing technologies. This hypothesis leaned towards the discourse on data exceptionalism where new rules suitable for cyberspace are introduced to address data. However, after a comprehensive and critical analysis on the views of territorialists, this study finds that there is more cynicism about the relevance of adopting new jurisdictional principles. Due to differences in domestic laws and policies, political agendas, and economic strategies, it is pellucid that states are not going to agree on the same jurisdictional principles to apply to cloud data. An analysis of the international efforts to combat cybercrime together with digital policy frameworks indicates that territory is still a relevant basis for states to exercise jurisdiction. Despite the calls for revisiting the jurisdictional principles applicable to data and possibly reformulating most suitable principles, states have remained adamant to sink their jurisdictional claws over data where the data infrastructure is located within their territories. This could be because of the importance for states to preserve state sovereignty in the digital era.

While the Belgian approach may be more effective especially when states are investigating serious crimes which are time sensitive, this approach is subject to potential abuse by governments. Data location and territoriality principle is and remains the basis for exercising jurisdiction. While academics and scholars may stimulate debate on the importance of cyber-centric laws to deal with cybercrimes and data jurisdiction, one should not overlook the importance of government policy on these issues. If governments are not willing and comfortable in partaking new principles to address cyberspace, any proposal for a reformulation of principles will be met with resistance. At the same time, the practice of governments over time may create state practice and can potentially contribute to international customary law rulemaking.

This study agrees with the current status quo over publicly accessible data that any state can exercise enforcement jurisdiction over publicly available data. The territoriality principle should be observed even in the digital space as it is the realistic approach which is also in line with political will of many countries. In practice, LEA should be permitted to order service providers to preserve any data that may be relevant to an investigation. After data has been preserved, LEA could then approach the relevant state for permission to seize the data or to access the data. This is reasonable for a plethora of reasons. First, once the data are preserved, the suspect is not able to alter the data or delete the data or move it to another country. The evidence is preserved and remain available for LEA to be able to access it when the relevant authorisations have been granted. Data preservation also gives LEA adequate time to investigate the state with the appropriate jurisdiction over the data and to prepare applications for MLA. Data preservation serves the interests of the state in investigating and prosecuting crime. It also serves the interests of the victims in bringing the perpetrator to justice. Service providers similarly benefit as they are not caught up in a web of conflict of laws.

The different types of data may require different types of assistance. If LEA are only looking for subscriber information, the service provider should provide access to the data despite the location of data. Subscriber information is very limited and there is no serious invasion of privacy when such data are disclosed. However, if the sought-after data are content data, then the necessary MLA processes should be followed. Chapter 6 of this study explores these solutions and recommendations in greater detail.

CHAPTER 5: THE ROLE OF DATA LOCALISATION IN RESOLVING THE DATA JURISDICTION DEBATE

I. INTRODUCTION

In the global and interconnected world, data are indispensable. Importantly, the sharing of data between service providers and customers in different countries is the backbone of international trade.[903] The COVID-19 pandemic facilitated the growth in digital trade and cross border data flows even when global GDP growth rates plummeted.[904] International discussions on data localisation are mainly in the context of international trade, preferential trade agreements and the negative economic implications.[905] There is very little discussion on data localisation and its relevance for access to information (evidence) for criminal investigation purposes. There are five branches of law under which data are regulated. These branches are data protection law, competition law, cybersecurity law, intellectual property law and electronic communications and transactions law. This study focuses on cybersecurity and data protection laws. Apart from benefitting the digital economy, cloud computing technologies and cross border data transfers are crucial in crime investigations.[906] Crime investigators and LEA need to gather evidence for purposes of a successful prosecution. This evidence can be in the form of electronic cloud data stored on remote cloud servers. As enunciated in chapter 4 of this study, the powers of LEA to conduct searches and seizures of data hosted in foreign territory may be limited. This may be because the foreign state where the data are hosted may have restrictive statutes preventing service providers from directly assisting foreign LEA. Due to the slow processes of mutual legal assistance treaty channels, investigating states may end up getting frustrated in failing to investigate and prosecute crime. To avoid these hurdles, states may resort to implementing data localisation measures which are aimed at making data easily accessible for law enforcement purposes.[907] When a country needs access to cross border evidence and is denied access, such a country may look at data localisation as a solution.[908]

Criminal justice interests, among others, have motivated a lot of countries to adopt data localisation laws.[909] One of the justifications for data localisation measures is that when data or copies of data are locally hosted, governments can demand disclosure without regard to foreign substantive

[903] Recital 101 of the GDPR recognises that transborder data flows outside the EU are necessary for the expansion of international trade and international cooperation.
[904] Kholofelo Kugler 'The impact of data localisation laws on trade in Africa' (2021) *Mandela Institute Policy Brief* (08) 1 at 1.
[905] Javier Lopez Gonzalez, Francesca Casalini and Juan Porras 'A preliminary mapping of data localisation measures' June 2022 OECD Trade Policy Paper 1.
[906] H Jacqueline Brehmer 'Data localization: The unintended consequences of privacy litigation' (2018) *American University Law Review* 927 at 944.
[907] Woods op cit note 212 at 751.
[908] Murdoch Watney 'Analysing different approaches to cross border electronic evidence data sharing in criminal matters' (2019) *14th International Conference on Cyber Warfare and Security* (ICCWS2019) 484.
[909] Daskal op cit note 147 at 1047.

rules and procedural standards.[910] This is because states can exercise enforcement jurisdiction over local data infrastructure. In such instances, it is easier for LEA to access data stored locally than it is for them to access data in another jurisdiction.[911] They will not need to seek permission from a foreign state or wait prolonged periods for such a request to be processed. The discussion in chapter 4 has demonstrated that territory remains to be the determinative factor over data jurisdiction. It is a matter of policy for many states to either require copies of data to be stored on local data servers or prohibit data from being transferred to foreign data centres. The preceding chapters of this study have discussed the jurisdictional challenges presented by cloud computing technologies during cybercrime investigations. This chapter demonstrates that the difficulties in accessing remote evidence has resulted in some states resorting to data localisation.

The underlying theme of the chapter will highlight the role played by data localisation measures in the emerging issue of data sovereignty or digital sovereignty. This chapter discusses some of the reasons why data localisation measures are implemented. It considers the underlying policy goals for implementing such measures and assesses whether there are any other less disruptive ways to achieve same goals. Whilst acknowledging the different objectives and justifications for data localisation measures, this discussion is limited to data localisation measures as a justified response to the problem faced by LEA in accessing cross border data. With this research project focused on cybercrime investigations in South Africa, the chapter also discusses South Africa's position on data localisation with the aim of interpreting South Africa's approach to cloud data jurisdiction. The chapter notes that South Africa as a democratic state has a legitimate interest in setting limits and procedures regarding how to access relevant cloud evidence or how foreign governments access its citizens data. This discussion is meant to answer the question of whether data localisation measures solve the jurisdictional challenges of remote data. The chapter engages existing literature on data localisation and its effects on privacy interests and citizens' rights. The discussion assesses if there are any other restrictions to transborder data flows which are proportionate to the risks presented. The chapter also adopts a comparative analysis of data localisation measures in other jurisdictions.

II. DATA SOVEREIGNTY AND DATA LOCALISATION

Data sovereignty is still a nebulous term.[912] Some define data sovereignty as the highest jurisdiction over all data produced by individuals, enterprises, and related organisations within the jurisdiction of a

[910] There are three consequences for slow MLA systems. First, states may resort to unilateral extraterritorial assertion of compulsory disclosure obligations. Secondly, states may pursue expanded hacking or broad decryption mandates. Thirdly, states may resort to data localisation measures. Daskal op cit note 733 at 47. Chapter 4 of this study has expanded on the two consequences and this chapter will focus on data localisation.
[911] Emily Wu 'Sovereignty and data localization' (2021) *The Cyber Project Harvard Kennedy School* 1 at 12.
[912] Carol M Celestine 'Cloudy skies, bright futures: In defense of a private regulatory scheme for policing cloud computing' (2013) *University of Illinois Journal of Law, Technology & Policy* 141 at 148.

country.[913] The AU Data Policy Framework defines data sovereignty as the control that a state has over data generated in or passing through its national internet infrastructure.[914] The Policy Framework identifies two types of data sovereignty, weak data sovereignty and strong data sovereignty. Weak data sovereignty refers to private sector-led data protection initiatives with an emphasis on the digital rights aspects of data sovereignty, while strong data sovereignty favours a state-led approach with focus on safeguarding national security.[915] Data sovereignty is the extension of the sovereign authority that a state enjoys over its territory into the digital world.[916] This sovereign authority is defined by the state having autonomy and freedom to regulate data in line with its policies and laws.[917] It also extends to the power of a state to put in place laws, practices and customs on how data are to be processed.[918] This data sovereignty extends to the authority that a state has not only over the data or data infrastructure, but the people and entities who use the data and data infrastructure.[919] Simply put, data sovereignty is the effort by a state to exercise control over data and its flow and one way to achieve data sovereignty is through adoption of data localisation measures.[920]

Data localisation measures are usually a direct result of political strategies adopted by governments to gain sovereignty over data. These political strategies usually form part of state practice which reflects governments' understanding of data jurisdiction. Governments are realising that their power is diminishing in the digital age[921] due to the growth in market share by major multinational technology companies. Take Facebook (recently rebranded to Meta) for instance, it has nearly3 billion users across the world.[922] This means that a non-governmental entity is in control of data of nearly a third of the world population. Due to the amount of data under their control, major technology companies can be said to possess *quasi* sovereign power. Mark Zuckerberg, the founder of Facebook

[913] Weiwei Zheng 'Comparative study on the legal regulation of a cross border flow of personal data and its inspiration to China' (2020) 15 *Frontiers of Law in China* 280 at 286.
[914] AU Data Policy Framework 2022 at 47.
[915] Ibid
[916] Jing de Jong-Chen 'Data sovereignty, cybersecurity, and challenges for globalization' (2015) 16 *Georgetown Journal of International Affairs* 112 at 112. While discussing rights of indigenous people, Tsosie defined data sovereignty as the right of a nation to govern the collection, ownership and application of data concerning the tribe or its members and to control data that is housed within tribal territory. Rebecca Tsosie 'Tribal data governance and informational privacy: Constructing indigenous data sovereignty' (2019) 80 *Montana Law Review* 229 at 230.
[917] Zheng op cit note 924 at 286.
[918] Ibid.
[919] Jack Goldsmith 'Sovereign difference and sovereign deference on the internet' (2018-2019) 128 *Yale Law Journal Forum* 818 at 818.
[920] Razzano op cit note 396 at 5.
[921] Andrew Keanu Woods 'Litigating data sovereignty' (2018) 128 *Yale Law Journal* 328 at 358.
[922] 'Facebook statistics and trends' Data Reportal. Available at *https://datareportal.com/essential-facebook-stats* accessed on 1 May 2023.

was correct when he said, 'in a lot of ways Facebook is more like a government than a traditional company'.[923]

Major multinational technology companies benefit from market dominance by being able to provide services to businesses, individuals, and governments. Ultimately, these companies exercise monopoly over data which allows them to capture political power. While internet users reluctantly share a lot of their personal information with service providers to receive tailored digital services, they try to limit the amount of personal information they share with their governments. A service provider is likely to know more about a citizen than the government of that citizen. The amount of influence and control over people's data enjoyed by technology companies may not always be welcome by governments. Multinational technology companies also have an indirect involvement in international rulemaking than most governments. Domestic laws are usually shaped by local culture, religion, political climate, and history. However, multinational companies deal with users from different cultural, political, and religious backgrounds. Service providers play a pivotal role in shaping internet policy. With increased efforts on multi-stakeholderism, most internet service providers and technology companies are increasing their influence and control. These companies are at the forefront in developing internet policies, community guidelines and internet standards and best practices. These guidelines apply to users from different demographics and not restricted to states' geographical borders. A user who fails to comply with community guidelines may end up having their content removed, or their account suspended or deleted.[924] With every request, these private actors must determine whose rules govern data and how such rules are interpreted and applied.[925] In practice, content may be legal in a country but may be taken down for not complying with the community guidelines put in place by these companies. Data localisation measures can as well be tactical strategies by governments to establish some form of dominance in the global digital geopolitics.

Similarly, these companies also play a significant role in cybercrime investigations. Crime investigators rely on service providers to provide technical assistance when investigating crime, to preserve digital evidence or disclose digital evidence. Service providers have some form of power over who may or may not access data.[926] It is up to service providers to provide access to sought-after data

[923] Henry Farell, Margaret Levi and Tim O'Reilly 'Mark Zuckerberg runs a nation-state, and he's the king' https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king Vox accessed 12 June 2021.

[924] The former President of the United States, Mr Donald Trump's Twitter and Facebook accounts were suspended due to his constant violation of community guidelines. 'Twitter 'permanently suspends' Trump's account' BBC News 9 January 2021. Available at https://www.bbc.com/news/world-us-canada-55597840 accessed on 15 July 2021.

[925] Daskal op cit note 227 at 185.

[926] Matthew C Snipp 'What does data sovereignty imply: What does it look like?' in Tahu Kukutai and John Taylor *Indigenous data sovereignty* (2016) Chapter 3 at 40.

or resist search and seizure requests from LEA.[927] The sovereignty of a state may be threatened when companies refuse to cooperate to disclose data.[928] Since most service providers have access to data and have the technical expertise to access customer data, they are central to crime investigations.

These observations show that major multinational corporations wield a lot of influence in how laws around access to data are shaped. These companies exercise discretion over who may get access to customer data. The role of governments has both been supplemented and sometimes supplanted by these private actors. In certain situations, these companies manage data and mediate conflicting legal obligations across borders.[929] The concern is that if states are not careful on the amount of influence and authority exerted by these service providers, their powers are likely to wane off. To exert their sovereignty over data, states may resort to data localisation measures.[930] The prevailing approach to data and jurisdiction commonly accepted by states is there should be a correlation between data and sovereignty.[931] If a country can reasonably control and dominate data in its territory, then the national sovereignty and the legality of cyberspace can be proved. Several countries are motivated to adopt data localization measures as they are of the view that governments should have sovereign interests in data held in their own territory.[932] When states impose data localisation measures or requirements, it is an attempt to regain their declining power in the wake of global service providers and increased foreign influence.

a. Global trends on data sovereignty

With the 'scramble for data' or 'data imperialism', most states are rushing to establish their dominance in the data economy. Governments want to have a strategic advantage over data produced within their territories in face of competition from other governments. Incidentally, governments employ data localisation measures as protectionist measures. When states adopt these measures, they seek to protect their own sovereignty in the face of surveillance from foreign states[933] as well as to protect citizens' data from foreign government surveillance. However, data localisation requirements

[927] AWS recently updated its policy for EU customers to provide assurances that in the event of an access request under the US CLOUD Act, AWS would commit to challenge the request in court. Wu op cit note 922 at 20.
[928] Ibid.
[929] Daskal op cit note 227 at 237.
[930] Daskal op cit note 753 at 16.
[931] Zheng op cit note 924 at 285.
[932] Daskal op cit note 147 at 1047.
[933] Kesan warns that data centers located in the US are vulnerable to intelligence-gathering instruments like the USA PATRIOT Act, the Homeland Security Act and the National Security Letters. Kesan and Bashir op cit note 262 at 4.

could facilitate state surveillance as states would not need to go through foreign countries or intermediaries to access their residents' data.[934] [935]

So far, this study has shown that data plays an important role in the global economy. The country where data are hosted or where digital infrastructure is set up enjoys limitless possibilities in how the data are manipulated and exploited for its own socio-economic benefits. To reiterate, data are the new oil[936] and the country which controls this data has a significant influence in how the data are exploited. The US and China have significant numbers of technology companies infiltrating the global digital market. Meanwhile, African economies with the least market share in data centres and digital architectures have been struggling to level the playing field. Within the EU, the pursuit for digital sovereignty is mainly because the leading technology companies like Google, Apple, Facebook, Amazon, and Microsoft (GAFAM) are companies from the US. This places the United States government at a strategic advantage in that it enjoys personal jurisdiction over these US entities. These US based companies have a global presence and have heavily penetrated both African and European markets. As discussed in chapter 2, most cloud service providers operating on African soil are US companies. The Forbes 2019 list of the top one hundred digital companies showed that only one European Union company called Deutsche Telekom was in the top 20, with the US having 12 companies and China with 2 companies.[937]

The dominance of the GAFAM companies in European markets as well as the dominance in use of Chinese products[938] by Europeans has been one of the factors driving Europe towards digital sovereignty and the need to grow European capabilities in digital infrastructure. In 2020, the European Commission indicated that the European Union had to be a 'rule maker and not a rule taker' when it comes to how digitalisation affects its citizens and companies.[939] Through the 'Team Europe Initiatives'[940] such as the Global Gateway[941], the European Union is making efforts to compete in the global digital geopolitics. Hence, data or digital sovereignty is an important policy consideration for the

[934] Kugler op cit 915 at 2.
[935] Matthias Bauer, Hosuk Lee-Makiyama, Erik Van Der Marel and Bert Verschelde 'The costs of data localisation: Friendly fire on economic recovery' 2014 *European Centre for International Political Economy Occasional Paper* (No. 3) 1 at 3.
[936] Some argue that the analogy of data as the new oil are misleading and confusing as they create the impression that data is finite and confined within the borders of a country. This has also inadvertently led to the development of policy positions such as South Africa's National Data and Cloud Policy. Adeleke op cit note 397 at 3.
[937] Frances G Burwell and Kenneth Propp 'The European Union and the search for digital sovereignty: Building "Fortress Europe" or preparing for a new world' (2020) *Atlantic Council* at 3.
[938] Huawei, a Chinese company is playing a very active role on the rolling out of 5G networks to European markets.
[939] Burwell and Propp op cit note 948.
[940] Available at *https://international-partnerships.ec.europa.eu/policies/team-europe-initiatives_en*, accessed on 1 May 2023.
[941] Available at *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en*, accessed on 1 May 2023.

European Union. One of the notable European countries at the forefront in asserting sovereignty over data is Germany. In 2014, Germany cancelled a contract it had with a US company called Verizon. It raised concerns over the possibility for US intelligence agencies to demand Verizon to disclose stored data relating to Germans.[942] The Germany Minister, Peter Altmaier, raised concern that when US cloud services companies store European data abroad, the EU experiences a loss of sovereignty.[943] After conducting a research on digital sovereignty in public administration, Germany noted that government agencies were increasingly dependent on standardized software products from foreign companies.[944] Germany and France noted that data sovereignty by design is one of the guiding principles for the development of software for platforms.[945] The two countries seek to prevent non-European governments from getting access to data generated within Europe.[946]

The furthering of political priorities, interests, and perspectives are some of the notable reasons motivating countries to establish data sovereignty.[947] This is quite evident in both Africa and Europe. For Europe, the debate over digital sovereignty was rooted in a widespread perception that Europe had been disadvantaged by large US tech companies offering cloud services[948] as well as Chinese companies which infiltrated the 5G infrastructure market.[949] The US companies currently supply the overwhelming share of cloud computing services in Europe, with 92 per cent of the western world's data stored in the United States. The leading cloud service provider is AWS which has one third of the global market for hosting corporate data. Microsoft and Google control 6 per cent and 7.8. per cent of the market respectively.[950]

China's approach to data sovereignty is being led by the state, unlike the US where the private sector is at the forefront.[951] Through the Chinese Belt and Silk Road, China was able to invest in digital infrastructure in other regions especially Africa. With the internet having been originally invented by the United States, and with most root servers still located in the United States, China is concerned that

[942] https://www.bbc.com/news/business-28047877#:~:text=The%20German%20government%20has%20cancelled,giving%20data%20to%20US%20authorities.&text=The%20firm%20did%20not%20comment,bugged%20Chancellor%20Angela%20Merkel's%20phone accessed 25 April 2021.
[943] Burwell and Propp op cit note 948.
[944] Ibid at 7.
[945] Project GAIA-X https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html accessed on 25 April 2021.
[946] The European Commission's Strategy for Data is another effort to reduce technological dependencies in cloud infrastructure and services. Burwell and Propp op cit note 948 at 9.
[947] Jong-Chen op cit note 927 at 117.
[948] Burwell and Propp op cit note 948.
[949] Wu op cit note 922 at 5.
[950] Ibid.
[951] Jan Hofmeyer, Ndeapo Wolf and Deon Cloete 'SADC Futures of digital geopolitics: Towards African digital sovereignty' Occasional Paper 337 SAIIA.

it does not have control over internet technology.[952] This is what motivates China to adopt seemingly data imperialistic policies.

The EU's concerns about foreign influence in its digital infrastructure are also similar to what Africa is experiencing.[953] Most data centres and cloud services in Africa are under the control of foreign entities.[954] Chinese owned companies like Baidu, Alibaba, Tencent and Xiaomi (BATX) as well as US GAFAM companies have significant presence on the African data centre market. Either these foreign companies invest (directly or through local entities) in data centres on the African continent, or they host African data on data centres outside Africa.[955] Even routine communications between ordinary people who reside in the same African country often involve US-based platforms.[956] For example, Microsoft is a big cloud player on the African cloud data market and has launched two enterprise grade data centre regions in Cape Town and Johannesburg as well as edge nodes in Kenya, Nigeria and Egypt.[957] Data centre capacity is also not evenly distributed on the African continent and data centre infrastructure in Africa still lags leading markets. There are nearly 50 data centres in Africa, five in Kenya, eleven in Nigeria, five in Morocco and twenty-five in South Africa.[958] There are 643 technology hubs on the African continent and the growth forecast in cloud and data centre capacity is up to 80 per cent.[959][960] African governments believe that data localisation requirements will help them re-gain their data sovereignty and have autonomy to decide for themselves how to regulate their digital infrastructure and how to plan their digital futures.[961] There are arguments that data about people in Africa should

[952] Anqi Wang 'Cyber sovereignty at its boldest: A Chinese perspective' (2020) 16 *Ohio State Technology Law Journal* 395 at 404.
[953] Vincent Hofmann and Matthias Ketteman 'Towards an African narrative on digital sovereignty' (2022). Available at https://www.hiig.de/en/african-digital-sovereignty/#:~:text=Data%20about%20people%20in%20Africa,to%20plan%20their%20digital%20futures accessed 19 October 2022.
[954] Ibid.
[955] A US entity acquired a stake in Teraco which owns Africa's largest data centres. Actis launched pan-African data centres in countries like Nigeria. Africa Infrastructure Investment Managers private equity firm acquired a majority of stake in Ngoya Etix DC, a carrier-neutral data centre located in Ghana. Liquid Intelligent Technologies recorded an influx in investor interest including from the US government's International Development Finance Corporation. Digital Council Africa 'Africa Digital Infrastructure Market Analysis 2021 Report'. Available at https://www.wcoesarpsg.org/wp-content/uploads/2021/11/juanita-clark-africas-evolving-digital-landscape.pdf accessed on 18 August 2022.
[956] Halefom op cit note 22 at 13.
[957] An interactive view of cloud computing in Africa 2021 International Finance 25 January 2021 https://internationalfinance.com/an-interactive-view-of-cloud-computing-in-africa/ accessed 02 October 2022.
[958] Gugu Resha 'Addressing the potential for African digital governance to facilitate inclusive development: rights, rules & revenues' 2021 Discussion Paper.
[959] An interactive view of cloud computing in Africa 2021 International Finance 25 January 2021 https://internationalfinance.com/an-interactive-view-of-cloud-computing-in-africa/ accessed 02 October 2022
[960] The total estimate of data centres serving 1,26 billion people in Africa is about 140,000 square meters which is the same amount of data centre space serving Switzerland's 8,5 million people. Africa Digital Infrastructure Market Analysis 2021 Report op cit note 966 at 18.
[961] AU Data Policy Framework 2022.

remain in Africa and African states should have autonomy to decide for themselves how to regulate their digital infrastructure and how to plan their digital futures.[962]

The trends in data imperialism strongly indicate the views of governments on data jurisdiction. Governments understand that when states enjoy data sovereignty, they have a stronger legal basis in terms of their national laws and international law to unilaterally access the data for crime investigation purposes. When a state can demonstrate its sovereign interests over data, particularly where it has territorial jurisdiction over data, its national laws as well as international law permits it to unilaterally access any data of interest. Similarly, service providers who normally play a pivotal role in assisting LEA to access sought after data will find it difficult to resist complying with any search warrants, preservation orders or disclosure orders. Data sovereignty brings clarity particularly in instances where service providers would argue the lack of extraterritorial jurisdiction. Service providers will not be able to argue that a state does not have extraterritorial jurisdiction over the data. This would expedite cybercrime investigations and prosecution of crime.

b. South Africa's approach to data sovereignty

There are concerns that South Africa's cloud computing infrastructure (data centre) investment is mostly foreign owned.[963] The growing concern is that data generated in South Africa is mostly stored in foreign lands, and when stored locally, is owned by international technology giant companies[964] like the GAFAM and BATX. To address these concerns as well as provide clarity on its data governance issues, South Africa's Department of Communications and Digital Technologies recently published the National Data and Cloud Policy[965] for public comment. As discussed earlier in chapter 2 of this study, this is the first draft policy to clearly demonstrate South Africa's approach to data sovereignty. The policy seeks to create an enabling environment for the provision of data and cloud services to ensure socio-economic development for inclusivity. The NDCP raises key issues around the role played by South Africa in the market for cloud computing technologies. The NDCP notes that South Africa and Africa are unequal participants in the cloud market when compared to North America, Europe, and Asia.[966] It identified important policy concerns which justifies the adoption of data localisation measures. South Africa is not competitively participating in data centre infrastructure. First, the cloud market is dominated by foreign owned companies who are providing local cloud services. Secondly, a

[962] Hofmann and Ketteman op cit note 964.
[963] NDCP op cit note 390 at 20.
[964] Ibid at 29.
[965] The NDCP seeks to put in place a conducive and enabling environment for the data ecosystem to thrive. To do this, the NDCP prioritises the promotion of connectivity and access to data and cloud services, the removal of regulatory barriers and enable competition as well as ensuring the implementation of effective cybersecurity, privacy and data and cloud infrastructure protection measures. The NDCP seeks to provide for institutional mechanisms for the governance of data and cloud services as well as supporting the development of small, medium and micro enterprises and research, innovation and human capital development. Every person in South Africa, including companies, government and government departments are all subject to this policy.
[966] NDCP op cit note 390 at 29.

significant amount of data of South African businesses, citizens, residents, and government departments is being hosted on foreign based data centres. South Africa is not integrally involved at any stage in the adoption of data centres and cloud services. This would mean that South Africa will always have a weaker claim to jurisdiction over transborder cloud data. Conversely, at any given time, a foreign government may have a stronger form of jurisdictional authority over the data either because the data are being hosted on its territory or its local companies have control over the data.

The South African government is concerned that there is no policy to guide localised data acquisition, ownership, storage, use and analytics which is a threat to national security and social and economic growth.[967] South Africa recognises that data ownership, data sovereignty and data protection are critical elements for the digital economy and seeks to put in place measures to decentralise investments to ensure distribution of opportunities in the cloud computing area.[968] In essence, South Africa seeks to promote its data sovereignty and security by controlling how data produced within its borders (whether produced by government or the private sector) is exploited.[969]

To exercise its data sovereignty over cloud data, South Africa's NDCP provides that data generated in South Africa are the property of South Africa, regardless of where the technology company is domiciled. The draft policy also clarifies that data generated by foreign tech companies belongs to the South African government.[970] This means that if a US company like Microsoft produces data within South Africa, the data are the property of South Africa. With government being one of the highest producers of data, there is rationality for the government to want to exercise control over this data.

Global service providers threaten states sovereignty in various ways. Service providers have access or control over data which may be relevant for a criminal investigation. In most instances, criminal investigators need technical support from these service providers to gain access to electronic evidence. If the service providers are not convinced by the justification and the need for LEA to gain access to their customers' data, they may deny access. South Africa's NDCP identified that there is critical data held by the private sector which could enhance government's planning and service delivery capability. The sharing and flow of data within government is limited and restricted, thus depriving government of access to critical insights for crime prevention.[971]

Chapter 4 of this study discussed the *Microsoft Ireland* case, which is a typical example of the role played by service providers in crime investigations and gathering of electronic evidence. Service

[967] Ibid at 9.
[968] Ibid at 20.
[969] Razzano points out that 'localisation provisions are an attempt to assert sovereign data control (with the data infrastructure providing the means to do it), underscored by an assumption that state centrism is a mechanism both for ensuring protection and for preserving value retention'. Razzano op cit note 396 at 5.
[970] Policy intervention 10.4.4. NDCP op cit note 390.
[971] Ibid at 24.

providers usually have in-house legal counsel who independently assess requests from LEA or search warrants or other orders from court. The assessment usually involves considering the interests of the customers, applicable law, and the requests. If upon their interpretation of the law, they are of the opinion that the requested record should not be disclosed, they will refuse access to that record and contest the request. This would usually result in LEA and the service providers seeking further recourse from the courts. If LEA do not have the financial resources to litigate, such court cases may end up being dropped. The bargaining power that service providers yield places them in a very strategic and powerful position when dealing with law enforcement requests. The amount of power yielded by tech companies can be threatening to the sovereign interests of states who subsequently take measures to re-establish dominance over data.

c. Data sovereignty and balkanisation of the internet

There are arguments that the exercise of states' data sovereignty and the introduction of data localisation measures will result in the balkanisation of the internet. Internet balkanisation is described as dividing the internet into fragmented, national domains, rather than the global commons it has operated as thus far.[972] The internet architecture was designed to be borderless without any regard for national borders. A borderless internet has enabled technical innovations like cloud computing, which spreads data across various data centres to make affordable and convenient on-demand access to a shared pool of processing or storage facilities, while the actual physical locations of the data remains largely invisible to users.[973] Scholars argue that the strengthening of national borders through data localisation laws is likely to fragment the global network into various distinct idiosyncratic internets resulting in delays, inefficiencies and higher costs.[974] Apart from balkanising the internet, data localisation is also criticised for negatively impacting on international trade, increased data storage costs, and greater susceptibility to destruction of data by natural disasters.[975]

Cosmopolitans or data exceptionalists accuse sovereigntists (territorialists) of trying to break apart the internet.[976] They often frame the debate as over whether the internet should be open or balkanised.[977] Woods and Mueller disagree with the arguments that data localisation results in the balkanisation of the internet. Woods correctly points out that the internet can both be open and balkanised at the same time. This argument is relevant in discrediting the arguments against data localisation as resulting in a

[972] Reema Shah 'Law enforcement and data privacy – a forward looking approach' (2015) 125 *Yale Law Review Journal* 543 at 549.
[973] Erica Fraser 'Data localisation and the balkanisation of the internet" (2016) *SCRIPTed: A Journal of Law, Technology and Society* 359 at 362.
[974] Ibid.
[975] Jordan A Klumpp 'International impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations' (2020) 48 *Georgia Journal of International and Comparative Law* 613 at 642.
[976] Woods op cit note 932 at 368.
[977] Ibid.

balkanised internet. Woods argues and correctly so, that digital boundaries exist because of sovereign difference. Due to differences in history, culture, norms and other commitments, governments develop different laws. For example, the internet founding fathers (the United States) championed the internet's ability to spread knowledge without borders. Conversely, China never had internet founding fathers who fought for the independent internet spirit and its objectives are to use the internet as an economic developmental tool to boost its economy.[978]

The internet is already fragmented based on language, culture, legal compliance, etc. The service that a company may offer to people in America can vastly differ from those offered to customers in Saudi Arabia or China. Service providers understand the differences in religion and culture and can refine their services to meet these requirements. Woods and Mueller note that the internet can both be fragmented and uniform at the same time.[979] One does not lose openness or interoperability by embracing sovereign differences.[980] Woods further submits that the second reason this dichotomy is unhelpful is that fragmentation is already here.[981] Fragmentation is not only the product of state policy or laws but it happens because internet users and service providers want it.[982] Woods stresses the point that the question should not be whether the internet fragment but rather what kind of fragmentation we should encourage.[983] Though different services are offered to different geo-political regions, the internet is still open and interoperable. Mueller points out that there is a difference between an internet that is technically fragmented and one that is technically compatible but heavily filtered.[984].Goldsmith also argues that content filtering does not lead to the fragmentation of the internet.[985] In most instances, those who speak of the balkanisation or fragmentation of the internet will be referring to content filtering. This study argues that data localisation requirements do not lead to the balkanisation of the internet. It supports Mueller's argument that internet filtering is not the same as technical fragmentation of the internet. Content filtering at national borders is not the same as a permanent break in interoperable connectivity, split in DNS root or the challenge in the transition from IPv4 to IPv6.[986]

To argue that content filtering leads to the fragmentation of the internet is nonrational. From a technical perspective, the internet is already fragmented, and it is not fragmented by laws and measures such as data localisation measures. Mueller points out that the internet is a federation of autonomous systems with an extensive capability for selective, fine grained secession from practically any other part

[978] Wang op cit note 963 at 465.
[979] Woods op cit note 932 at 368.
[980] Ibid.
[981] Ibid.
[982] Ibid.
[983] Woods op cit note 932 at 369.
[984] Milton Mueller *Will the Internet Fragment? Sovereignty, Globalisation and Cyberspace* (2017) chapters 1 and 2.
[985] Goldsmith op cit note 930 at 819.
[986] Ibid at 820.

of the federation.[987] An unfragmented internet is terrifying and incompatible with all of the enormous pleasures and benefits fostered by the internet, and indeed incompatible with the internet as a coherent communications medium.[988] Ultimately, internet filtering is inevitable and omnipresent on endless dimensions, one of which is the geographical space controlled by national governments. Every nation filter internet content at its borders in different degrees. This study agrees with Woods' submission that the political reality is states will always insist that their rules apply.[989] Woods points out that unless a state has explicitly waived its own rules, sovereign deference is the rule rather than the exception.[990]

III. DATA LOCALISATION MEASURES

a. What is data localisation?

There is no single or official definition of data localisation.[991] Data localisation mandates come in different forms or manifestations which also determine how the term is defined. The underlying policy objectives, legal environment, targeted sectors (health, telecommunications, banking, insurance, etc) all have a bearing on the types of data localisation measures adopted.[992] The adopted measures move along a sliding scale of restrictiveness (from bad to worst).[993] Data localisation measures are aimed at controlling what goes out of national digital borders. Such measures vary from the imposition of restrictions on transfer of data to other countries to mandatory requirements to store data on local servers or keeping copies of data locally.[994] Fraser defines data localisation as the laws or measures put in place by governments which encumber the movement of data across national borders or limit where and by whom they are stored or processed.[995] Some define data localisation as an explicit requirement that data be stored and / or processed within the domestic territory.[996] Scholars like Chander define data localisation as a second-generation internet border control which seeks not to keep information out but rather to keep data in.[997] The first generation of internet border control was aimed at restricting the type of information entering a territory.[998] The AU Data Policy Framework defines data localisation as

[987] Ibid at 821.
[988] Ibid.
[989] Woods op cit note 932 at 369.
[990] Ibid at 370.
[991] Gonzalez, Casalini and Porras op cit note 916 at 4.
[992] Ibid at 6.
[993] Cory and Dascoli identifies different types of data localisation rules ranging from local data mirroring, explicit local data storage, de facto local storage and processing, explicit local data storage and processing and explicit local and discriminatory, data processing, routing and storage. Nigel Cory and Luke Dascoli 'How barriers to cross-border data flows are spreading globally, what they cost, and how to address them' 2021 *Information Technology and Innovation Foundation* 1 at 4.
[994] Dorothee Flaig, Javier Lopez-Gonzalez, James Messent and Marie-Agnez Jouanjean 'Modelling data localisation measures' 2016 *19th Annual Conference on Global Economic Analysis* 1 at 1.
[995] Fraser op cit note 984 at 360.
[996] Gonzalez, Casalini and Porras op cit note 916 at 4.
[997] Anupam Chander and Uyen P Le 'Data Nationalism' (2015) 64 *Emory Law Journal* 677 at 679.
[998] Ibid.

involving the artificial erection of legislative barriers to data flows, such as through data residency requirements and compulsory local data storage.[999]

Policy conversations regarding data residency on the African continent have frequently centred on localisation as a governance mechanism.[1000] A lot of African governments, as reflected by the language of the AU Policy Framework seek to gain control over the processing and utilisation of data generated on their territories. Due to the divergent views on data localisation, there is tension between its proponents and opponents. Data localisation proponents view sending data abroad as increasing citizens' vulnerability to serious security and threats from foreign actors. To resolve these threats, data localisation measures can be implemented to safeguard privacy of citizens, promote local economies and protect national security interests.[1001] Globally, about 62 countries had adopted data localisation requirements and 144 countries had adopted data localisation restrictions by 2021.[1002] States consider data localisation measures as justifiable.[1003] One should note that though data localisation is taking centre stage in recent debates, these measures are not new. They have existed in varying degrees[1004] dating back to the origins of telegraghy[1005] and have recently increased due to governments' unease after the Snowden revelations.[1006] The long arm of the United States government has caused governments to work towards maintaining their national sovereignty over data and data infrastructures within their borders.

Data localisation is emerging because governments are motivated to adopt such measures by different factors. They justify data localisation as a protectionist measure to protect their citizens and local business.[1007] There is a general trend to adopt data localisation measures as a means of ensuring that domestic privacy and data protection principles and rights of citizens are respected.[1008] Growing concerns about cybersecurity have sparked an intense international debate about data sovereignty and the degree to which governments should control the flow of data both within and across their borders.[1009]

---

[999] AU Data Policy Framework at 47.
[1000] Razzano op cit note 396 at 5.
[1001] Mapping and analysis of privacy laws in Africa 2021 CIPESA 1 at 28. Available at https://cipesa.org/resources/ accessed on 4 June 2022.
[1002] Kugler op cit note 915 at 1.
[1003] Zheng op cit note 924 at 285.
[1004] Kuner notes that data nationalism dates back to the 1970s with countries such as Brazil imposing requirements for requesting permission from a government board for the use of international computer networks that transferred or accessed data outside the country. Christopher Kuner 'Data nationalism and its discontents' (2014-2015) 64 *Emory Law Journal Online* 2089 at 2091.
[1005] Drake notes that the jealous protection of national sovereignty has been foundational to international communications and information policy since the dawn of the international telegraphy. For example, when concluding the 1850 Treaty of Dresden and the 1865 Treaty of Paris, governments were careful to codify mutually exclusive control of their respective national networks. William J Drake 'Background paper for the workshop on Data localisation and barriers to transborder data flows' 16 *World Economic Forum* 1 at 5.
[1006] Van der Berg op cit note 394 at 5.
[1007] For example, one of the drivers of data localisation in Kenya was national security.
[1008] Gonzalez, Casalini and Porras op cit note 916 at 6.
[1009] Jong-Chen op cit note 927.

Some governments resort to data localisation measures to protect information that is deemed to be sensitive from a national security perspective.[1010]

As already discussed in this study, territoriality remains a primary basis for exercising enforcement jurisdiction in the cloud. States understand that foreign governments cannot unilaterally access data if it is hosted on foreign-based data centers. The aim is to protect citizens from foreign surveillance or potential privacy violations.[1011] Governments believe that such measures can help develop domestic capacity[1012] and provide a competitive advantage to local companies amid the globalisation of the digital economy.[1013] Data localisation opponents contend, and correctly so, that strengthening state control over users' data does little to address genuine grievances surrounding cybersecurity, disinformation, or the online targeting of marginalised communities by the state and non-state actors.[1014] This section of the chapter discusses the different data localisation measures adopted by countries and the link to the interests of law enforcement and crime investigations.

b. Strict data localisation

Ferracane identifies two types of restrictions to cross border data flows. The first one is strict restrictions where there is a blanket ban on transferring of data abroad or a requirement for local storage or processing of data.[1015] These restrictions can manifest in the form of policy, standards, laws, and regulations. In other instances, the restrictions come in the form of technical efforts aimed at the technical and physical architecture of the internet. For instance, Germany had planned to have its own data centres and re-route email traffic to avoid surveillance from the US.[1016] Whilst Germany's plans did not come to fruition, countries like China have been successful in controlling the physical infrastructure through which internet traffic is exchanged.[1017]

Localisation measures aimed at local storage requirements can either be generally broad or industry specific. Some measures can make it mandatory for any form of data to be locally stored or processed, while others may focus on specific industry sectors such as finance, telecommunications, health, or the public sector.[1018] For example, Nigeria's Guidelines for Content Development in ICTs strictly prohibits all government data and all subscriber and consumer data held by telecommunications

[1010] Gonzalez, Casalini and Porras op cit note 916 at 6.
[1011] Lachmayer and Witzleb op cit note 346.
[1012] Gonzalez, Casalini and Porras op cit note 916 at 6.
[1013] Fraser op cit note 984 at 361.
[1014] CIPESA op cit note 1012 at 28
[1015] Rishab Bailey and Smriti Parsheera 'Data localisation in India: Questioning the means and ends' (2018) 242 *National Institute of Public Finance and Policy.*
[1016] W Kuan Hon, Christopher Millard, Jatinder Singh and Ian Walden 'Policy, legal and regulatory implications of a Europe-Only cloud' (2016) 24 *International Journal of Law and Information Technology* 251 at 253.
[1017] Neha Mishra 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows' (2019) 52 *Vanderbilt Journal of Transnational Law* 463 at 474.
[1018] Flaig, Lopez-Gonzalez, Messent and Jouanjean op cit note 1005 at 7.

companies from being transferred outside the country.[1019] The measures were adopted to promote local content and increase domestic value in ICT products and services. Nigeria also has specific data localisation regulations in the financial sector. In 2011, the Guidelines on Point-of-Sale-Card Acceptance Services were issued by the Central Bank of Nigeria. In terms of these guidelines, all domestic transactions had to use local switch services and switching between Nigerian issuers and acquirers cannot be done outside Nigeria.[1020] Ethiopia also imposes strict data localisation requirements in respect of domestic payment information, payment switch and ATM transaction data.[1021] Rwanda also has similar restrictions.[1022] As mentioned in chapter 2 of this study, South Africa's Reserve Bank also passed a directive on use of cloud services by financial institutions and circumstances where financial data may be migrated to foreign cloud servers. The motivation for localising financial records is that it can be available for urgent review in the event of a bank failure.[1023]

Russia is one of the world leaders insisting on forced localisation or hard localisation.[1024] Russia's Federal Law No. 242-FZ is a good example of a requirement for local storage and processing of data. Russian law requires that all operators must ensure that recording, systematisation, accumulation, storage, adjustment (update, modification), extraction of personal data of citizens of the Russian Federation must be done by means of databases, situated on the territory of the Russian Federation.[1025] The government justifies this adoption by relying on national security and the protection of Russian citizens privacy.[1026] All operators and service providers in Russia are expected to comply with the localisation requirements. This compliance extends to companies (such as foreign social networking, online shopping and other websites that receive information about Russian citizens) carrying out business activities in Russia that involve processing of personal data of Russian citizens, regardless of

[1019] Guideline 12.1.(4) of the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2013. The guidelines were established by Nigeria's National Information Technology Development Agency (NITDA)
[1020] Guideline 4.4.8. Guidelines on Point of Sale Card Acceptance Services 2011.
[1021] The Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020 provides that the transfer of domestic payment information outside of Ethiopia for the purposes of authorisation, clearing and settlement by Point of Sale (POS) machine operators is outlawed. Consequently, only payment data made through the international card scheme to the financial institution or national switch can be sent. Similarly, ATM operators are prohibited from sending any transaction data outside Ethiopia for processing, authorisation and switching.
[1022] Article 3 of the Regulation No. 02/2018 on Cybersecurity provides that any bank licensed by the Central Bank of Rwanda must maintain its primary data within the territory of Rwanda. Further, article 27 of the 2010 Law Governing the Credit Information System in Rwanda provides that the Central Bank shall have the authority to approve the sharing of customer information beyond the borders of Rwanda. Similarly, the Regulation No. 03/2018 on Outsourcing provides that banks shall not outsource their primary data outside Rwanda as provided in the regulation on cyber security.
[1023] Burwell and Propp op cit note 948 at 10.
[1024] The other notable countries are China, India and Turkey. Cory and Dascoli op cit note 1004 at 4.
[1025] Article 2 of the Federal Law 242-FZ amends Federal Law No 152-FZ by inserting Article 18 (5) which reads as follows –During personal data collection, inter alia, through the internet, the operator shall ensure that databases within the Russian Federation are used to records, systematize, accumulate, store, clarify (update or modify) and retrieve personal data of citizens of the Russian Federation, except for cases specified in clauses 2, 3, 4, 8 of part 1 of Article 6 of this Federal Law.
[1026] Fraser op cit note 984 at 369.

whether they have a physical presence in Russia.[1027] Zambia's Data Protection Act also adopts a strict data localisation requirement. Section 70 of the Act provides that 'a data controller shall process and store personal data on a server or data centre located in the Republic. Despite subsection (1), the Minister may prescribe categories of personal data that may be stored outside the Republic. Despite subsection (2), sensitive personal data shall be processed and stored in a server or data centre located in the Republic.'[1028] Due to these restrictions, any transfer of personal data outside Zambia will only be possible if relevant approvals have been obtained. Similar provisions are also found in Brazil's General Personal Data Protection Law.[1029]

South Africa's NDCP also proposes that copies of personal data should be kept locally for purposes of law enforcement.[1030] This is similar to Russia's approach to data localisation.[1031] While promoting the requirements for cross border flow of personal data in line with the requirements set out under POPIA, the NDCP also imposes *quasi* strict localisation measures. As for data residency, the NDCP is very clear on South Africa's position. There are strict data localisation requirements in respect of all data that are critical infrastructure data.[1032] The NDCP proposes that critical infrastructure data should be processed and stored within the borders of South Africa. This means that no international transfers are permitted in respect of critical information infrastructure data.[1033] The NDCP reflects that South Africa is no longer passive about the global issue of data sovereignty. The policy is a good indicator that the South African government seeks to take an active role in data nationalism and promote its own data sovereignty and digital sovereignty agenda. Considering the critical role played by data in the digital ecosystem, it is commendable when governments, as primary consumers, and producers of

[1027] 'Russia enacts data localisation requirement' Deloitte https://www2.deloitte.com/be/en/pages/risk/articles/data-localisation-requirement-russia.html accessed on 18 April 2021. A failure to comply with these requirements may lead to fines being imposed on the operator or the relevant IP address included on Russia's blacklist registry of offenders. The Roskomnadzor, Russia's Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications is responsible for enforcing this legislation. In 2016, Linkedln was blocked in Russia after it refused to repatriate data related to Russian citizens. Alexandra V Orlova 'Digital sovereignty, anonymity and freedom of expression: Russia's fight to reshape internet governance' (2020) *UC Davis Journal of International Law & Policy* 225 at 237.

[1028] Zambia Data Protection Act 3 of 2021.

[1029] Article 1 Law No. 13.709 of 14 August 2018 as amended by Law No. 13.853 of 8 July 2019. Brazil's General Personal Data Protection law (LGPD) provides for the processing of personal data by natural persons or legal entities either of public or private law with the purpose of protecting the fundamental rights of freedom and privacy and the free development of personality of the natural persons. Article 3 of Brazil's General Personal Data Protection law (LGPD) applies to the processing of personal information including personal data in remote cloud data centers.

[1030] Policy intervention 10.4.3. NDCP op cit note 388.

[1031] Van Der Berg op cit note 394 at 5.

[1032] Kugler classifies restrictions on sensitive data or data relating to national security as a type of data localisation requirement different from strict data localisation and conditional flow regime. Kugler op cit note 915 at 1.

[1033] Policy intervention 10.4.1. NCDP op cit note 388.

data, are actively involved in shaping data policy. The NDCP highlights a transition from a conditional approach to data localisation as advocated under POPIA to a strict data localisation approach.[1034]

c. Conditional data localisation requirements

The second type of data localisation requirements or measures allow transfer or processing of data outside a country under clearly defined conditions.[1035] When governments with no express data localisation requirements enact laws or mandates that impose conditions for cross border data transfers, there is *de facto* data localisation.[1036] Conditional data localisation measures are prevalent in data protection laws.[1037] It is argued that data protection laws create barriers to cross border data transfers to such an extent that they are effectively data localisation requirements.[1038] Cory and Dascoli argue that the complicated data transfer requirements under the GDPR has the potential to make the GDPR the world's largest de facto localisation framework.[1039] Most data protection laws have conditional data localisation provisions[1040] and cross border transfer of personal data is only permissible subject to complying with those conditions.[1041] One of the reasons why data protection laws amount to *de facto* data localisation is that compliance with conditional flow regimes can be very costly to the extent that some entities are forced to store data locally by default.[1042] Conditional data localisation requirements offers more balance between data protection and the need for openness of data transfer for value creation. They provide clear guidelines and mandatory regulatory safeguards that once met allow for the free flow of cross-border data.[1043]

POPIA does not specifically mandate the local processing of personal data. Instead, it provides a list of conditions which must be met prior to transferring any personal data outside the Republic. If any of the provisions set out in section 72 of POPIA are met, personal data may be transferred outside of South Africa. The conditional flow of data transfer under POPIA have been considered a balanced and moderate approach which align with the ACHPR Declaration of Principles on Freedom of Expression and Access to Information and the UN High Commissioner for Human Rights necessity criteria.[1044] At

[1034] The NDCP provides a sense of the direction the South African government potentially intends to follow in the future. Alexander Beyleveld 'Data localisation in Kenya, Nigeria and South Africa: Regulatory frameworks, economic implications and foreign direct investment' 2021 *Mandela Institute Policy Brief 01 University of Witwatersrand* 1 at 3.
[1035] Gonzalez, Casalini and Porras op cit note 916 at 6.
[1036] Lindsey R Sheppard, Erol Yayboke and Carolina G Ramos 'The real national security concerns over data localization' (2021) Center for Strategic & International Studies. Available at https://www.csis.org/analysis/real-national-security-concerns-over-data-localization accessed on 2 July 2022.
[1037] Wu op cit note 922 at 13.
[1038] Bauer, Lee-Makiyama, Van Der Marel and Verschelde op cit note 946 at 3.
[1039] Cory and Dascoli op cit note 1004.
[1040] Kugler op cit note 915 at 1. Van der Berg op cit note 394 at 4.
[1041] Bailey and Parsheera op cit note 1026.
[1042] Kugler op cit note 915 at 1.
[1043] AU Data Policy Framework 1 at 41.
[1044] Adeleke op cit note 397 at 4.

a regional level, the Malabo Convention also contains conditional data localisation requirements.[1045] Article 14 of the Malabo Convention permits transborder data flows to non-member states if such a state ensures an adequate level of protection of privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed.[1046] The ACHPR Declaration of Principles of Freedom of Expression and Access to Information generally discourages data localisation measures. Principle 40 permits data localisation measures if they are justifiable and compatible with international human rights law and standards.[1047]

Within the SADC region, the SADC Model Law on Data Protection also contains conditions for transborder flow of data. The conditions depend on whether the recipient is in a SADC member state that has transposed the model, a member state that has not transposed the model law or any other non-member states.[1048] Another example from the African continent is Kenya's Data Protection Act (KDPA). The KDPA contains specific conditions on data localisation requirements.[1049] Beyleveld argues that the provisions of the KDPA gives 'the Data Commissioner the power to impose *de facto* data localisation requirements as well as giving the Cabinet Secretary the power to impose storage and processing localisation requirements.[1050] Data protection laws in Chad, Senegal, Tunisia, Uganda, and Zimbabwe also contain conditions for data transfers.[1051] Nigeria's draft Data Protection Bill also contain provisions which, if implemented could amount to *de facto* localisation requirements of personal data.[1052]

Similarly, chapter V of the GDPR contains a list of similar conditions. If a data controller or data processor is unable to meet any of the listed conditions, they cannot transfer data outside the European Union. The GDPR permits international data transfers based on an adequacy decision.[1053] For the EU Commission to pass an adequacy decision, it considers a variety of factors which includes whether a foreign state respects human rights and fundamental freedoms. Importantly, the EU Commission assesses the foreign states' legislation such as that relating to criminal law, the ability of public

[1045] Van der Berg op cit note 394 at 5.
[1046] Article 14 (6) (a) of the Malabo Convention.
[1047] Principle 40 provides that states shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localisation requirements, unless such measures are justifiable and compatible with international human rights law and standards'.
[1048] Articles 43 – 45 of the SADC Model Law on Data Protection.
[1049] Section 48 and 49 of the Kenya Data Protection Act.
[1050] Beyleveld op cit note 1045 at 1.
[1051] Kugler op cit note 915 at 2.
[1052] The Nigerian Data Protection Regulation (NDPR) 2019 and the Nigerian Data Protection Bill (2021). Beyleveld op cit note 1045 at 3. It should be noted that Nigeria has another draft Data Protection Bill 2022 which is due to be tabled in parliament. Ayang Macdonald 'Nigerian parliament set to scrutinize new draft data protection law'. Available at https://www.biometricupdate.com/202210/nigerian-parliament-set-to-scrutinize-new-draft-data-protection-law#:~:text=The%20new%20draft%20bill%2C%20dated,according%20to%20the%20bill's%20memorandum accessed 17 October 2022.
[1053] GDPR, Article 45.

authorities to access personal information, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.[1054] Daskal correctly points out that in restricting the transfers of data outside the EU absent a finding of adequate data protection safeguards, the EU, presumes that location of data (whether in or out of the EU) dictates control.[1055]

In addition, cross border transfers of personal data under the GDPR are also permitted if there are appropriate safeguards.[1056] The GDPR provides that appropriate safeguards may be provided for by a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority and approved by the Commission, approved codes of conduct or approved certification mechanism.[1057] Apart from relying on the adequacy decisions and appropriate safeguards, the GDPR also permits transborder flow of personal data under specific situations.[1058]

Whilst most data protection laws like the GDPR do not apply to criminal investigations and prosecutions,[1059] they provide some guidance on sharing of personal information between countries. This section provides an analysis of the relationship between data protection laws and the sharing of personal data in the context of criminal investigations. Cross border transfers of personal data for criminal investigations are permitted under certain conditions. As mentioned above, adequacy decisions include the assessment of the third country's rule of law and legislation concerning public security, defence, and national security as well as public order and criminal law.[1060] For instance, an adequacy decision was made by the European Union Commission over Japan's data protection laws. What is important to note is that though Japan's privacy laws were not or are not as comprehensive as the GDPR, the EU Commission found Japan to provide adequate safeguards by considering three points. First, Japan was bound by the Supplementary Rules set out by the Commission to reconcile the differences in Japanese law and GDPR.[1061] Secondly and most importantly, Japan assured the European Union Commission that its law enforcement agents will only access data in a necessary and proportionate

[1054] GDPR, Article 45 (2) (a).
[1055] Daskal op cit note 157 at 682.
[1056] GDPR, Article 46.
[1057] GDPR, Article 46 (2).
[1058] Article 49 of the GDPR provides that in the absence of an adequacy decision pursuant to Article 45 (3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place under certain conditions.
[1059] Recital 19 of the GDPR specifies that the GDPR should not apply to the processing of personal information by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Competent authorities are expected to put in place relevant criminal laws to address criminal investigations.
[1060] GDPR, Recital 104.
[1061] Jonathan McGruer 'Emerging privacy legislation in the international landscape: Strategy and analysis for compliance' (2020) 15 *Washington Journal of Law, Technology & Arts* 120 at 151.

manner subject to an independent oversight. Thirdly, the Japanese government implemented a compliance handling mechanism to address complaints from consumers.[1062]

To transfer personal data for criminal proceedings, the GDPR requires the investigating state to have in place adequate safeguards to protect the personal information once it has been handed over. In cases where there is international judicial cooperation regarding drug trafficking, human trafficking and terrorism, countries can share intelligence and evidence during a criminal investigation.[1063] Article 48 of the GDPR provides that -

> 'Any judgement of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.'

Law enforcement agents can only receive evidence containing personal data if there is an MLAT in place. In the absence of such an agreement, cross border transfer of personal data for criminal purposes is not permitted under the GDPR. The decisions of the European Court of Justice[1064] as well as the provisions under the GDPR have shaped how personal data of European citizens may be shared outside of the European Union. An important consideration that the EU considers is the ability of the foreign entity to access data once it has been shared with an entity outside the EU. If a foreign state does not have laws with essential equivalence to EU standards with respect to how government might access data, cross border data transfers are not permitted. At the same time, if a foreign state does not meet any of the requirements in terms of the GDPR, there cannot be a cross border transfer of data.

To sum up, data protection laws set conditions which must be met before data can be transferred to another territory. If such conditions cannot be met, data will not be permitted to leave the territory, and this results in *de facto* localisation. The GDPR, unlike other data protection frameworks goes the extent

[1062] Ibid.
[1063] Flaig, Lopez-Gonzalez, Messent and Jouanjean op cit note 1005 at 6.
[1064] Prior to the GDPR, the European Union and the United States of America had concluded an agreement called the Safe Harbour Agreement. The Safe Harbour Agreement had put in place certain standards to be met before personal information of EU citizens could be shared with US based companies. When Mr Schrems sued Facebook, the validity of the Safe Harbour Agreement was under scrutiny. Upon analysis of the agreement, the European Court of Justice (ECJ) found the Safe Harbour Agreement not to align with data protection law within the EU. The ECJ found that data transfers from the EU to the US were unlawful. *Maximillian Schrems v Data Protection Commissioner* Case Number C-362/14 Court of Justice of the European Union (Schrems I). Following the Schrems I case, the two economic regions negotiated another agreement called the Privacy Shield. The decision in *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties*, Case C-311/18 (Schrems II) was that EU companies must conduct due diligence exercises before cross border transfers of data. Due diligence exercises include a consideration of the recipient party's data processing and data governance. If the recipient party does not have adequate data privacy framework in place, then personal data cannot be shared with the party. The EU company must also consider the recipient party's state's data protection laws. If there are no adequate data protection laws in the receiving state, then transfer of data is not permitted.

of providing additional guidance before personal data is transferred in the context of crime investigations. Where LEA are seeking access to foreign based data and the foreign entity cannot meet any of the conditions set out under the GDPR, data must be processed within the EEA. If a foreign state's laws permit government to access any data without adequate safeguards to protect the data or any justifiable and legal basis to access the data, transfers of personal data to such a state may not be permitted. The condition also extends to whether a foreign state provides effective judicial review available to any surveilled persons to exercise their rights of redress. In the absence of such reviews, they will not be sharing of personal information. If a foreign state can easily access the data or does not have strong data protection measures, the transfer may not be permitted, and such data should remain localised. The following section discusses in detail how the data localisation measures apply in the context of cybercrime investigations.

d. Open transfers regime

The opposite of strict data localisation measures is an open transfer regime. In terms of this framework, there are minimum regulatory burdens to movement of data. Under this regime, processing of data can take place abroad, but there could be requirements for mandatory local storage of data.[1065] Gonzalez *et al* points out that there is a new category of data localisation emerging. In terms of this approach, states do not require local storage of data. However, service providers are required to guarantee access to data when required by regulators. This new form of localisation is prevalent in Mexico and New Zealand.[1066] The risk with this approach is that companies can adopt vastly different standards for different jurisdictions and do not guarantee any minimum standard for personal data protection.[1067]

IV. THE ROLE OF DATA LOCALISATION IN CYBERCRIME JURISDICTION

As briefly mentioned above, states impose data localisation measures to address various concerns. The measures range from protecting domestic markets, promoting local business to exercising sovereignty over data. The measures could also be to ensure data privacy, protection, and cybersecurity, to support local LEA by ensuring that local authorities have access to the data needed to investigate crimes, for government censorship and surveillance, to mitigate geopolitical risk and financial sanctions and for economic development purposes.[10681069] As mentioned earlier, ease of access to data during a criminal

[1065] Gonzalez, Casalini and Porras op cit note 916.
[1066] Mexico's Federal Telecommunications Law requires data to be made available for 12 months, without stipulating that it must be stored in Mexico. New Zealand's data retention regulation for business records allows for data to be stored outside New Zealand provided it meets certain data integrity and access criteria. Gonzalez, Casalini and Porras op cit note 916 at 8.
[1067] AU Policy Framework 1 at 41.
[1068] Kugler op cit note 915 at 1.
[1069] Adeleke 'op cit note 397 at 2.

investigation is one of the justifiable reasons for states to adopt data localisation measures. Incidentally, states consider data localisation measures as effective tools to protect the privacy rights of citizens. For instance, the AU Data Policy Framework recommends data sharing and enhanced interoperability among AU member states and other AU mechanisms, including mechanisms for police cooperation such as AFRIPOL.

a. Data localisation supports local law enforcement interests

The overall theme of this study is to demonstrate the challenges that LEA face when attempting to access remote cross border cloud data. Principles of international law consider cross border cloud data as extraterritorial and subject to the laws of the foreign state where data centres are located. To comply with international law, foreign LEA seeking cloud evidence on foreign servers need to follow the available channels for assistance instead of acting unilaterally. If foreign governments are not forthcoming in cooperating with the investigating state, this can delay the investigation process. Apart from the administrative challenges of MLATs, states also find the resistance from service providers to disclose data as justification for mandatory data storage. Investigating states therefore find locally accessible cloud data evidence convenient thus justifying the mandatory storage of data on local servers.[10701071]

As discussed in previous chapters, a state should not unilaterally access remote cloud data. To access the data, the state will have to get permission through the mutual legal assistance channels. As discussed in chapter 4, processes for MLAT channels are very slow. The danger with snail-paced processes is they are likely to result in miscarriage of justice as criminals may get rid of evidence while an investigating state is still waiting for approval from the foreign state. In instances where data are in transit, the service provider may not have knowledge of the location of data. This will make it difficult for the investigating state to identify the foreign state with jurisdiction at that given moment. This could potentially delay the process of gathering evidence. Mores, remote cloud data may be subject to conflicting laws from different states. Compelling service providers to disclose data may be unreliable in instances were laws of the state where the data are hosted do not permit disclosure. This will likely make crime investigation for a state a cumbersome process. A state can exercise territorial jurisdiction over data hosted on local data infrastructure. Upon the authority of a warrant or disclosure order or preservation order, LEA can request access to cloud evidence from service providers. Data localisation therefore makes the processes of gathering electronic evidence for criminal investigations fast and efficient.

[1070] Brehmer op cit note 917 at 930.
[1071] Adeleke op cit note 397 at 4.

South Africa's NDCP should be commended on its requirement for storage of copies of data on local servers. The challenges to cloud evidence as discussed in chapters 2, 3 and 4 of this study can be resolved by mandating service providers to keep local copies of data. First, local copies of data means that local law enforcement authorities will have territorial jurisdiction over the cloud data. Secondly, LEA save time and resources by not having to go through the MLAT processes. Thirdly, territorial jurisdiction reduces the friction between law enforcement and service providers as they cannot dispute the jurisdictional authority of the LEA. Fourthly, service providers will not be able to rely on excuses such as data being in transit and thus not certain whether the state has jurisdiction, as copies of the same data will be required to be stored locally.[1072]

It has been identified that some states threaten companies to access data they could not get through MLA channels.[1073] For example, South Korean officials raided Google's offices in Seoul and seized digital evidence after it was alleged that Google had inappropriately collected users' data.[1074] Woods notes that such tactics are often hard to document because LEA can subtly intimidate companies into cooperating with their requests.[1075] It can be argued that by adopting data localisation measures, states avoid unilaterally accessing cross border data or forcing service providers to disclose data.

Another tactic deployed by states when they cannot get data with the company's assistance is covert surveillance.[1076] Woods points out that it is preferable for the law to permit a government to access relevant data for law enforcement than for the government to access the same data through covert surveillance.[1077] The inability to access data that are needed for law enforcement operations is a problem for an investigating state.[1078] From the perspective of internet companies, being caught in the middle of two countries' dispute over jurisdiction may make it hard to establish clear and consistent policies.[1079] The current regime is also problematic for users as it encourages states to take extraordinary measures to obtain data necessary for law enforcement.[1080] Woods argues that it is not a threat to privacy when LEA can access data when they have a legitimate interest instead of resorting to other tactics to access data.[1081] This is an underappreciated point: regardless of whether one's normative goals are to maximise user privacy, to maximise law enforcement capabilities, or to maximise the efficiency of the internet,

[1072] Woods op cit note 932 at 355. Companies like Google and Yahoo! move data around the world and company servers located on different continents. When requested for data by governments, they usually argue that the data has been moved to another jurisdiction where it is inaccessible to law enforcement.
[1073] Woods op cit note 212 at 753.
[1074] Ibid.
[1075] Ibid.
[1076] Ibid.
[1077] Woods op cit note 212 at 754.
[1078] Ibid.
[1079] Ibid.
[1080] Ibid.
[1081] Ibid.

the equilibrium point is likely the same.[1082] More privacy can be achieved by giving governments greater lawful access to data in the cloud when that access is justified.[1083]

b. Protection of the right to privacy and security of citizens data

States justify the adoption of data localisation measures to protect their citizens' fundamental human rights. This justification is eminent in data protection laws. The Institute of International Finance noted that the objectives of data localisation measures, such as security, privacy and inclusive sustainable economic growth are worthy of pursuit.[1084] Kuner argues that data nationalism measures particularly on data protection are meant to protect the rights to privacy and not as a protectionist measure[1085] such as to protect domestic business interests from international competition. When data are stored abroad, there are legitimate concerns relating to the privacy interests of the owners of the data. There are concerns that many organisations which collect, process and store massive amounts of data lack security and privacy protections.[1086] This argument emanates from the lack of robust data protection laws in other jurisdictions. Absence of effective data protection laws means that foreign based data can easily be accessed by foreign governments. As mentioned earlier, some countries view localisation as critical to protecting their respective citizens from foreign surveillance[1087] mainly from the US government.[1088] What the revelations made by Edward Snowden highlight is that the US carries out mass surveillance on foreign governments and foreign citizens.

The US is certainly not the only government which employs covert surveillance on foreign nationals and entities. Some governments are of the view that placing data abroad jeopardises the privacy of their citizens and residents.[1089] This reason was also identified during negotiations for a Europe-only cloud by the EC's European Cloud Partnership.[1090] When foreign states access data, the data subjects often do not enjoy the protection of constitutional or other human rights legislation in the surveilling country.[1091] Generally, most states are able to protect fundamental human rights if they have an element of control over the data and the persons accessing the data. When foreign states access data, the data subjects often do not enjoy the protection of constitutional or other human rights legislation in the surveilling country.[1092] If a third country accesses the data and any privacy infringement over the

[1082] Ibid.
[1083] Ibid.
[1084] Institute of International Finance (IIF).
[1085] Kuner op cit note 1015.
[1086] Jong-Chen op cit note 927 at 114.
[1087] Flaig, Lopez-Gonzalez, Messent and Jouanjean op cit note 1005 at 5.
[1088] Brehmer op cit note 917 at 930.
[1089] Fraser op cit note 984 at 364.
[1090] Hon, Millard, Singh and Walden op cit note 1027 at 255.
[1091] Fraser op cit note 984 at 364.
[1092] Ibid.

data occurs outside the state, the state is incapacitated to exert its authority over the data. This leaves citizens data vulnerable.

The other notable justification for data localisation is that foreign governments may not have adequate data protection or privacy laws in place. Since the principle of territoriality is still grounded in most jurisdictions, location of data centers matters. If there are no adequate data protection laws in countries where data centers are located, there is a threat to privacy rights. The same concerns apply in instances where data are intended to be shared with a foreign government which does not have adequate privacy laws. One of the reasons why the ECJ ruled against Facebook and in favor of Mr Schrems was because the US did not have adequate safeguards in place to prevent the US government from accessing any amount of data.

Remote cloud data also limits the exercise of other ancillary rights to the right to privacy. Most data protection laws like the GDPR and POPIA recognise the rights for data subjects to be informed of any breaches, the right to have certain records of their information deleted and the right to move data from one service provider to the other. If remote data are in a country with no similar data protection laws, then data subjects are not able to fully exercise their rights.[1093] At the same time, data subjects may not have access to the relevant foreign data protection authorities. There are no guarantees that a foreign data protection authority will fairly represent the interests of a foreign data subject. Such challenges are less likely to rise in cases where the data are hosted on domestic data centers. Data subjects enjoy the full protection and benefit of the law.

Another advantage of adopting data localisation measures is that it disincentivises foreign government entities. When data are stored within the servers of a country, the surveilling foreign state may expend a lot of resources and time to gain access to this data.[1094] This would be different in instances where one of the surveilling state's service providers has control over the data or the data are hosted within its territory.

Some view data localisation as a means for states to exercise domestic surveillance over their citizens.[1095] In instances where a state conducts domestic surveillance over its citizens, the privacy rights of citizens are infringed. Data localisation can negatively impact user privacy and enterprise security by creating greater government access to user data.[1096] The ease of access to data by LEA may result in

[1093] GDPR supra note 340 Recital 116.
[1094] John Selby 'Data localisation laws: Trade barriers or legitimate responses to cybersecurity risks, or both' (2017) *International Journal of Law and Information Technology* 213 at 228.
[1095] Surveillance and related phenomena such as data localisation requirements have a bearing on citizens' right to privacy and other digital rights. CIPESA op cit note 1012.
[1096] Brehmer op cit note 917 at 931.

domestic surveillance of citizens.[1097] Cachalia and Klaaren made important remarks while discussing South Africa's constitutional right to privacy in the digital age. They emphasised on the need to focus on the systemic harms to privacy by governments and private actors who design technologies for their own interests.[1098] When governments implement data localisation strategies for their own political agendas, there is need to assess if such self-serving interests protect the rights to privacy of citizens. Strict data localisation laws have also been considered to promote political repression in some governments. If information is under governmental control, the government can easily suppress dissenting political opinions and threaten individual rights such as the rights to privacy, data protection, anti-discrimination and freedom of expression and democratic values.[1099] An open internet enhances liberty as political dissidents often rely on foreign speech platforms to disseminate information. Data localisation can erode this benefit by preventing dissidents from using foreign based services or shrinking the services available to citizens as businesses will be reticent to operate data centres in authoritarian countries with strong state censorship and surveillance laws.[1100]

While the prevention of foreign surveillance has been found as a justifiable reason to localise data, there are still concerns that this reason is not justifiable. It has been argued that forcing data localisation of personal information to prevent foreign surveillance is flawed as many of the recent legislative proposals pre-date the surveillance revelations.[1101] Mishra argues that data localisation does not prevent foreign surveillance. When data are hosted on local servers, it does not mean they are under an impenetrable shield. Foreign governments can still deploy covert surveillance tools to access the data if necessary.[1102] Foreign surveillance is an issue that existed before the use of cloud technologies. Due to the internet infrastructure, data localisation does not stop foreign surveillance. Furthermore, information security is not a function of where data are physically stored or processed and threats to data are oftentimes domestic.[1103] Fraser also argues that in practice, governments denounce foreign surveillance on behalf of their citizens while secretly sharing information with others.[1104] Fraser submits that considering this, localisation is not an effective means of keeping data from foreign intelligence agencies.[1105] McKenna also argues that data localisation will not protect data stored in another state if

[1097] Study has shown that some states use access to data under their jurisdiction for local surveillance on citizens, which also violates the rights to privacy and threaten the rule of law. Adeleke op cite note 397 at 4.
[1098] Cachalia and Klaaren op cit note 68 at 8.
[1099] Fraser op cit note 984 at 366.
[1100] Ibid.
[1101] Bauer, Lee-Makiyama, Van Der Marel and Verschelde op cit note 946 at 3.

[1102] Mishra op cit note 1028.
[1103] Bauer, Lee-Makiyama, Van Der Marel and Verschelde op cit note 946 at 3.
[1104] Fraser op cit note 984 at 365. For example, members of the Five Eyes community (of which Australia and Canada have imposed data localisation requirements) and bilaterally between Germany's BND and America's NSA (although Germany has been outspoken in criticising the PRISM program and its leading telecom company is contemplating a localised German-only network).
[1105] Fraser op cit note 984 at 365.

the foreign state enjoys jurisdiction over the cloud service provider.[1106] For example, the US has authority to compel Microsoft to disclose cloud data regardless of where the data are hosted.

One can argue that not all data localisation measures result in the infringement of the right to privacy. When countries with adequate data privacy laws adopt data localisation measures, violation of the right to privacy is highly unlikely. When a state's criminal laws have adequate security safeguards to protect the right to privacy, there is less likelihood of unlawful domestic surveillance or foreign surveillance. All foreign governments intending to access data will have to comply with local laws which protect privacy rights. Threats to privacy only manifest in cases where states with laws which permit unreasonable government access to data subsequently adopt data localisation measures.

c. Data localisation and national security interests

The way data are collected, used, stored, and transferred can have a material impact on national security, industry growth, geopolitical relationships, and civil society.[1107] National security interests are one of the commonly cited reasons for adoption of data localisation measures. However, the definition of national security is broadly defined. It is argued that the free flow of data to hostile or authoritarian regimes threatens the national security of their geopolitical adversaries. For example, South Korea does not want data on its citizens and corporations to be accessible by North Korea.[1108] Van Der Berg points out that Article 19 of the ICCPR protects the right to freedom of expression, the free flow of information and restrictions on data flows for national security purposes.[1109] Without clear definitions for national security interests and data localisation, governments have an opportunity to argue for stronger data localisation mandates.[1110] Some countries are concerned about the consequences of hosting their data in foreign data servers in instances of severed diplomatic relations with a government hosting their data.[1111] There is a danger that authoritarian governments can use data localisation as a tool to limit democracy and human rights. This includes the infringement and violation of freedom of movement, the right to speak freely and express political dissent, and the right to personal privacy as well as overall control over people.[1112]

d. Do data localisation measures address the growing spectre of cybercrimes?

Ironically, data localisation measures aimed at making it easier for LEA to access cloud evidence can potentially result in an increase in cybercrimes. When data are locally hosted on limited number of data centres, it creates an enticing target for those seeking illicit access.[1113] There are concerns that data

[1106] McKenna op cit note 230 at 1438.
[1107] Wu op cit note 922 at 1.
[1108] Sheppard, Yayboke and Ramos op cit note 1047 at 6.
[1109] Van Der Berg op cit note 394 at 3.
[1110]Sheppard, Yayboke and Ramos op cit note 1047 at 6.
[1111] Resha op cit note 969 at 7.
[1112] Sheppard, Yayboke and Ramos op cit note 1047 at 6.
[1113] Fraser op cit note 984 at 363.

localisation minimises the efficacy of corporate privacy and security controls and expanding the corporate network.[1114] If information is centralised and concentrated within specific servers in a country, it is more vulnerable to cyberattacks and external surveillance.[1115] By pooling and storing data in designated physical sites, it creates easy targets for hackers.[1116] It has also been argued that data localisation may result in less cybersecurity for data.[1117]

The African continent has weak domestic cybersecurity infrastructure which also results in less privacy protection.[1118] Van der Berg also argues that countries with weak cyber security protections (like Brazil, Indonesia, Vietnam) are at the forefront in advocating for data localisation measures.[1119] Some argue that domestic companies may not have the same or better technologies that leading global companies have due to fewer financial resources, less available expertise, less competitive need to draw customers or the presence of technological restrictions.[1120] Fraser's arguments are very generalised and based on the assumption that local companies will have less cybersecurity tools in place. To avoid such general assumptions, there is need for a detailed investigation of the implications of data nationalism.[1121] Kuner takes issue with these arguments. He argues that hackers and national intelligence services tend to target large global data centres because they have more data to access, thus putting them more at risk.[1122] Whilst this study shares Kuner's concern, there are points of disagreement or contention. Though bigger organisations may be attractive targets for syndicate cybercriminals, there is no evidence to suggest that most cybercriminals target big corporates. As discussed in chapter 3, with the prevalence of use of the internet and IoTs, different groups of cybercriminals have emerged, from inexperienced script kiddies who may target smaller businesses and individuals to criminal syndicates with experienced cybercriminals targeting big organisations and critical information infrastructure.

Successful cybercrime prosecutions are dependent on the investigating state being able to lawfully access electronic evidence either unilaterally or through the assistance of service providers. Adeleke argued that justifications for data localisation such as law enforcement purposes are not necessary in practice since companies are mandated to comply with government access requests for data regardless of where the data may be stored.[1123] This study has shown that this is not the case as service providers often deny access if data are stored in another country. As noted above, data localisation is likely to reduce the number of global service providers in a domestic market. Generally, local service providers

[1114] Brehmer op cit note 917 at 931.
[1115] Mishra op cit note 1028 at 496.
[1116] Shah op cit note 983 at 549.
[1117] Sheppard, Yayboke and Ramos op cit note 1047 at 7.
[1118] Kugler op cit note 915 at 7.
[1119] Van der Berg op cit note 394 at 6.
[1120] Fraser op cit note 984 at 363.
[1121] Kuner op cit note 1015 at 2098.
[1122] Ibid at 2096.
[1123] Adeleke op cit note 397 at 4.

do not have the financial resources and expertise compared to multinationals like Microsoft and Amazon.[1124] This would potentially mean that the level of cooperation and assistance that may be offered to law enforcement agencies will be reasonably poor and limited. If domestic companies do not have better technologies or expertise to assist LEA, that could potentially result in a decline in successful cybercrime prosecutions.

It should also be noted that the data localisation requirements set out in South Africa as well as in other African countries are new and yet to be fully implemented. As such, it is not possible to discern the exact extent to which these data localisation measures will assist LEA[1125] when accessing remote cloud data. Whilst there are economic benefits in unrestricted data flows, it is important to assess the benefits of data localisation vis-à-vis the storage and processing of data outside a country. This requires empirical research and empirical evidence and none has yet to take place.[1126] An analytical and empirical research on data localisation and its barriers should cover not only the scope and impact, but also the root causes and the design of governance mechanisms that could mitigate their negative effects.[1127] Van der Berg recommends that South Africa should 'exert its data sovereignty through innovative mechanisms' which allow it to extract value from data while protecting human rights.[1128] Van der Berg also opines that focus on location of data storage detracts from other important issues (such as purpose of data collection, persons processing the data and where data are collected from).[1129]

Some have also argued that instead of providing LEA with ease of access to electronic evidence, data localisation measures inhibit cybercrime investigations. It is argued that strict data localisation measures can further complicate an already convoluted and outdated MLAT system and increase barriers to law enforcement. Data localisation can potentially weaken current information sharing channels and businesses' reporting obligations, and ultimately impact intelligence gathering methods and criminal investigations.[1130]

V. CONCLUSION

Nations are sovereign in the sense that they wield legitimate and usually effective authority within a territory, including authority over data and data infrastructure in the territory, and over the people and firms in the territory that use the data and infrastructure.[1131] If such data and data infrastructure were to be placed in another territory, the nation's sovereignty interests are inhibited. This justifies data

[1124] Fraser op cit note 984 at 363.
[1125] Beyleveld op cit note 1045 at 4.
[1126] Ibid at 7.
[1127] Drake op cit note 1016.
[1128] Van der Berg op cit note 394 at 11.
[1129] Ibid.
[1130] Sheppard, Yayboke and Ramos op cit note 1047 at 7.
[1131] Goldsmith op cit note 930 at 818.

localisation and data sovereignty. Data localisation enables LEA to access electronic evidence from local service providers without having to wait for long winding processes associated with MLAT channels. Data localisation avoids the challenge currently associated with conflicting jurisdictions between different states. With territorial jurisdiction remaining as the basis to exercise enforcement jurisdiction, data localisation measures are in line with this principle.

Data localisation encourages and promotes the right to privacy of individuals during crime investigations as the individuals can easily enquire about the processes involved and get proper support in how their data are accessed. In a country with robust privacy laws like South Africa, data localisation measures will likely promote the right to privacy even during crime investigation. Where data are locally stored, LEA are compelled to put in place adequate security safeguards to protect personal data as well as to process evidence in a lawful manner. However, strict data localisation requirements may not be ideal for other economic reasons. Strict data localisation measures also cover non-personal data which may present a practical challenge for businesses such as undue financial obligations. This study submits that instead of adopting strict data localisation measures for purposes of LEA interests, states should opt for conditional data transfers or sectoral data restrictions. Strict data localisation measures stem from the fact that policymakers are reluctant to address the underlying challenges with existing legal mechanisms to improve the process of making cross-border requests for data.[1132] Conditional or liberal data localisation requirements strike the right balance between the interests of states to access evidence for crime investigation and the economic interests of businesses to share data globally.

Data localisation can speed up the process involved in investigating cybercrime. A state with data localisation measures is likely to solve or prosecute cybercrime cases much quicker as there are no MLAT processes to impede or slow down the process. On the downside, data localisation measures can potentially lead to an increase in cybercrime as the local service providers may not have the same cybersecurity systems as the international companies. This of course may not be a huge problem if the local service providers comply with internationally recognised cybersecurity standards or if multinational companies are permitted to operate locally subject to complying with the data localisation requirements. Data localisation also undermines cybersecurity by increasing cybersecurity threats as the attack surface area is increased due to local data centres. The security of data has nothing to do with who owns or controls the servers or the location of the data centres.[1133] The measures may also lead to increase in cybercrime particularly in cases where a state does not have cybercrime laws or laws regulating cloud computing services. Furthermore, data localisation measures restrict service providers from adopting cybersecurity best practice such as sharding, data fragmentation and partitioning.

[1132] Cory and Dascoli op cit note 1004 at 9.
[1133] Ibid at 5.

South Africa is in the top 5 countries mostly affected by cybercrime. Addressing cybercrime involves investigating the crime, gathering evidence, and prosecuting the cybercriminals. If the police are unable to get access to electronic evidence or if the process of getting electronic evidence is daunting, only fewer cybercriminals will be prosecuted. The importance of data localisation measures particularly the requirement to keep copies or duplicates of data locally is one of the effective ways to guarantee cybercrime investigations and prosecutions. When states wish to enforce their criminal laws, they should not be met with resistance from corporate entities. South Africa's NDCP should be applauded to the extent that it makes it mandatory for copies of data to be locally stored for purposes of LEA's access to the data. It is also important that government data and critical infrastructure data be locally hosted and processed. This will add another layer of protection of people's data that is under the control of government. Of the three main approaches to data localisation, conditional data localisation measures provide a balanced approach to the interests of LEA on the one hand the interests of service providers and users on the other. Conditional data localisation measures promote the flow of data with limited restrictions while also ensuring the protection of privacy and personal data. Strict data localisation measures should be avoided. Ideally, states should not adopt data localisation measures as a solution to the challenge of cross border cloud data. Instead, states should find other less inhibiting solutions to these legal challenges. The succeeding chapter of this study explores these solutions.

CHAPTER 6: TOWARDS RESOLVING THE JURISDICTIONAL CHALLENGES OF CLOUD DATA

I. INTRODUCTION

The underlying question of this research project was whether the nature of cloud computing technologies merited a reformulation or re-evaluation of jurisdictional principles in the context of cybercrime investigations. With the diverging approaches to jurisdiction at play, a proposal on new jurisdictional principles seems palatable. This study is not the first to discuss an alternative set of principles around internet jurisdiction globally. It is however, one of the fewer studies on this aspect in South Africa as the Cybercrimes Act was passed recently. Due to the lack of clarity in the Cybercrimes Act on the extent to which LEA can exercise enforcement powers over cross border data and the constant change in technology, this study will not be the last. It is inevitable that there will be further research on jurisdiction to address the technological changes of the future. This study is a point of reference for both current and future research on jurisdiction in technologically advanced environments.

The learned scholars who have previously interrogated and debated on this matter all advocated for somewhat different propositions to address internet and data jurisdiction.[1134] South African laws also seem to have adopted different approaches to data jurisdiction. Some approached data jurisdiction by focusing on where the data infrastructure is located, with the interpretation that the state where the data servers are located exercises territorial jurisdiction over the hosted data. This approach has been referred to as the location of data approach. Some interpreted data jurisdiction as the place where the data are accessible from. Meaning that location of the data centres hosting the data plays no role in determining data jurisdiction. This study referred to this approach as the Belgian approach. Data jurisdiction has also been established by focusing on the location of the cloud service provider with control over the data. If the cloud service provider is within the jurisdiction of a state, the state could easily request the service provider to disclose the data despite where the data centres are located.

This study is timely and may be a point of reference in interpreting South Africa's newly enacted Cybercrimes Act. As a new law, it is highly unlikely that the Cybercrimes Act will be amended at this early stage to address some of the concerns raised in this study. It is hoped that recommendations from this study can provide some guidelines when drafting the Cybercrimes Act's regulations or Standard Operating Procedures.[1135] These procedures must be observed by the police and investigators when investigating cybercrime committed using or facilitated by an article 20. This chapter seeks to

[1134] Kohl op cit note 676. Cedric Ryngaert *Jurisdiction in International Law* (2015) 2ed. Dan Jerker B Svantesson *Solving the Internet Jurisdiction* (2017).

[1135] Within 12 months after the Cybercrimes Act's commencement date, the Minister of Police is expected to issue Standard Operating Procedures. Section 26 (1) Cybercrimes Act.

provide meaningful and practical guidelines in the development and amendment of these SOPs issued by the SAPS.[1136] Some of the objectives of the draft SOPs include providing guidelines for the investigation, search, access, or seizure of an article; the procedure for dealing with data held by third parties and independent data holders, the operation of SAPS Designated Point of Contact, etc. The draft SOPs are a commendable step in the right direction. For example, they provide clarity on important considerations when preparing for search, access or seizure of an article.[1137] This study's discussion around the jurisdictional challenges over remote cloud data can be illuminating for the Minister of Justice and the Minister of Police. This discussion has the potential to influence the development of law and policy within this area. While the draft SOPs are commendable, they fail to provide solutions to the legal challenges identified in this study. For example, paragraph 4.5.2. of the draft SOPs permit a police official to receive and use non-publicly available data if the data are disclosed to the police official by a person who is in control of, or possession of the data. The provision also emphasises that it does not matter where the data are geographically located. As discussed in chapter 4 of this study, this approach to cloud data jurisdiction is problematic.

This chapter focuses on providing recommendations or solutions to the jurisdictional challenges associated with transborder cloud data. The chapter affirms that there is no 'one size fits all' solution to the complex problem of transborder cloud data.[1138] The proposed recommendations harmoniously protect privacy interests, the sovereignty of states and allow the criminal justice system to prevail. The aim of this chapter is to analyse the alternatives to jurisdiction as proposed by different scholars and critically assess them. The chapter seeks to not only propose pedagogical solutions but discusses pragmatic solutions which can be implemented in South Africa's cybercriminal justice system. The study acknowledges that any proposed recommendations or solutions do not provide definitive answers to jurisdiction and no solution is unblemished. However, some solutions are likely to bring us closer to a better approach to cloud data jurisdiction where there are minimal infringements on human rights and violation of interests of sovereign states.

One of the proposed solutions discussed in this chapter is rather unconventional for a study of this nature. The proposition has extraordinarily little to do with amending or reformulating law and policy. It is a solution which nudges lawyers, lawmakers, and policymakers to look elsewhere outside the letter of the law for viable solutions. The chapter explores alternative solutions to the jurisdictional dilemma which have more to do with the multistakeholder approach, code, and internet infrastructure.

[1136] The first draft Standard Operating Procedures were released for public comment on 15 July 2022. The deadline for submission of written comments on the draft was 15 August 2022. At the time of submission of this study, the procedures are not yet finalised. Invitation for Public Comments: Draft Standard Operating Procedures for the investigation, search, access or seizure of articles in terms of Section 26 of the Cybercrimes Act, 19 of 2020 Government Notice No 47021 GG 2292.
[1137] Paragraph 4.2. of the Standard Operating Procedures supra note 1119.
[1138] Halefom op cit note 22 at 40.

The chapter glosses over code as a solution. This solution, it should be unequivocally stated, is outside the scope of expertise for most legal and policy experts but can be incorporated into law and policy through insisting on certain principles like privacy by default and privacy by design.

II. REFORMULATING JURISDICTIONAL PRINCIPLES

From the discussions held in chapters 4 and 5 of this study, it became clear that states are more inclined to rely on the territoriality principle when exercising data jurisdiction. This is despite the heavy criticism levelled against this approach to jurisdiction by territoriality-nihilists. The preceding discussion has highlighted that despite different approaches to jurisdiction over cloud data, territory still plays a dominant role. The territory or location of data servers, the territory where the cloud service provider is located or the territory from where the cloud data are accessible from. The Belgian approach has left us questioning which relevant territory matters considering data are everywhere and anywhere.[1139] With these diverging jurisdictional principles and approaches, the question becomes which is the best approach to adopt?

Chapter 3 highlighted the importance of law being certain and easy to ascertain particularly when dealing with conduct in cyberspace. If the law is not clear on whether LEA can exercise jurisdiction over transborder cloud data, it is difficult for people to know with certainty which laws apply to their data hosted in the cloud. Chapter 4 of this study emphasised that data jurisdiction and internet jurisdiction principles emanate from the traditional principles of jurisdiction which are rooted in the territoriality principle. To avoid relying on the territoriality principle when dealing with data, it may require reforming our statutory mechanisms on jurisdiction and formulate distinct jurisdictional principles ideal for cyberspace and internet governance, whatever these principles might be. For South Africa, this would mean removing references to territory in the Cybercrimes Act and the ECT Act when determining the extent or reach of search warrants and powers of investigating officials.

A proposal for reformulation of jurisdictional principles is only worth considering if the existing approaches to data jurisdiction fail to meet the technological developments and the requirements of both domestic and international law. With each industrial revolution, laws were constantly updated to meet the needs and the changing circumstances. The 4th Industrial Revolution is no exception. The understanding is that if we have different or slightly different principles for cyberspace, then we can discard location of data as the basis for establishing jurisdiction.[1140] Lawmakers should be mindful of individual rights and sovereign interests of states when developing new jurisdictional rules.[1141] The above discussion has clarified that neither the location of data nor the 'give

[1139] Daskal op cit note 280 at 378.
[1140] Ibid.
[1141] Daskal op cit note 227 at 231.

us everything' approaches are satisfactory. Both approaches fail to reflect the sovereign and normative interests in settling baseline procedural and substantive protections of individual rights.[1142]

a. *What is the proposed framework?*

This study has shown that territoriality is problematic when asserting jurisdiction over cross border cloud data. As shown in chapter 5 of this study, territoriality-based thinking encourages data localisation[1143] and states should shift away from blind adherence to territoriality as the foundation of jurisdiction. The preceding debate has questioned whether the territoriality principle should continue to have relevance in cyberspace. If it is agreed that data defies territory and that technological developments warrant an amendment of the law, should states adopt non-territorial based jurisdictional principles? If so, what should these jurisdictional principles entail?

The proposed solution moving forward is for states to 'recognise that the territoriality principle and the associated territorial sovereignty no longer serve as useful starting points for the analysis of jurisdictional claims'.[1144] Instead of focusing on territorial-based jurisdictional principles, states should focus on core principles of substantial connection, legitimate interests and balancing of interests. This is the ultimate hybrid approach which considers several factors before a state can exercise jurisdiction over transborder cloud data. Svantesson proposes that –

> 'in the absence of an obligation under international law to exercise jurisdiction, a state may only exercise jurisdiction where:
>
> 1. there is a substantial connection between the matter and the state seeking to exercise jurisdiction;
> 2. the state seeking to exercise jurisdiction has a legitimate interest in the matter; and
> 3. the exercise of jurisdiction is reasonable given the balance between the state's legitimate interests and other interests.'[1145]

Non-territorialists have made a compelling argument that due to the arbitrariness, instability and location independence of data and its users, the territoriality doctrine does not suffice in determining the jurisdictional rules that apply to data.[1146] Substantial connection is determined by looking at whether there is a genuine connection between the subject matter of jurisdiction and the territorial base or reasonable interests of the state in question.[1147] Legitimate interests can be ascertained by looking at internationally recognized basis of jurisdiction such as nationality, protective principle, universality and

[1142] Daskal op cit note 227 at 231.
[1143] Svantesson op cit note 104 at 60.
[1144] Svantesson op cit note 1145 at 57.
[1145] Ibid at 60 - 61.
[1146] Daskal op cit note 280 at 378.
[1147] Svantesson op cit note 1145 at 63.

passive personality.[1148] This approach would mean that a state investigating a cybercrime committed by one of its citizens against one of its nationals, has both a substantial connection and a legitimate interest to access cloud data despite the location of the data.

With the potential infringement of sovereign interests of another state, Svantesson proposed that the third core principle will be to balance the interests of the investigating state and the interests of the state where data are based.[1149] Daskal also echoes the same viewpoint. She opines that an ideal jurisdictional approach should reflect both the legitimate sovereign interest in sometimes accessing data outside a state's borders and the countervailing interests in limiting access to citizens' and residents' data.[1150] Such an approach will also set a baseline procedural and substantive standards that apply to law enforcement requests for data.

Some of the interests that a state needs to assess relate to human rights and freedoms. The Malabo Convention confirms the establishment of regulatory frameworks on cybersecurity which takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and People's Rights.[1151] Article 15 of the Cybercrime Convention requires every member state to have domestic laws which provide for adequate protection of human rights and liberties. The implementation of conditions and safeguards shall include judicial or other independent supervision, grounds justifying application and limitation of the scope and the duration of such power or procedure.[1152] Importantly, the Cybercrime Convention provides that to the extent that is consistent with the public interest, in particular the sound administration of justice, each party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.[1153] The negotiations by the Cybercrime Convention Committee aimed at expanding the provisions of Article 15 of the Cybercrime Convention resulted in the drafting of the 2nd Additional Protocol.[1154] The protocol highlights the importance of the right to privacy and the protection of personal data during cybercrime investigations. It also sets out the important data

[1148] Ibid at 64.
[1149] Ibid
[1150] Daskal op cit note 227 at 231.
[1151] Preamble to the Malabo Convention.
[1152] Article 15 (2) Cybercrime Convention.
[1153] Article 15 (3) Cybercrime Convention.
[1154] Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

protection principles that states need to comply with when accessing electronic data.[1155] The 2nd Additional Protocol was opened for signature on 12 May 2022.[1156]

b. *What is the significance of this new framework?*

Svantesson correctly points out that a new framework represents an important philosophical and theoretical change. It changes the point of departure when discussing jurisdictional claims. Instead of primarily focusing on territory (where the data infrastructure is located, where the data are accessible from or where the person with control over the data is located), the new framework allows a state to consider other primary and relevant principles. The primary principles are to consider the interests of the LEA investigating the crime, the interests of the victim of the crime and the interests of the suspect or perpetrator. Svantesson argues that this new framework could 'liberate us from thinking that a particular state must always have jurisdictional claim over all aspects of data that happen to be located on a server located in that state'.[1157] Svantesson further argues that the dangers of a territoriality-focused single factor test are that we are forced to overlook matters such as the location, nationality and residence of data subjects, the situs of the crime, the availability of alternative means to access the data and the degree of interference with the sovereignty of other states.[1158] This has been the primary argument debated by data exceptionalists as discussed in chapter 4.

III. LEGAL SOLUTIONS TO ADDRESS THE JURISDICTIONAL CHALLENGES OVER CLOUD DATA

A proposal to reformulate jurisdictional principles is not an easy task. First, a proposition to amend domestic laws is not taken lightly. Apart from the superior courts' ruling in favor of amendment of a law, it is usually not easy for lawmakers to change laws. Secondly, at an international level, it is highly unlikely that countries will easily agree to change well-established principles which have shaped international interactions for decades. Thirdly, due to the differences in national laws, states may not be

[1155] When a state has received personal data, it is required to process them for a specific purpose and not for any other purpose. Article 14 (2) (a) 2nd Additional Protocol. State parties are also required to have appropriate technological, physical, and organisational measures for the protection of personal data against loss or accidental or unauthorised access, disclosure, alteration or destruction (Article 14 (7) (a) 2nd Additional Protocol. The Protocol also clarifies on how a state may share personal data with other domestic authorities as well as how to transfer personal data to another state or international organisation. Article 14 (9) (b) provides that '…a Party that has made a reservation under Article 27 may provide personal data it has received to its constituent States or similar territorial entities provided the Party has in place measures in order that the receiving authorities constitute to effectively protect the data by providing for a level of protection of the data comparable to that afforded by this article.' Article 14 (10) provides that 'the receiving Party may transfer the personal data to another State or international organisation only with the prior authorisation of the transferring authority or, for purposes of chapter II, section 2, the authority or authorities designated pursuant to paragraph 10.b.'

[1156] Available at https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention accessed 16 June 2022.

[1157] Svantesson op cit 1145 at 71.

[1158] Ibid at 73.

willing to adopt certain changes. For instance, common law countries mainly rely on territoriality when compared to civil law countries. Fourthly, creating separate rules for data introduces the problem of what counts as data.[1159] Fifthly, with the current developments towards digital sovereignty, it is highly unlikely that states are ready to let go of their sovereignty over data hosted on its servers and within its territories. This makes a reformulation of jurisdictional principles less effective, just like the rest of the other approaches to data jurisdiction discussed in chapter 4.

a. Change in terminology of legal text

To be successful in reformulating jurisdictional principles around data also involves rectifying the use of misleading language and terminology. One of the important points raised in cybercrime and cloud investigations is that inappropriate terminology may lead to unintended consequences. One such consequence is that geographical territory will continue to be the central basis to exercise data jurisdiction. For example, when data are in transit, the metaphor used is that there is a 'loss of location of data'. Such terminology suggests that objects including data, had a location which they lose when they are in the cloud.[1160] Koops and Goodwin argue that 'the metaphor of loss does not aptly capture the situation of data in the cloud as location may be difficult to determine at any point in time'.[1161] Some of these terms, though not necessarily mentioned in legal texts may help us understand cloud data jurisdiction better.

Instead of changing existing laws, one may change the language used in the law. The Explanatory Report to the Convention on Cybercrime also pointed out that certain words did not capture the essence of the internet. In a cyber-environment, instead of using words such as 'search' and 'seize', legislation should be replaced with more technological oriented computer terms such as 'access' and 'copy'. These changes, though seemingly subtle and insignificant, have the potential to change how people understand cloud jurisdiction and internet jurisdiction.

Changes in use of correct terminology should also extend to judicial decisions. Judges are responsible for developing law through their judgements. If judges continue to use incorrect analogies, this may diminish the meaning of certain concepts. For example, in *Google Inc v Equustek Solutions Inc*[1162], Google argued before the Canadian Supreme Court that a google search was akin to a librarian that managed one of several card catalogues. Justice Karakastanis suggested a different analogy,

[1159] Benton op cit note 171 at 207. The term data itself is very broad and there are different pieces of information which fall into the definition of data such as big data, electronic data, open data, personal data, non-personal data, etc. Basdeo defines data as unstructured facts or raw material that needs to be processed and organised to produce information. Vinesh Basdeo 'Criminal and procedural legal challenges of identity theft in the cyber and information age' (2017) 30 *South African Journal on Criminal Justice* 363 at 368.
[1160] Koops and Goodwin op cit note 146 at 42.
[1161] Ibid.
[1162] *Google Inc v Equustek Solutions Inc, Robert Angus and Clarma Enterprises Inc* 2017 SCC 34, [2017] 1 S.C.R. 824

comparing Google search to the person behind the counter of a bookstore. Svantesson seem to argue that the use of language plays an important role in data jurisdiction. Commenting on the *Google Inc v Equustek Solutions Inc* decision, Svantesson submits that the choice of analogy used can impact on the question of responsibility.[1163] If wrong terminology, wrong metaphors, and incorrect language are employed, we are likely to continue with regulatory challenges and inadequacy of regulatory tools.

b. Improvements on mutual cooperation

Cooperation among states remains the founding basis for any viable solution to data jurisdiction, criminal investigations, and successful criminal prosecutions especially for cybercrime. There are several international covenants which promote cooperation between states for purposes of criminal investigations.[1164] Chapter 5 of the Cybercrimes Act provides a framework to enable mutual assistance in cybercrime investigations. Section 47 of the Cybercrimes Act provides that the National Commissioner or the National Head of the Directorate may furnish any information obtained during any investigation to a law enforcement agency of a foreign state when he/she is of the opinion that the disclosure of such information may assist the foreign state in its cybercrime investigations.[1165] Similarly, the SAPS may receive any information from a foreign state which assist the SAPS with its own cybercrime investigations.[1166]

Lack of mutual understanding by countries may result in this study's proposed framework being futile. States can only be efficient in processing large numbers of requests for electronic evidence if they receive mutual assistance from other states. Cooperation among governments remain as one of the pillars for effective cybercrime prosecution at a global level.[1167] To respect the sovereign interests of other states, states should deal with jurisdictional questions through a series of bilateral or multilateral agreements.[1168] Such agreements would allow states to begin to set the applicable jurisdictional, procedural and substantive requirements without having to achieve total consensus as to the outcome.[1169] If bilateral and multilateral agreements on mutual cooperation are successful, other countries may adopt similar agreements which may result in such agreements being applied as international norms and standards.[1170]

[1163] Svantesson op cit note 104 at 29.
[1164] Article 25 of the Budapest Convention. Article 28 of the Malabo Convention. Part 9 of the Rome Statute deals with international cooperation and judicial assistance in respect of serious crime. SADC Protocol on Mutual Legal Assistance in Criminal Matters.
[1165] Section 47 (1) of the Cybercrimes Act.
[1166] Section 47 (2) of the Cybercrimes Act.
[1167] Murdoch Watney 'The way forward in addressing cybercrime regulation on a global level' (2012) 1 *Journal of Internet Technology and Secured Transactions* 61.
[1168] Daskal op cit note 280 at 395.
[1169] Ibid.
[1170] Ibid.

Mutual cooperation starts with states reaching consensus on important aspects relating to transborder data. The type of data sought can be used as a determining factor on whether the investigating state should obtain permission from the foreign state. This is made possible by the cooperation and mutual understanding among states on which type of data requires direct access and which types of data requires indirect access. This distinction on the types of data is absent under the Cybercrimes Act. Hence it is important to consider the solutions under the 2nd Additional Protocol. Mutual assistance requests are the primary methods to obtain electronic evidence of a criminal offence from other States, including the mutual assistance tools of the Budapest Convention. However, the T-CY found out that mutual assistance is not always an efficient way to process an increasing number of requests for volatile electronic evidence. Therefore, it was considered necessary to develop a more streamlined mechanism for issuing orders or requests to service providers located in other signatory parties to produce subscriber information and traffic data. The 2nd Additional Protocol to the Convention on Cybercrime provides a clear guideline on how to achieve this.

The 2nd Additional Protocol provides for measures for enhanced cooperation and provide a more streamlined mechanism for issuing orders or requests to service providers in other state parties to provide data. When LEA enter the territory of another state, they violate the principle of non-interference in the domestic affairs of another state. The acceptable approach is for a state to apply for assistance from the foreign state. There are different forms of assistance that a state may seek from the foreign state. These include mutual legal assistance[1171], extradition, transfer of criminal proceedings, transfer of prisoners, seizure and forfeiture of assets or recognition of foreign criminal judgements.[1172] One of the criticisms levelled against the Malabo Convention is its failure to provide broad cooperation amongst all AU states.[1173] This is also increased by the lack of ratification and implementation of the Malabo Convention by its member states.

It has been argued that mutual legal assistance system is not an effective solution for African countries. This is because most African countries do not make use of voluntary direct cooperation with foreign based service providers and neither do they have any jurisdictional leverage to compel foreign service providers nor the means to enforce their laws in an extraterritorial manner.[1174] Halefom further

[1171] Article 18 (3) of the UN Organised Crime Convention provides that mutual legal assistance may be requested for any of the following purposes – taking evidence or statements from persons; effecting service of judicial documents; executing searches and seizures and freezing; examining objects and sites; providing information, evidentiary items and expert evaluations; providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records; identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes; facilitating the voluntary appearance of persons in the requesting State Party; and any other type of assistance that is not contrary to the domestic law of the requested State Party.
[1172] Watney op cit note 641 at 293.
[1173] Dalton, van Vuuren and Westcott op cit note 177 at 117.
[1174] Halefom op cit note 22 at 30, 34.

argues that most African governments do not have MLATs in place with foreign government especially with the US.[1175] However, South Africa will benefit from the improvement of mutual cooperation systems as it has concluded several agreements with foreign governments.[1176] The AU as a region is also recommended to collaborate with regional and international key stakeholders to review and identify national frameworks and practices related to cross-border data access.[1177]

Apart from individual countries cooperating, it is also important for regional organisations to cooperate, exchange information and come up with solutions on many issues of mutual and global concern.[1178] The information that can be exchanged by organisations may relate to the principles and standards for the global combat against cybercrime. Schjolberg and Ghernaouti-Helie point out that regional organisations have the ability to assist and make guidelines for their member countries within the regional traditions.[1179] Some of the guiding principles on data as set out under the AU Data Policy Framework are worth noting when developing and modernising laws to regulate data. Among others, South Africa should strive for cooperation with AU member states and other states for the exchange of data.

Some of the regional organisations which can play a critical role in fighting cybercrime include the SADC, AU, EAC, ECOWAS, EU, Council of Europe, G8 Group of States, OAS, ASEAN, APEC, SCO, OECD, NATO, the League of Arab States, the Commonwealth and EU. There are also recommendations for global organisations such as ITU, INTERPOL and UNODC to cooperate and share information with these regional organisations. The ITU previously nominated members of the High-Level Experts Group to provide it with advice on complex issues surrounding cybersecurity. One of the recommendations made by the HLEG was that governments should cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime.[1180]

Under the 2nd Additional Protocol, LEA are permitted to cooperate directly with service providers in other state parties when requesting either domain name registration information[1181] or subscriber information. Information that is submitted when registering a domain name can be useful in identifying either the person who registered the domain name or the entity associated with the domain

[1175] Halefom op cit note 22 at 30, 34.
[1176] A detailed list of the agreements in place is available at *https://www.justice.gov.za/ilr/mla.html* accessed on 12 October 2022.
[1177] Halefom op cit note 22 at 42.
[1178] Schjolberg and Ghernaouti-Helie op cit note 520 at 59.
[1179] Ibid at 60.
[1180] Report of the Chairman of HLEG. ITU Global Cybersecurity Agenda (GCA) High-Level Expert Group (HLEG).
[1181] Domain name registration information is held by entities which provide domain name registration services and include organisations that sell domain names to the public (registrars) as well as regional or national registry operators which keep databases of all domain names registered for a top-level domain and which accept registration requests. 2nd Additional Protocol supra 1132 at 43.

name. The explanatory note to the 2nd Additional Protocol notes that access to information of the person who registered the domain name is critical to identify a suspect in a specific criminal investigation or proceeding.[1182] For example, when registering a domain name in South Africa, one would need to provide information such as the registration number of a legal entity, the ID number of the director of the entity, email address, phone number, fax number and physical address.[1183] Article 6 of the 2nd Additional Protocol provides that when a State Party is investigating specific crimes, it may issue a request to an entity providing domain name registration services in the territory of another State Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name. Obtaining the domain name registration data is often indispensable, as a first step for many criminal investigations and to determine where to direct requests for international co-operation.[1184]

While Article 18 of the Cybercrime Convention already addresses some aspects of obtaining subscriber information[1185] from service providers, the 2nd Additional Protocol provides complimentary tools to enable investigators to obtain the disclosure of the subscriber information directly from a service provider in another state. To address the challenges associated with subscriber information, the 2nd Additional Protocol allows an investigating state to directly approach a service provider in a foreign state and request for disclosure of subscriber information in that service provider's possession or control. The subscriber information must be needed for purposes of specific criminal investigations or proceedings.[1186] The service provider must be in the territory of a foreign state who is a signatory to the Budapest Convention. Like domain name registration information, subscriber information is information that a person submits when subscribing to receive certain services from a service provider and includes names, addresses, telephone number, IP address or credit card or bank account number linked to the subscriber's account. Subscriber information can identify the user of a service and is the most often sought information in cybercrime investigations as well as other crimes involving electronic evidence. Without subscriber information, it is often impossible to proceed with certain investigations.

[1182] 2nd Additional Protocol supra note 1132 at 42.
[1183] Registration of domain names can be done with the Companies and Intellectual Property Commission (CIPC). https://eservices.cipc.co.za/files/DomainNameServices_Guide.pdf accessed 10 August 2021.
[1184] 2nd Additional Protocol supra 1132 at 42.
[1185] The Cybercrime Convention defines subscriber information as;
'…any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (a) the type of communication service used, the technical provisions taken thereto and the period of service; (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. Article 18.3. Budapest Convention.
[1186] Article 7 of the 2nd Additional Protocol supra note 1132.

The tools provided under the 2nd Additional Protocol would increase the efficiency of the process and relieve pressure on the mutual assistance system.[1187] The disclosure of subscriber information may be of a lower degree of intrusiveness compared to the disclosure of other categories of data.[1188] As discussed in chapter 4 of this study, Article 18 of the Budapest Convention is limited as it only applies when a service provider is 'in the territory' of the investigating party or 'offering its services' in the investigating party. Article 18 did not provide a complete solution to cross border subscriber information. The 2nd Additional Protocol goes beyond the scope of Article 18 of the Budapest Convention by allowing a party to issue certain orders to service providers in the territory of another party.[1189] This is commendable and goes to a greater extent in addressing the challenge of cross border data amongst signatory parties to the Cybercrime Convention.

Certain forms of data require the investigating state to obtain permission from the foreign state before accessing the data. Traffic data and stored computer data require cooperation from the foreign state. Traffic data is defined as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication'.[1190] The disclosure of traffic data may be necessary for tracing the source of a communication as a starting point for collecting further evidence or to identify a suspect.[1191] The purpose of Article 8 of the 2nd Additional Protocol[1192] is for a requested state to have the ability to compel a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control for the benefit of a requesting state.[1193]

One of the concerns with mutual cooperation is that MLAT systems are slow and clumsy. For example, the United States takes an average of ten months to respond to law enforcement requests made pursuant to the MLAT process while other countries take even longer.[1194] MLAT systems were generally designed to handle rare transnational cases and not the rapid international cooperation

[1187] 2nd Additional Protocol supra 1132 at 32.
[1188] 2nd Additional Protocol supra 1132 at 46.
[1189] 2nd Additional Protocol supra 1132 at 47.
[1190] Information Commissioner's Office (ICO). https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/traffic-data/ accessed 10 August 2021.
[1191] Explanatory Report to the 2nd Additional Protocol para 23.
[1192] Article 8 of the 2nd Additional Protocol provides that each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested party's territory to produce specified and stored subscriber information and traffic data in that service provider's possession or control which is needed for the party's specific investigations or proceedings.
[1193] 2nd Additional Protocol supra note 1132 at 53.
[1194] Daskal op cit note 280 at 393.

required in today's interconnected world.[11951196] However, it should be clear that an improvement in the efficiency of the MLAT channels does not solve the issues of data jurisdiction.[1197] Article 8 of the Budapest Convention is designed to be more streamlined than mutual assistance currently is, in that the information the requesting party must provide is more limited, and the process for obtaining the data more rapid. Article 8 of the Budapest Convention compliments and is without prejudice to, other mutual assistance processes under the Budapest Convention or other multilateral or bilateral agreements which a party remains free to invoke. The requested party must service the service provider within 45 days and order a return of requested information or data no later than 20 days for subscriber information and 45 days for traffic data.[1198]

As discussed in chapters 3 and 4, cybercrime can have a huge impact on economies and social life and as such, investigation of such crimes can be time sensitive. For example, if a cybercriminal hacks into and cripples a hospital IT system that can be life threatening to patients, and can cause financial losses for the hospital and its service providers. Emergencies may also arise in situations such as in the immediate aftermath of a terrorist attack or when investigating email accounts used by kidnappers to issue demands and communicate with the victim's family.[1199] Such crimes may require expediency to investigate. However, due to the slow-paced processes of MLAT channels, it may take a very long time before the investigators get access to relevant evidence in cases where the evidence is in another country. To address this jurisdiction related problem, the 2nd Additional Protocol provides for an investigating state to request for immediate assistance in obtaining the stored computer data in a service provider's possession or control, without a request for mutual assistance.[1200]

c. Cooperation between police officials and cybersecurity experts

Mutual cooperation should not be limited to governments entering into agreements to permit their foreign counterparts to gain access to locally stored electronic evidence. Cooperation should also extend to law enforcement agencies. International cooperation by countries remains the most effective way to address the jurisdictional challenges presented by the internet and the cloud. If different players are involved, domestic law enforcement agencies do not need to exercise extraterritorial jurisdiction to access data and potentially infringe on the sovereign interests of a foreign state. One of the recommendations suggested by Cassim to combat cybercrime was the collaborative initiatives involving the police, the private sector and academia.[1201] Snail also highlighted the importance of the

[1195] Halefom op cit note 22 at 17.
[1196] Laviero Buono "Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches" (2016) 17 *ERA Forum* 343.
[1197] Daskal op cit note 280 at 394.
[1198] Article 8 (6) of the 2nd Additional Protocol to the Budapest Convention.
[1199] 2nd Additional Protocol supra note 1132 at 58.
[1200] 2nd Additional Protocol supra note 1132 Article 9.
[1201] Cassim op cit note 41 at 132.

police cooperating with cybersecurity experts when securing electronic evidence due to the technical nature of many of the cybercrime investigations.[1202] Sutherland also confirms that there should be joint action by governments, ministries and international bodies to deal with cyberthreats.[1203] The South African Police Service is in dialogue and working closely with various departments, national and international experts in the field of cybersecurity to develop the SAPS Cybercrime Strategy.[1204] Some of the collaborators include the EU. Through such cooperation, governments can effectively address the global nature of cybercrime and ensure the integrity of the internet.[1205]

The 2nd Additional Protocol also encourages joint investigations between state parties. Under Article 12, competent authorities of signatory parties may establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings. An arrangement under this protocol allows the competent authorities to communicate directly[1206] and the investigating party does not need to submit a request for mutual assistance.[1207]

In terms of the Cybercrimes Act, foreign states can submit a request for preservation of data, seizure of data, expedited disclosure of traffic data, interception of communications and obtaining of real-time communication-related information or archived communication-related information.[1208] This request must be submitted to the designated point of contact. The point of contact can provide the foreign state with assistance such as technical advice, legal assistance, identification and location of an article or identification and location of a suspect.[1209] With the Cybercrimes Act still relatively new, it remains to be seen how effective the point of contact will be in aiding foreign states. The draft SOPs also provide that the designated point of contact will be within SAPS structures.[1210] With the lack of adequate skill within South Africa's police force, one can argue that foreign states may not get meaningful assistance from South Africa unless if they bring their own skilled investigators on board.

Calcara cautions however that there are traditional legal issues hampering international police cooperation which arise from the incompatibility of national laws and criminal justice system.[1211] The challenges are that police services might decide to desist on activating cooperation processes if

[1202] Sizwe Snail, Anthony Oliver and Jason Jordaan *Cybercrimes and Cybersecurity Bill: What you need to know: Reflecting the law as at 16 March 2018* (2018) at 55.
[1203] Ewan Sutherland 'Cybersecurity: governance of a new technology' PSA18 Political Studies Association International Conference, Cardiff 26 -28 March 2018.
[1204] Annalise Kempen 'EU-SAPS Dialogue Facility: Cybercrime project' (2021) *Servanus Community-based Safetyand Security Magazine* 30 at 30.
[1205] Cassim op cit note 41 at 126.
[1206] 2nd Additional Protocol supra note 1132 Article 12(4).
[1207] 2nd Additional Protocol supra note 1132 Article 12 (5).
[1208] Section 48 (1) Cybercrimes Act.
[1209] Section 53 (3) Cybercrimes Act.
[1210] Paragraph 13 of the draft SOPs.
[1211] Giulio Calcara 'Rethinking legal research on matters of international police cooperation: Issues, methods and raison d'tre' (2019) 40 *Liverpool Law Review* 95 at 98.

differences in substantive criminal law are significant. Police services might share documents which possess legal status in some countries while being void of any legal value in others. The other concern with cooperation is that it may be misused by countries to track dissidents outside their borders.[1212] Unfortunately, this challenge is likely to persist regardless of the type of approach to cloud data jurisdiction.

While a lot of cybercriminals have been apprehended through joint efforts of law enforcement agencies from different countries and organisations like INTERPOL[1213] and EUROPOL[1214], there are other collaborative efforts worth exploring. Cooperation should extend to members of the police force working together with cybersecurity experts in the private sector who have the skillset to deal with cybercriminals as well as the extensive knowledge on relevant information security practices. One of the drawbacks when it comes to cybercrime investigation and particularly gathering of electronic evidence is that most police officers lack the relevant skills to seize, access and analyse electronic evidence. The lack of compatibility of national laws and criminal justice systems can also hamper efforts for police cooperation in cybercrime investigations.[1215] South Africa's NCPF[1216] also noted the importance of capacity building through skilling LEA with relevant skillsets to deal with cybercrime.[1217] The HLEG also emphasised on the importance of collaborative work to enhance security procedures and technical measures. The ITU was identified as a global centre of excellence for the collection and distribution of timely telecommunications / ICT cybersecurity-related information, including a publicly available institutional ecosystem of sources to enhance cybersecurity capabilities worldwide.[1218] Part of this cooperation include collaborating in the development of materials for establishing national CSIRTs and for effectively communicating with CSIRT authorities.

South Africa's Cybercrimes Act and the NCPF also make provision for cooperation between foreign governments and local law enforcement agents and cooperation with cybersecurity experts. The NCPF recognises that South Africa does not have coordinated cybersecurity efforts.[1219] Some of the goals of the NCPF are to coordinate the promotion of cybersecurity measures by all role players in relation to cybersecurity threats, through interaction with and in conjunction with the Cybersecurity

---

[1212] Ibid.
[1213] https://www.interpol.int/en/Crimes/Cybercrime accessed 05 February 2022.
[1214] https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime accessed 05 February 2022.
[1215] Calcara op cit note 1222 at 98.
[1216] The NCPF provides that '… a cybercrime strategy would nevertheless need to ensure that the forensic capabilities be created that are necessary to analyse electronic evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect'. National Cybersecurity Policy Framework for South Africa GG 39475 GN609 4 December 2015 at 71.
[1217] Lack of skilled LEA is not only common in South Africa but is prevalent in other countries. Research study conducted in Nigeria pointed that the Nigerian government is not well equipped with sophisticated hardware to track down cybercriminals. Onuora, Uche, Ogbunude and Uwazuruike op cit note 59 at 4.
[1218] Report of the Chairman of HLEG op cit note 1163.
[1219] NCPF supra note 1194 at 77.

Hub and strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyberterrorism and cyber warfare and establishing PPPs for national and action plans in line with the NCPF.[1220] Whilst this solution is commendable, one should note that this is a long-term goal which is likely to take a considerable time for skilling all police officers to enable them to deal with cybercrime cases.

Apart from cybersecurity experts training LEA and working closely with them, another form of cooperation worth mentioning is in the development of new norms and standards or incorporation of existing information technology standards. For example, the ISO standards are generally viewed as international best practice. Such standards can be used to provide guidelines and recommendations on what may need to be done in situations were sought after electronic evidence is transborder. For example, if it becomes standard practice for investigators to secure evidence regardless of its location and to subsequently apply to relevant courts for permission to access such evidence, it becomes much easier for states to amend their laws around data jurisdiction as well as to enter into more multilateral agreements to permit LEA to gain access to the evidence.

d. A United Nations Treaty on Cybercrime

One of the most effective ways to address the global problem of cybercrime and the common challenge with cross border access to cloud data is by adopting a more global framework on cybercrime through the United Nations. Nduka and Basdeo argue that the reliance on national and regional legislative initiatives to tackle cybercrime are inadequate and states should strive for a global legislative framework.[1221] Schjolberg and Ghernaouti-Helie also argue that the problems presented by cloud computing may only be solved through a global Convention or Protocol. Such a global framework should include the necessary jurisdictional provisions in terms of international law. The learned scholars submit that the jurisdictional provisions would relate to serious crimes in cyberspace whether or not they were possible to prosecute under national law.[1222] Cassim also argued that the United Nations should draft a UN treaty within the ambit of international law. This treaty should make provision for extra-territorial jurisdiction, the establishment of an International Criminal Court for Cyberspace, and provide developing countries with technical and financial assistance to enforce cybercrime laws.[1223] Unlike the Budapest Convention, a UN based treaty is much wider in geographic scope and open to all

[1220] NCPF supra note 1194 at 71.
[1221] Rapuluchukwu Ernest Nduka and Vinesh Basdeo 'The need for harmonised and specialised global legislation to address the growing spectre of cybercrime' (2021) *Southern African Public Law* 1.
[1222] Schjolberg and Ghernaouti-Helie op cit note 520 at 49.
[1223] Murdoch op cit note 1178.

member states.[1224] Clough correctly points out that there is an opportunity to address challenges identified with the Budapest Convention to allow for wider acceptance.[1225]

Currently, the United Nations is considering a UN treaty on cybercrime. In 2019, the General Assembly passed a resolution on countering the use of information and communication technologies for criminal purposes.[1226] In terms of this resolution, an open-ended ad hoc intergovernmental committee of experts and representatives of all regions was established. During its first session held from 28 February to 11 March 2022, the ad hoc committee proposed its road map and mode of work.[1227] There are six sessions planned between 2022 and February 2024. The final output of the ad hoc committee is the finalisation and approval of the draft text of the convention, the discussion and approval of a draft resolution to which the text of the draft convention will be annexed, for consideration and adoption by the General Assembly at its 78th session in 2024. While most countries understand and recognise the importance of a global treaty on cybercrime, there are still concerns of lack of trust among governments.[1228] The development of a UN treaty on cybercrime is welcome. An effective cybercrime treaty should consider the challenges of cloud data jurisdiction and propose solutions that will enable criminal investigations to proceed while protecting and promoting human rights.

IV. NON-LEGAL SOLUTIONS TO ADDRESS THE JURISDICTIONAL CHALLENGE TO CLOUD DATA

It should be noted that legal solutions are only a partial response to the challenge posed by cross border data.[1229] This section explores other avenues which addresses the jurisdictional dilemma without necessarily changing the *ex lege lata*. The aim of this discussion is to provoke a discussion on the importance of solutions which lie outside the realm of legislative terrains but has a meaningful impact in how we view data jurisdiction.

a. Regulating the internet infrastructure – code is law

When one considers the impasse between territorialists and non-territorialists, it becomes clear that whatever approach to data jurisdiction is adopted, there will continue to be a conflict of laws. Even

[1224] Clough op cit note 57 at 729.
[1225] Ibid.
[1226] United Nations Resolution adopted by the General Assembly on 27 December 2019 A/RES/74/247.
[1227] Road map and mode of work for the Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/AHC_Road_map.pdf accessed on 15 May 2022. Report of the ad hoc committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes on its first session. A/AC291/7 UN General Assembly 24 March 2022.
[1228] Summer Walker and Ian Tennant 'Control, alt or delete? The UN cybercrime debate enters a new phase' 2021 *Global Initiative Against Transnational Crime Policy Brief* 1 at 1.
[1229] Joanna Kulesza 'New technologies and the need of a uniform legal system' 2007 https://dx.doi.org/10.2139/ssrn.1446768 accessed 12 October 2022.

in instances where parties cooperate by means of multilateral agreements and conventions, the system is still flawed as not every state will be willing to accept and ratify the terms of a convention or MLATs. The Cybercrime Convention for instance, has a lot of member states but a state may only accede to the Convention upon invitation.[1230] If some countries do not accede to the Convention or are not invited to accede to the Convention, this may suggest continuous gaps in mutual cooperation around cybercrime. A question that needs to be asked is whether there are other solutions outside law which can address the problem of jurisdiction once and for all. Some of these solutions, like use of software programs, have also been proposed in the context of protecting users against cybercrime.[1231] This study considers these mechanisms as solutions for the cloud data jurisdiction problem.

The internet infrastructure has been considered as the most effective way to regulate the internet. Murray discusses the arguments presented in Joel Reidenburg's Lex Informatica book. Reidenburg argued that instead of focusing on what laws, regulations or policies governments should adopt, the solution should focus on regulating the infrastructure itself. The regulation would involve indirectly mandating changes to network infrastructure or supporting self-regulatory activities of network designers.[1232] This study submits that these views should be explored further. According to Lessig, there are four methods of regulation that apply to both cyberspace and the natural world.[1233] These are regulation through architecture, through norms, through the market and the law. Of these methods, Lessig believes that internet architecture is the most effective.

Lessig expounds more on the important role played by code and expresses that understanding proper regulation of cyberspace consists of going back to the internet infrastructure and allowing code to regulate conduct in cyberspace.[1234] As we have already seen in chapter 4, states have diverging approaches to data jurisdiction. Internet infrastructure or code seem to be the objective approach to jurisdiction. While commenting on a problem that online gamers faced, Lessig pointed out that problems can be programmed or coded and they can be coded away.[1235] Lessig points out that the nature of the internet is not God's will. Its nature is simply the product of its design.[1236] This means that if we need a different outcome on how the internet works, we can easily do that by changing the internet infrastructure. The cloud is unique because it was designed that way. By design, cloud data can move from one server to the other seamlessly, to be replicated and to be split. Following the argument by

[1230] Article 37 of the Budapest Convention provides that 'after the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention.'
[1231] Chawki, Darwish, Khan and Tyagi op cit note 446 at 74.
[1232] Murray op cit note 801 at 16.
[1233] Lawrence Lessig *Code and Other Laws of Cyberspace* 1999.
[1234] Lawrence Lessig *Code version 2.0.* 2ed (2006) at 5.
[1235] Ibid at 15.
[1236] Ibid at 38.

Lessig, this study submits that if this design of cloud data is tampered with, or perhaps changed, then it is possible from an architectural level for one state to have primary jurisdiction over the cloud data. The design of the architecture may investigate whether the state where the data originated from should have the primary jurisdiction or substantial connection to the data. Alternatively, the architecture can be designed in such a way that the state where data are stored will have substantial connection to the data. Whichever protocol is applied, the underlying code has the power to effectively alter how states view cloud data jurisdiction.

Code affects regulability and governments are using law to interact with code to induce it to regulate differently.[1237] Current developments across the globe reflect the importance of regulation by code, though laws and policies may end up being put in place to rubber stamp such a position. Chapter 5 of this study discussed about data localisation laws and policies being implemented by states to prevent free flow of data across borders. What should be noted is that service providers would need to regulate cross border data at an infrastructural level. They must change the underlying cloud infrastructure which allows for data to be shared cross border. The new instruction to the cloud infrastructure software means that data may only be transmitted to another cloud server if the data centres are both within the physical borders of a state. This is code at work.

Architecture is a kind of law which determines what people can and cannot do.[1238] Internet shutdowns, internet throttling and content filtering are some of the popular ways that governments use code to regulate conduct. Though Lessig's arguments were made at a time when the world was not overtaken by social media companies like Facebook, Twitter and Tiktok, they are quite revelational. Technology companies, apart from being under government regulation, are also regulated by code. Social media companies, as discussed in chapter 2, have put in place terms of service and community guidelines. There is certain content which may be automatically unavailable in certain regions for a plethora of reasons. Some of the reasons may be domestic laws in that area do not permit the publishing of certain content or because the content could be against the cultural practices of the people in that area. A lot of governments resort to geo-blocking technologies and requesting service providers to block access to certain online content.[1239] The *Google Spain*[1240] and *Google French*[1241] right to be forgotten cases also reflect how in practice code is used as a form of regulation in addition to existing forms of

[1237] Ibid at 72.
[1238] Ibid at 77.
[1239] Content blocking, filtering and other technical or legal limits on access to internet content restricts the right to freedom of expression and freedom of assembly and association. AfDEC Principles op cit note 344 at 17 and 20.
[1240] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12.
[1241] *Google v CNIL* Case C-507/17.

regulation. Service providers would need to change the underlying code of the internet infrastructure which makes certain content accessible in one state while not accessible in another state.

Lessig correctly points out that code writers are increasingly lawmakers. Of course, he did not mean lawmakers in the sense of parliamentarians or policymakers. Rather, code writers act as proverbial lawmakers in how they use code to determine how cyberspace activities are carried out. Computer algorithms determine where the data will be stored and the pathway that data takes when in transit.[1242] Through code, one can determine who has access to what data and to what extent. Through code, the defaults of the internet and the degree of anonymity are set. Code can also be used to determine if privacy will be protected or not.[1243] Similar to Lessig's thinking, Reidenburg also identifies network architecture as the second rule making process after contractual agreements between ISPs and customers.[1244] Reidenburg asserted that whereas political governance processes usually establish the substantial laws of nation states, in lex informatica the primary sources of default rule making are the technology developers and the social processes through which customary uses of the technology evolve.[1245]

Murray submits that, 'in light of the lex informatica's dependence on design choices, the attributes of public oversight associated with regulatory regimes could be maintained by shifting the focus of government actions away from direct regulation of cyberspace towards influencing changes to its architecture'.[1246] Reidenburg's concept of regulatory control led to the development of a new cyberpaternalist school. This new school viewed legal controls as merely part of the network of effective regulatory controls in the online environment.[1247] Lawmakers seeking to control the online activities of their citizens would seek to control these activities indirectly by mandating changes to the network infrastructure or by supporting self-regulatory activities of network designers.[1248]

[1242] Daskal op cit note 280 at 368.
[1243] Lessig op cit note 1245 at 79.
[1244] Murray op cit note 801 at 15.
[1245] Ibid.
[1246] Ibid at 16.
[1247] Ibid.
[1248] Ibid at 16. Murray poses a question on whether a rule of law exist online in the face of increasing legal interventions into online activity by both governments and judges and if so, who is the legitimate lawmaker and what values are enshrined by cyberlaws and cyberlawmaking? Murray argues that when we venture out with the world of atoms and into the world of bits, both paths lead to the same destination. No one seems to agree on what the rule of law actually is. 'At its core the rule of law requires that government officials and citizens are bound by and act consistent with the law. This basic requirement entails a set of minimal characteristics: Law must be set forth in advance (be prospective), be made public, be general, be clear, be stable and certain, and be applied to everyone according to its terms. In the absence of those characteristics, the rule of law cannot be satisfied'. Murray understands that it is not quite simple to suggest that law must be set forth in advance and law must be made public. While many laws from around the world are made available online, not all are and where they are available many are not available in translation. The author notes that this is a challenge to the rule of law if we accept the principle of extraterritorial effect.

When one considers issues around data governance in the age of the internet of things, one can appreciate and agree with the notions presented by Lessig. Principles such as privacy by design and privacy by default are not focusing on regulating how service providers process personal data. Rather, they focus on the design and development of the software and the products themselves to ensure the products have privacy enhancing and privacy protecting mechanisms in place. What this means is that there is a shift from regulation itself to the infrastructure or code. Code therefore plays an important role in regulating the internet space. If code is law, it will not matter if states have differences in laws and regulations. For example, if products are designed with privacy enabled technologies, users are more protected and enjoy a sense of privacy regardless of being in jurisdictions which have no data protection laws.

Code can play the same role as the regulator and produce similar effects as when laws or regulations are in effect. By applying code, important rules are imposed, not through social sanctions, and not by the state, but by the very architecture of the space.[1249] The internet architecture itself will affect behaviour and indirectly lead to change of behaviour.[1250] For instance, cryptocurrencies' underlying blockchain technology is designed to promote anonymity. Even though most countries do not have laws regulating cryptocurrencies or crypto-assets, people are still able to transact and engage in crypto-assets as the underlying code regulate the transactions. People do not need to trust each other but can trust the blockchain technology. Cybercriminals, though acting unlawfully in terms of government laws and rules, still rely on code to regulate their 'unlawful' behaviour. Cybercriminals on the dark web can 'trust' each other and transact in bitcoin. Their trust is on the underlying blockchain technology and its proof of use concept which provides all the assurances necessary for a successful transaction. Because of the anonymity of code, criminals can break the law as they know their identities will not be revealed. While code is law, it should also be noted that the same code can create the potential for more criminal activities as cybercriminals can rely on the anonymity offered by the architecture.[1251]

One important aspect worth discussing is the importance of multi-stakeholderism which is explored in detail in the following paragraphs. As already mentioned above, instead of lawmakers focusing on means to exercise jurisdiction over remote cloud data, the focus should be on engaging software programmers, software developers and tech service providers to assist in developing code which can regulate internet jurisdiction. Through code, certain countries should be able to determine if they have enforcement jurisdiction over cloud data without having to go through unreasonable lengths to get assistance from foreign states. Such code should be designed to promote international trade, free flow of information and protect human rights. It should be noted that it is not for lawyers to decide how

[1249] Lessig op cit note 1245 at 24.
[1250] Ibid.
[1251] Hee Jhee Jiow 'Cyber crime in Singapore: An analysis of regulation based on Lessig's four modalities of constraint' 2013 *International Journal of Cyber Criminology* 1 at 16.

code can be used to resolve the jurisdictional dilemma. Lawyers should demand and expect a technology which can meet expected outcomes. It is not for lawyers to worry about how the underlying software will be developed and how it will function. Lessig's words resonate here -

> "All of us must learn at least enough to see that technology is plastic. It can be remade to do things differently. And that if there is a mistake that we who know too little about technology should make, it is the mistake of imagining technology to be too plastic rather than not plastic enough. We should expect and demand that it can be made to reflect any set of values that we think important. The burden should be on the technologists to show us why that demand can't be met…"[1252]

b. If code is law, what does it mean for the debate between territorialists and non-territorialists?

Daskal observes that the features of data mean that it is difficult to draw a line in the sand on the differences between what is territorial and what is extraterritorial.[1253] The argument is that attributes of data should be taken into account in determining the jurisdictional rules that apply.[1254] However, if code is law, code can make cloud data features bound to a particular territory apart from the cloud data being hosted in a certain state. Software developers can develop code in such a way that the territoriality principle can be the default principle applicable to cloud data. At present, the underlying cloud infrastructure and code has been designed to make a particular location of less relevance and what is more relevant is who can access the cloud data. This is what Lessig meant when he said that code can be used by government to reinforce a particular viewpoint.[1255] Of course, when changing the underlying architecture of the cloud, coders need to preserve the prominent features which make cloud computing an attractive computing solution such as location independence of data, data mobility and data divisibility.

c. Multi-stakeholder approach

When it comes to safeguarding the privacy interests and security of data, governments are usually not the primary actors as that role falls on service providers as data controllers[1256]. As discussed in chapter 5 of this study, private actors are powerful institutions which control a lot of data belonging to governments, businesses, and individual persons. Service providers are also central to investigations as the bulk of sought-after data are under their control or possession. For instance, chapter 8 of the Cybercrimes Act recognises the role of electronic communications service providers and financial

[1252] Lessig op cit note 1245 at 32.
[1253] Daskal op cit note 227 at 222.
[1254] Ibid at 226.
[1255] Lessig op cit note 1212 chapter 5.
[1256] A data controller is defined in most data protection laws as the person who determines the purpose and means of processing personal data.

institutions in cybercrime investigations. There is an obligation on service providers to report an offence or preserve any information which may be relevant to an investigation.[1257] Decisions of private actors often determine which government's rules apply, how these rules are interpreted, and how much of data are and should be accessible to governments.[1258] Efforts have been made to resolving the conundrum of internet jurisdiction through either a more global law or a less global internet.[1259] The exercise of territorial jurisdiction leads to a less global internet.[1260] Innovative governance promotes a more global law which comprises of the harmonisation of rules regarding jurisdictional competence and harmonisation of substantive law, by treaty, by deregulation (private imposition of code, user self-help) or by default (courts adopting country of origin / destination approaches).[1261]

The current global cybercrime legislative landscape reflects a multilateral model. Under this model, countries exercise cyber sovereignty by formulating the rules that apply in cyberspace based on their sovereignty over the territory or the persons involved.[1262] Innovative governance means replacing the multilateral model with the multi-stakeholder approach. The multistakeholder model of internet governance is the best mechanism for maintaining an open, resilient, and secure internet. Such an approach is informed by a broad foundation of interested parties, including businesses, technical experts, civil society, and governments. It follows a bottom-up process regarding policies affecting the underlying functioning of the internet domain system.[1263] Article 12 of the AfDEC principles also promote a multistakeholder form of internet governance.[1264]

Instead of focusing on the relationships between governments and how to improve mutual legal assistance processes, there should be a cross-cutting sector engagement with other stakeholders. After all, the private sector plays the most important role in assisting LEA in accessing electronic evidence. A dialogue should be open between all stakeholders on how to deal with cross border cloud data jurisdiction. Service providers have put in place terms of service and community guidelines which play a significant role in what type of information may be accessed by law enforcement. However, as chapter 2 illustrated, these terms differ from one service provider to the other. If a multi-stakeholder approach is adopted and all interested players are engaged in the discussion, perhaps better jurisdictional terms

[1257] Section 54 of the Cybercrimes Act.
[1258] Daskal op cit note 227 at 239.
[1259] Scassa and Currie op cit note 628 at 1080. Kohl op cit note 673 at 28.
[1260] Ibid.
[1261] Ibid.
[1262] Watney op cit note 919.
[1263] Stuart N Brotman 'Multistakeholder internet governance: A pathway completed, the road ahead' (2015) *Center for Technology Innovation at Brookings*.
[1264] 'Everyone has the right to participate in the governance on the internet. The internet should be governed in such a way as to uphold and expand human rights to the fullest extent possible. The internet governance framework must be open, inclusive, accountable, transparent and collaborative'. Article 12 of the African Declaration on Internet Rights and Freedoms.

of service may be drafted which balances the needs and rights of individuals, service providers, governments, civil society, and overall public interest.

a. Innovative Governance

Apart from addressing the issue of language as a mechanism to bring clarity on data jurisdictional principles, one should consider adopting innovative governance. Innovative governance is not territorial in nature, it is transnational. Innovative governance means 'developing standards for legal interoperability and policy coordination so that we are equipped with methods and tools that are as transnational, distributed, scalable and resilient as the internet itself'.[1265] One of the criticisms levelled against the Malabo Convention is the lack of interoperability and policy coherence across African countries as some remain without data protection laws or cybercrime and cybersecurity laws.[1266] Global service providers have been able to navigate the conflicting jurisdictional challenges by developing standard community guidelines and uniform terms of service. These guidelines have been developed after consideration of different laws in different states and harmonising such laws. Innovative governance means harmonisation of laws by different governments along the same lines as done by service providers. Of course, there are doubts that states can never reach such harmonisation considering the cultural, economic, societal, and religious differences between states.[1267]

V. CONCLUSION

This chapter's proposed solutions to the jurisdictional challenges associated with transborder cloud data should be considered for adoption by South Africa and other states. The advantage of these solutions is that they provide a uniform and collective approach to data jurisdiction. Any state can easily adopt some of these solutions without necessarily going through the long-winded bureaucratic processes of law-making. In addition, these solutions protect privacy interests, the sovereignty of states and allow the criminal justice system to prevail. The solutions are more pragmatic and can be implemented in the cybercriminal justice system.

The chapter has highlighted the importance of revising the existing legal frameworks in place such as mutual cooperation. The challenges with MLAT processes are mainly around time delays and long processes. The solution to these problems includes enhancing cooperation amongst states and providing an enabling legal framework for law enforcement agents across jurisdictions to exchange information. There is room for expedited processes by shortening the turnaround times for processing requests from foreign LEA. Service providers play an important role in criminal investigations. Viable solutions to data jurisdiction and the exercise of enforcement jurisdiction should include a framework

[1265] Svantesson op cit note 104 at 17.
[1266] Van der Berg op cit note 394 at 12.
[1267] Svantesson op cit note 104 at 62.

to engage service providers who may be in control or possession of the sought-after cloud evidence. The solutions discussed provide clearly defined procedures on how to involve the service providers. In addition, service providers should be part of decision-making processes or law-making process. Instead of focusing on the relationships between governments and how to improve mutual legal assistance processes, there should be a cross-cutting sector engagement with other stakeholders. Service providers already regulate large portions of the internet through their community guidelines and terms of service. Involving these stakeholders in decision-making will result in better solutions to data jurisdiction.

Non-legal solutions are a different, yet effective way to address cloud data jurisdiction. Instead of relying on national laws, international treaties and conventions, cloud data jurisdiction can be resolved through technical means. The internet infrastructure and cloud infrastructure can be designed in a way that provides easier interpretation of cloud data jurisdiction. In explaining the principle of 'code is law', this study has argued that it is possible for one state to have primary jurisdiction over cloud data by re-designing the infrastructure at the architectural level. If code is law, code can make cloud data features bound to a particular territory apart from the cloud data being hosted in a certain state. Software developers can develop code in such a way that the territoriality principle can be the default principle applicable to cloud data.

With the United Nations working on developing text on a cybercrime convention, it is hoped that these solutions should be considered in the ongoing discussions. It is hoped that this study provides support on how the anticipated UN cybercrime convention will address some of the legal challenges with establishing jurisdiction over cloud data.

CHAPTER 7: CONCLUSION

I. OVERVIEW

The birth of the internet brought with it a paradigm shift in not only how business is conducted but also in how crime is committed and investigated. With the rapid increase in use of technology came an exponential growth in the number of criminal activities relying on the internet and technology. At the inception of the internet, some people like John Perry Barlow wanted an internet that was not under the influence and control of government authority. Non-territorialists, as they are referred to in this study, argued that the internet had to be subject to its own set of rules and no government should have any say over internet-based interactions. Unfortunately, those who shared Barlow's views of an independent internet have been disappointed. Governments successfully found other ways of exerting authority over internet activities and the confidence of the internet exceptionalists has waned.[1268] In most cases, governments have established connection between cyber-activities to their territory and relied on such a connection to exercise authority.

With the emergence of cloud computing technologies and the increase in the amount of data processing, a new school of thought similar to non-territorialists also emerged. The scholars of this new school of thought argue for data exceptionalism – a concept that data are unique from other forms of property (including intangible property) and should be treated differently. Instead of relying on territorially based principles of jurisdiction, data exceptionalists argue that there are other compelling interests which should be considered, and territory should never be a determining factor. While data exceptionalism has gained momentum in academic circles, unfortunately state practice has continued to support data territoriality when dealing with the exercise of enforcement powers.

This study has demonstrated that there are other alternative solutions to resolve the jurisdictional challenge which by-passes territorially inclined attributes. These alternate solutions are not concerned about the territory where the data are located, where the crime was committed or where the suspect is located. One of the solutions considers factoring in core principles of substantial connection, legitimate interests and balancing of interests. If an investigating state can demonstrate a substantial connection between the crime and the state, its legitimate interests in the investigation as well as demonstrating a balance between its interests and those of a foreign state, the investigating state should be permitted to exercise jurisdiction. This approach to cloud jurisdiction helps us to stop thinking about data jurisdiction in terms of territory or thinking about reformulating territorially based jurisdictional principles. In applying these solutions, lawmakers should be mindful to use the correct

[1268] Lessig op cit note 1245 at ix.

terminology and judges and magistrates should also make sure that the correct terminology is adopted when handing court judgements.

Complimenting these measures is the need for improvements on mutual cooperation between states and cooperation between LEA and cybersecurity experts. This solution is not new but can complement these solutions particularly in cases where states do not adopt the same data jurisdiction principles. The framework set out in the Cybercrime Convention and the 2nd Additional Protocol is effective to relieve the pressure on the current mutual assistance system. By making it easier for member states to obtain subscriber information directly from a service provider without having to request for permission from another member state is a useful solution to fast-track cybercrime investigations. Cybersecurity experts have the relevant skillset which can complement investigations and the gathering of electronic evidence.

This study has also demonstrated that apart from legal solutions, there are other non-legal solutions which, if adopted, can effectively address the cloud data jurisdictional dilemma. The primary solution is recognising that code is law which means that code and the internet infrastructure can shape how, where and who can have jurisdiction over cloud data. Governments are already using code to regulate different areas such as internet access, freedom of speech and expression, right to privacy and data protection. If code is law, it can make cloud data features bound to a particular territory apart from the cloud data being hosted in a specific state.

II. DID THE STUDY PROVE THE HYPOTHESIS?

At the commencement of this research project, the hypothesis was that the advancement in technology warrant a reconceptualisation or re-evaluation of jurisdictional principles in the context of extraterritorial enforcement jurisdiction. The hypothesis was premised on the argument presented by data exceptionalists and non-territorialists. The understanding was that since cybercrimes are committed not in a physical pinpointed location on a map but in cyberspace, the territoriality principle has no relevance in determining what LEA can and cannot do. The emergence of cloud computing technologies has resulted in a lot of data relevant for criminal investigations being stored on cloud servers. The unique features of data further justify the need to depart from the territoriality principle in the context of accessing cross border cloud evidence. The ability of cloud data to be stored in multiple jurisdictions simultaneously and being accessible from multiple jurisdictions presented different challenges to LEA. The first challenge is that territorial jurisdiction may result in a state with less interests in the data exercising primary jurisdiction over the data. The second challenge being that multiple states with access to cloud data may exercise jurisdiction over the cloud data resulting in conflict of laws.

If traditional jurisdictional principles are exercised over cloud data, there is a grave danger that criminals will remain unprosecuted as states may clash over who has jurisdiction over the crime or the evidence to prove the crime. The hypothesis was that when investigating crimes committed in cyberspace or evidence stored in cyberspace, the principles of jurisdiction must be reformed. Without reforming the jurisdictional principles, some criminals will slip through the jurisdictional loopholes and go unprosecuted. Without adequate jurisdictional principles to govern conduct in cyberspace and clarity on jurisdiction of data in the cloud, the powers of law enforcement agencies are limited.

To give a fair and balanced assessment of the hypothesis, the study investigated the legal challenges that cloud computing technologies and cloud data present to law enforcement agents. The study found that the unique features of data means that territory should not be the primary basis to exercise enforcement jurisdiction. This is because the territory where the cloud data are hosted may not have any normative interest in the data and the location of data in that territory may be fortuitous. The study also found that there is lack of legal and policy coordination at an international level which makes it difficult for cybercrimes to be investigated and for relevant evidence to be secured. Lack of coordination could be because of lack of laws which adequately address cybercrimes and clearly set out the procedural processes for investigating cybercrimes. Lack of legal interoperability is also because of differences in national laws which makes it difficult for different governments to cooperate. The study found that governments are resorting to unilateral actions in seizing cloud data as international frameworks have failed to provide comprehensive solutions to challenges with cross border cloud data. The study also found that the relaxed approach to update antiquated criminal laws created legal uncertainty on the prosecution of certain conduct as well as on gathering of relevant electronic evidence. This uncertainty transcends into negatively impacting criminal procedural processes and investigations. With cloud data potentially being located on foreign territory, LEA are not able to ascertain whether their powers to conduct searches and seizures extend to cloud data.

Part of the study was to understand what amounts to cybercrime, the different types of cybercrime and more importantly, criminal conduct taking place in the cloud. An analysis of cybercrimes was important for this study as it signified the role of the cloud in storing data which may constitute electronic evidence relevant to a criminal investigation. It was also important to demonstrate how cybercrimes differ from traditional crimes and why the hypothesis is justified. The analysis of the different types of cybercrimes, the different laws applicable to permit LEA to investigate cybercrimes and the discussion on legal gaps in cybercrime law was very pertinent to the overall objective of this study.

Both discussions on cloud computing technologies and cybercrimes were important in showing the challenges that LEA face when investigating crime and seeking to access relevant electronic evidence. The discussions explained the extensive nature of the internet and cloud computing and the

legal challenges in accessing transnational data in criminal investigations. This study examined three seemingly independent themes of cloud computing law, cybercrime law and law of jurisdiction. The study contextualised the three themes and demonstrated their interconnectedness and role in understanding the concerns around access to transnational data in criminal investigations.

The study discussed the different challenges that cloud computing technologies present to criminal investigations, particularly cybercrime investigations. The major challenge that was addressed throughout the study were the jurisdictional challenges that cybercrime investigators experience when intending to access transnational data. The study demonstrated the different jurisdictional principles which may be applicable to remote cloud data. It pointed out the concerns and limitations of the various jurisdictional principles to cloud data. Some of the limitations that were identified in this study relate to lack of international cooperation when states are seeking access to remote cloud data. Such a broken international system justifies the need for a reformulation of jurisdictional principles as proposed by the hypothesis.

An important part of the research objective was to consider South Africa's regulatory universe on cybercrime and determine if it is necessary to have new laws to deal with the challenges identified in this study. An extensive evaluation of the relevant legislation in South Africa was carried out. The study found that South Africa's cybercrimes law does not have very clear rules on the extent to which LEA can access remote cloud data. The study noted that in most instances, LEA exercise discretion to access transnational data using remote tactics. There are no prohibitions in terms of the law, to prohibit LEA from unilaterally accessing remote cloud data. The study found that this is mainly because the Cybercrimes Act does not clarify on what amounts to jurisdiction in the context of cloud data.

After discussing the law on cybercrime, the law on cloud computing, the law on jurisdiction and the approaches to jurisdiction over cross border cloud data, the study found that there are compelling reasons to justify the need to develop new jurisdictional principles. This was the hypothesis of this study. The study discussed the different cloud data approaches in detail but pointed out that data location and territoriality principles remain the basis for exercising jurisdiction. What is clear is that territorially based principles to jurisdiction are not easy to replace. Despite the calls for revisiting the jurisdictional principles applicable to data and possibly reformulating most suitable principles, states have remained adamant to sink their claws over data when the data infrastructure is located within their territories. This has perpetrated the increase in adoption of data localisation measures as states understand that territoriality plays a significantly important role in cloud data jurisdiction.

After a comprehensive and exhaustive research on the views of territorialists, there is cynicism about the relevance of adopting new jurisdictional principles. Due to differences in domestic laws and policies, political agendas, and economic strategies, it is pellucid that states are not going to agree on

the same jurisdictional principles to apply to cloud data. An analysis of the international digital policy framework indicates that territory is still a relevant basis for states to exercise jurisdiction. This could be because of the importance for states to preserve state sovereignty in the digital era. While it is important for academics to contribute to knowledge by identifying solutions to address the gaps in legal systems, this study acts as a reminder that academic solutions should not be provided in a void. Solutions should consider the existing or prevailing social, economic, and political circumstances. Pragmatic solutions are the ones which consider political developments and public policy considerations. The study has shown that states still heavily rely on territorially based principles. This makes solutions by territorialists to be more viable and likely to be adopted by states when addressing the issue of cloud data jurisdiction. Scholarly discourse in favor of this approach stands greater chances of impacting policy-making, decision-making and rule-making.

The study noted that the views expressed by Woods, Svantesson, and the drafters of the Tallinn Manual can change the legal discourse on data jurisdiction. While data exceptionalists like Daskal have made compelling arguments on data jurisdiction, it is unfortunate that their views are less likely to manifest in most legal instruments. Notwithstanding, this study does not mean that academic writings and critical thinking should always align with public policy developments and existing laws and policies. To make that conclusion will defy the purpose of legal research and critical thinking and writing. The study concludes that in the face of two conflicting camps on jurisdiction between data exceptionalism and data territoriality, this study sides with the later.

However, it should be clarified that the study supports data territorialism within the premise of the *lex lata* on jurisdiction. The current legal framework in South Africa on criminal procedure and criminal jurisdiction is based on the traditional principles of jurisdiction. This would mean that where data jurisdiction is in dispute, the applicable law will focus more on territory. The study submits that any principles which support data exceptionalism and the new framework to data jurisdiction as coined by Svantesson is only viable if cybercrime laws do not overtly rely on territorial jurisdiction. For example, the wording of section 24 of the Cybercrimes Act on jurisdiction evidently points to the territory of the Republic. To re-iterate the arguments presented in this study, a reformulation of distinct jurisdictional principles ideal for cyberspace and internet governance can only be possible if the underlying legislative instruments do not focus on territorial jurisdiction.

III. CONCLUDING REMARKS

As work on the drafting of a UN treaty on cybercrime is underway, it is imperative that the treaty clearly addresses the problem of transborder access to cloud data and appropriately establish reasonable jurisdictional principles. The proposed UN treaty should also ensure that it addresses the technological advancements and developments of this century as well as leave room for regulation of future emerging

technologies. We live in a world where there are constant technological changes. Our laws have and will likely continue to play ‘catch-up’ with technological developments. Currently, there is an increase in the adoption and use of artificial intelligence in everyday life, commerce, e-government, including in court systems. There is great potential in adopting and using artificial intelligence in combatting and fighting cybercrime. The future of cybercrime investigations and prosecutions will include the admissibility of evidence generated by artificial intelligence. The future of cybercrime also includes the weaponization of artificial intelligence to commit crime as well as considerations of whether artificial intelligence can be viewed as legal persons or statutory agents. It is imperative that legal issues of enforcement jurisdiction are clearly defined in the face of new.

BIBLIOGRAPHY

Conventions

1. African Charter on the Rights and Welfare of the Child 1990
2. African Union on Cyber Security and Data Protection Convention 2014
3. African Union Agenda 2063 the Digital Transformation Strategy for Africa 2020
4. African Union Data Policy Framework 2022
5. Council of Europe Budapest Convention
6. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS 108 of 1981
7. Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States
8. Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence
9. Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties
10. Council Framework Decision 2006/783/JHA on the application of the principle of mutual recognition to confiscation orders
11. Countering the use of information and communications technologies for criminal purposes. Resolution adopted by the General Assembly 26 May 2021 A/RES/75/282
12. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters
13. European Union Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matter 2008/977/JHA of 27 November 2009 [2008] OJ L 350/60
14. Establishment of Harmonised Policies for the ICT Market in the ACP Countries: Data Protection: Southern African Development Community Model Law 2013
15. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018
16. Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Directive 95/46/EC of the European Parliament and the Council of 24 October 1995
17. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD)
18. SADC Model Law Cybercrime
19. SADC Protocol on Mutual Legal Assistance in Criminal Matters 2002
20. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS 2010

21. The Rome Statute of the International Criminal Court
22. Universal Declaration on Human Rights
23. UN Charter
24. United Nations Convention against Transnational Organised Crime and the Protocols thereto

Acts

25. Cybercrimes Act 19 of 2020
26. Criminal Procedure Act 51 of 1977
27. Critical Infrastructure Protection Act 8 of 2019
28. Electronic Communications and Transactions Act 25 of 2002
29. Electronic Communications Act 36 of 2002
30. Extradition Act 67 of 1962
31. Films and Publications Act 65 of 1996
32. Financial Intelligence Centre Act 38 of 2001
33. International Cooperation in Criminal Matters Act 75 of 1996
34. Magistrate's Court Act 32 of 1944
35. National Prosecuting Authority Act 32 of 1998
36. State Information Technology Act 88 of 1998
37. South African Police Services Act 68 of 1995
38. Prevention of Organised Crime Act 121 of 1998
39. Protection of Personal Information Act 4 of 2013
40. Promotion of Access to Information Act 2 of 2000
41. Prevention and Combating of Hate Crimes and Hate Speech B9-2018 GG 41543 29 March 2018
42. Public Finance Management Act, 56 of 2003.
43. The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Regulations, delegated legislation and government notices

44. Digital Industrial Revolution. National e-Strategy Digital Society South Africa GN 887 GG 41242 of 10 November 2017
45. Draft Standard Operating Procedures for the Investigation, Search, Access or Seizure of Articles in terms of section 26 of the Cybercrimes Act, 19 of 2020. Government Gazette 47021 GN2292 15 July 2022
46. National e-Government Strategy and Roadmap GN 886 in GG 41241 of 10 November 2017.
47. National e-Strategy Digital Society South Africa GN 887 in GG 41242 of 10 November 2017

48. The Presidential Commission on the Fourth Industrial Revolution- The Department of Telecommunications and Postal Services GN 209 GG 42388 of 9 April 2019

Policy Documents

49. Draft National Data and Cloud Policy GN306 GG 44389 of 1 April 2021
50. National Cybersecurity Policy Framework 2015
51. State Information Technology Agency 'Digital Transformation 2020 – 2024 Strategic Plan'
52. SITA Annual Report 2018/2019
53. National Development Plan 2030 – Our future, make it work
54. National Integrated ICT Policy White Paper 2016
55. South Africa Connect: Creating opportunities, ensuring inclusion – South Africa's Broadband Policy 2013
56. South African Reserve Bank 'Cloud computing and the offshoring of data' Directive D3/2018
57. South African Reserve Bank 'Outsourcing of functions within banks' Guidance Note 5/2014

South African Case law

58. *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2019] 4 All SA 343 (GP).
59. *Carolissen v Director of Public Prosecutions* [2016] 3 All SA 56 (WCC).
60. *Grammaticus (Pty) Ltd v Minister of Police & Others* (unreported, GP case no 8694/17, 22 March 2017).
61. *Goqwana v Minister of Safety and Security NO & others* 2016 (1) SACR 384 (SCA).
62. *Harvey v Niland & Others* 2016 (2) SA 436 (ECG).
63. *Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd* 2006 4 SA 458 (SCA).
64. *Heaney v S* 2016 ZAGPPHC 257 (19 April 2016).
65. *Jafta v Ezemvelo KZN Wildlife* (Case D204/07).
66. *Magajane v Chairperson, North West Gambling Board* 2006 (2) SACR 447 (CC).
67. *Mandela and Others v Minister of Safety and Security and Another* 1995 (2) SACR 397 (W).
68. *Masiya v Director of Public Prosecution* 2007 2 SACR 435 [CC].
69. *Minister of Justice & Others v Desai NO* 1948 (3) SA 395 (A)).
70. *Minister of Safety and Security and Others v Bennett and Others* (302/06) [2007] ZASCA 139.
71. *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).
72. *National Commissioner of South African Police Service v Southern African Human Rights Litigation Centre & Others* 2014 ZACC 30.
73. *Ntoyakhe v Minister of Safety and Security* 2000 1 SA 257.
74. *Ruskopoint (Pty) Ltd t/a The Old Mill Gaming Centre v The Minister of SAPS NO & others* (unreported, ECG case no 1427/2016, 8 September 2016).

75. *Savoi and Others v National Director of Public Prosecutions and Another* (8006/12) [2013] ZAKZPHC 19.
76. *S v Dersley* 1997 (2) SACR 253 (Ck).
77. *S v Harper* 1981 (1) SA 88 (D).
78. *S v Heaney* (unreported, GP case no A464/2015, 19 April 2016 at 15).
79. *S v Motata* (Johannesburg District Court case number 63/968/07).
80. *S v Ndiki and Others* 2008 SACR 252.
81. *Toich v Magistrate, Riversdale & Other* 2007 (2) SACR 235 (C).
82. *Page & Others v Additional Magistrate, Somerset West & Others* 2016 3 All SA 619 (WCC).
83. *Podbielski Mhlambi Incorporated v Fourie: Landdroshof Welkom and Others (Podbielski Mhlambi Incorporated v Fourie: Landdroshof Welkom and Others)* [2009] ZAFSHC 26 (12 March 2009).
84. *Powell NO and Others v Van der Merwe and Others* (503/2002) [2004] ZASCA 25; [2005] 1 All SA 149 (SCA) (1 April 2004).
85. *R v Douvenga* District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003 (unreported case).
86. *S v Miller & Others* [2015] 4 All SA 503 (WCC).
87. *S v Myeni* 2019 (1) SACR 360 (ECG).
88. *Van Rooyen & Another v Minister of Police & Others* 2019 (1) SACR 349 (NCK).

Foreign case law

89. *Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain);* Second Phase, International Court of Justice (ICJ), 5 February 1970.
90. *Belgium v Yahoo!* Case No. Nr. P.13.2082.N.
91. *Democratic Republic of Congo v. Belgium 2002 I.C.J. 3 (Feb. 14)* Arrest Warrant of 11 April 2000.
92. *Dow Jones and Company Inc v Gutnick* [2002] HCA 56; 210 CLR 575; 194 ALR 433;77 ALJR 255 (10 December 2002).
93. *France v Turkey* (1927) P.C.I.J Reports, Series A, No.10.
94. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12.
95. *Google v CNIL* Case C-507/17.
96. *Moors v Burke* (1919) 26 CLR 265 (High Court of Australia).
97. *Oxford v Moss* [1978] 68 Cr App Rep 183.
98. *R v Waddon* [2000] WL491456 (No 99/5233/Z3 CA).

99. *Roofmart Ontario Inc. v. Canada (National Revenue)* 2008 FCA 348, [2010] 1 F.C.R. 145 (Can.C.A).
100. *Riley v California* 573 US (2014).
101. *R v Daniels [2004] NLSCTD 27 Supreme Court of Newfoundland and Labrador*.
102. *R v Land [1999] QB 65.*
103. *R v Owen [1988] 1 WLR 134.*
104. *R v Perrin [2002] EWCA Crim 747*
105. *R v Sharpe [2001] S.C.R. 45 Supreme Court of Canada.*
106. *R v Stanley [1965] 2 QB 327.*
107. *R v Toben (2000) Urt v 12.12.2000 – StR 184/00, reported in 54 (8) NJW (20001).*
108. *Skype Communications Sàrl v Belgian Institute of Postal Services and Telecommunications* Case C-142/18.
109. *The United States of America v The Netherlands* Permanent Court of Arbitration Case number 1925-01.
110. *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme* (LICRA) 433 F.3d 1199 [9th Cir. 2006].
111. *United States v Ivanov No.* 300CR00183AWT. 2001.
112. *US v Hockings* 129 F.3d 1069 (9th Cir.,1997).
113. *U.S. v Romm* 455 F.3d 990 (9th Cir., 2006).
114. *Zippo Manufacturing co. v Zippo Dot com, Inc.* 952 F.Supp. 1119.

Foreign legislation

115. Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks. Federal Law Np. 242 FZ (Russia)
116. Computer Fraud and Abuse Act 1986 (US)
117. Clarifying Lawful Overseas Use of Data Act (H.R. 4943) 2018 (US)
118. Data Protection Act 3 of 2021 (Zambia)
119. Data Protection Act 24 of 2019 (Kenya)
120. Electronic Communications Privacy Act of 1986 (codified as amended at 18 U.S.C. 2701-12, 3121 – 27) (US)
121. General Personal Data Protection Law (Brazil)
122. Stored Communications Act 18 U.S.C. § 2701 (US)
123. United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development (2020).
124. 1 Law No. 13.709 of 14 August 2018 as amended by Law No. 13.853 of 8 July 2019. Brazil's General Personal Data Protection law (LGPD.).

Books

125. Abraha, H Halefom 'Government access to digital evidence across borders: Some lessons for Africa' in KM Yilma (ed), The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties (Addis Ababa University Press, 2020) 1.
126. Ball, K. and Webster, F. (2003). The intensification of surveillance. In: Ball, K. and Webster, F. eds. The Intensification of Surveillance: crime, terrorism and warfare in the information era. London: Pluto Press.
127. Broadhurst, Roderic and Alazab, Mamoun 'Spam and crime' in Peter Drahos Regulatory Theory: Foundations and Applications (Australian University Press, 2017).
128. Broadhurst, Roderic and Bacon-Shone, John and Bouhours, Brigitte and Bouhours, Thierry and Kingwa, Lee 'Reporting Crime Victimisation and Satisfaction with Police Response' in Business and the Risk of Crime in China (Australian University Press, 2011).
129. Catteddu, Daniele Cloud computing: benefits, risks and recommendations for information security in Serrao C., Aguilera Diaz V., Cerullo F (eds) Web Application Security IBWAS 2009 Communications in Computer and Information Science vol 72, Springer, Berlin, Heldelberg.
130. Cerase, Andrea and Santoro, Claudia 'From racial hoaxes to media hypes fake news' real consequences' in Peter Vasterman From Media Hype to Twitter Storm (Amsterdam University Press, 2018).
131. Chang, Y.C. Lennon and Grabowsky, Peter 'The governance of cyberspace' in Drahos, P. (ed) Regulatory Theory: Foundations and Applications, Canberra: ANU Press (2017).
132. Clough, Jonathan Principles of Cybercrime 2 ed (Cambridge University Press, 2015).
133. Currie, Iain and De Waal, Johan The Bill of Rights Handbook 6 ed (2013)
134. Dugard, John International Law: A South African Perspective 2 ed (2003).
135. Dugard, John Dugard's International Law: A South African Perspective (2018) 5ed.
136. Fuchs, Christian 'Karl Marx in the age of big data capitalism' in Chander, David and Fuchs, Christian Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data (2019).
137. Goredema, Charles and Zoppei, Verena 'South Africa: Analyses of a Global Challenge to Democracy' in Stiftung, Boll Heinrich and Schonenberg, Regine Transnational Organized Crime: Analyses of a Global Challenge to Democracy (2013).
138. Goldsmith, Jack and Wu, Tim 'Who controls the internet? Illusions of borderless world' Oxford University Press 2006.
139. Harris, DJ Cases and Materials of International Law (2004) 6 ed.
140. Hollywood, S. John and Woods, Dulani and Silberglitt, Richard and Jackson, A. Brian 'Using Future Internet Technologies to Strengthen Criminal Justice' (2015).

141. Hon W Kuan, and Millard, Christopher ‘Cloud technologies and services’ in Christopher Millard (ed.) Cloud Computing Law (Oxford: Oxford University Press, 2013a).
142. Internet & Jurisdiction Policy Network Data and Jurisdiction Program: Operational Approaches, Norms, Criteria and Mechanisms (2019).
143. Kastner, Phillip and Megret, Frederic ‘International legal dimensions of cybercrime’ in Research Handbook on International Law and Cyberspace (Nikolas Tsagourias & Russell Buchan eds) 2015).
144. Kulesza, Joanna International Internet Law (2013).
145. Lessig, Lawrence Code and Other Laws of Cyberspace 1999.
146. Lessig, Lawrence ‘Code: Version 2.0.’ (2006) 2 ed.
147. Lynn, Theo and Mooney, G. John and Van der Werff, Lisa and Fox, Grace ‘Data privacy and trust in cloud computing’ (2020) 6 ed.
148. Mangan, E. David and Giles, G. Lorna The legal challenges of Social Media: Elgar Law, Technology and Society (2017).
149. Michael N Schmitt ‘Tallinn Manual 2.0. on the international law applicable to cyber operations’ 2017.
150. McConville, Mike and Chui, Wing Hong Research Methods for Law 2nd edition Edinburgh University Press.
151. Murray, D Andrew ‘Mapping the rule of law for the internet’ in David Mangan and Lorna E Gillies The Legal Challenges of Social Media (2017).
152. Murray, Andrew Information Technology Law: The Law and Society (2009).
153. Papadopoulos, Sylvia and Snail, Sizwe Cyberlaw @ SA IV: The law of the internet in South Africa 4 ed (2021).
154. Papadopoulos, Sylvia and Snail, Sizwe Cyberlaw @SAIII: The law of the internet in South Africa 3 ed (2012).
155. Polanski Paul Przemyslaw The internationalization of internet law in Klabbers, Jan and Sellers, Mortimer The Internationalization of Law and Legal Education 2008 Springer.
156. Porcedda, Grazia Maria ‘Law enforcement in the clouds: Is the EU Data protection framework up to the task?’ Chapter 10 in S. Gutwirth et al (eds) European Data Protection: In Good Health? (2012).
157. Porsche, R. Isaac and Sollinger, M. Jerry and McKay, Shawn A Cyberworm that Knows no Boundaries (2011).
158. Post G David ‘The challenges of cyberlaw’ in Sean A Pager and Adam Candeub Transitional Culture in The Internet Age (2012).
159. Probst, W. Christian and Sasse, M. Angela and Pieters, Wolter and Dimkov, Trajce and Luysterborg, Erik and Arnaud, Michel ‘Privacy penetration testing: How to establish trust in

your cloud provider' in Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (eds) European Data Protection: In Good Health? Springer, Dordrecht. https://doi.org/10.1007/978-94-007-2903-2_12.

160. Romanosky, Sasha and Libicki, C. Martin and Winkelman, Zev and Tkacheva, Olesya Why internet freedom tools? in Internet Freedom Software and Illicit Activity (2015).
161. Schroeder, Ralph Social Theory after the Internet: Media, Technology and Globalisation (2018).
162. Snail, Sizwe Cybercrimes and Cybersecurity Bill: What you need to know: Reflecting the law as at 16 March 2018 (2018).
163. Snyman, CR 'Criminal Law' 5 (ed) 2008.
164. Snipp, C Matthew 'What does data sovereignty imply: What does it look like? In Tahu Kukutai and John Taylor 'Indigenous data sovereignty' Australian National University.
165. Svantesson, Jerker B. Dan Internet & Jurisdiction: Global Status Report 2019 Internet & Jurisdiction Policy Network.
166. Taylor, Max and Quayle, Ethel Child Pornography: An Internet Crime 2003.
167. United Nations Office on Drugs and Crime: Comprehensive study on (Report, February 2013) 1 (Comprehensive Study on Cybercrime).
168. Uta Kohl Jurisdiction and the internet. Cedric Ryngaert Jurisdiction in international law 2 edition Oxford Monographs in International Law 2015.
169. Van der Merwe, Dana Computers and the Law 2ed (2000).
170. Van der Merwe, Commentary on the Criminal Procedure Act (Du Toit) (1987).
171. Walden, Ian 'Accessing data in the cloud: The long arm of the law enforcement agent' in Pearson Siani & Yee George Privacy and Security Cloud Computing (2013) 45.
172. Wall, David 'The internet as a conduit for criminal activity; (2005) 15 in Pattavina, A (ed) Information Technology and the criminal justice system' Thousand Oakes, CA: Sage 77.
173. Wall, S David 'Mapping out cybercrimes in a cyberspatial surveillant assemblage. The intensification of surveillance: crime terrorism and warfare in the information age in Webster, F. and Ball, K., eds., London: Pluto Press, 2003.
174. Watney, Murdoch 'Cybercrime and the investigation of cybercrime' in Papadopoulos S & Snail S Cyberlaw @SAIII: The law of the internet in South Africa 3 ed.

Journals

175. Ablon, Lillian and Libicki, Martin 'Hacker's bazaar: The markets for cybercime tools and stolen data' (2015) Defense Counsel Journal 143.
176. A.D. Abubakar; Bass, M Julian and Allison Ian 'Cloud computing: Adoption issues for Sub-Saharan African SMEs' (2014) 62 EJISDC 1.

177. Bailey, Rishab and Parsheera, Smriti 'Data localisation in India: Questioning the means and ends' (2018) 242 National Institute of Public Finance and Policy.
178. Balboni, Paolo and Pelino, Enrico 'Law enforcement agencies' activities in the cloud environment: A European legal perspective' (2013) 22 *Information & Communications Technology Law* 165.
179. Bana, Anurag and Hertzog, David 'Data security and the legal profession: Risks, Unique Challenges and Practical Considerations' (2015) 16 *Business Law International* 247.
180. Bank, James 'European Regulation of cross border hate speech in cyberspace: The limits of legislation' (2011) 19 *European Journal of Crime, Criminal Law and Criminal Justice* 1.
181. Bannon, Adrian 'Cybercrime investigation and prosecution – Should Ireland ratify the Cybercrime Convention' (2007) 3 *Galway Student Law Review* 115.
182. Baptiste, Jean Maillart 'The limits of subjective territorial jurisdiction in the context of cybercrime' (2019) 19 ERA Forum 375.
183. Barlow, John Perry Declaration of the Independence of Cyberspace.
184. Barmin, Yury and Jones, Grace and Moiseeva, Sonya and Winkelman, Zev 'International arms control and law enforcement in the information revolution: An examination of cyber warfare and information security' (2011) 10 *Connections published by Partnership for Peace Consortium of Defense Academies and Security Studies Institutes* 73.
185. Basdeo, Vinesh 'The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' (2012) SACJ 195.
186. Basdeo, Vinesh 'Criminal and procedural legal challenges of identity theft in the cyber and information age' (2017) 30 South African Journal on Criminal Justice 363.
187. Beale, Sun Sara and Berris, Peter 'Hacking the internet of things: Vulnerabilities, dangers and legal responses' (2017-2018) 16 *Duke Law & Technology Review* 161.
188. Bellia, L Patricia 'Chasing bits across borders' (2001) University of Chicago Legal Forum 35.
189. Benish, D. Kevin 'Whose law governs your data: Takedown orders and territoriality in comparative perspective' (2019) 55 Willamette Law Review 599.
190. Berge, Jean-Sylvestre 'The Datasphere as a new paradigm for relationship between territories in law' (2017) 7 Brazilian Journal of Public Policy III.
191. Benton, Diana 'Seeking warrants for unknown locations: The mismatch between digital pegs and territorial holes' (2018) 68 *Emory Law Journal* 183.
192. Bitensky, H. Susan 'Introductory note to Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse' (2010) 49 *International Legal Materials* 1663.

193. Blakesley, L. Christopher and Stigall, Dan 'Wings for talons: The case for the extraterritorial jurisdiction over sexual exploitation of children through cyberspace' (2004) Wayne Law Review 109.
194. Borghard, J. Erica and Lonergan, W. Shawn 'Confidence Building Measures for the Cyber Domain' (2018) 12 *Strategic Studies Quarterly* 10.
195. Bouwer, Gideon Petrus 'Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) SACJ 156.
196. Buono, Laviero 'Investigating and prosecuting crimes in cyberspace: European training schemes for judges and prosecutors' (2010) ERA Forum 207.
197. Buono, Laviero 'The genesis of the European Union's new proposed legal instrument (s) on e-evidence: Towards the EU Production and Preservation Orders' (2019) ERA Forum 307.
198. Buono, Laviero 'Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches' (2016) ERA Forum 343.
199. Bradshaw, Simon; Millard, Christopher and Walden, Ian 'Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services' (2011) International Journal of Law and Information Technology 187.
200. Brannon, Ike and Schwartz, Hart 'The new perils of data localisation rules' (2018) Regulation 41.
201. Brehmer, H Jacqueline 'Data localisation: the unintended consequences of privacy litigation' (2018) 67 American University Law Review 927.
202. Brenner, W Susan 'Fantasy crime: The role of criminal law in virtual worlds' (2008) 11 Vanderbilt Journal of Entertainment and Technology Law 1.
203. Brenner, W Susan and Koops, Bert-Jaap 'Approaches to cybercrime jurisdiction' (2004) 4 Journal of High Technology Law 1.
204. Brenner, W. Susan and Schwerha IV, J. Joseph 'Cybercrime Havens' (2008) 25 *The Computer & Internet Lawyer* 19.
205. Brenner, W Susan 'Is there such a thing as "virtual crime"?' (2001) 4 California Criminal Law Review 1.
206. Brenner, W Susan 'At light speed: Attribution and response to cybercrime / terrorism / warfare' (2007) 97 The Journal of Criminal Law & Criminology 379.
207. Brenner, W Susan 'Law in an era of pervasive technology' (2006) 15 Widener Law Journal 667.
208. Brenner, W. Susan 'Internet law in the courts' (2010) Journal of Internet Law 30.
209. Brenner, W. Susan 'Human and Humans+: Technological enhancement and criminal responsibility' (2013) 19 *Boston University Journal of Science and Technology Law* 215.

210. Brenner, W. Susan and Clarke, L. Leo 'Civilians in cyberwarfare: Conscripts' (2010) 43 *Vanderbilt Journal of Transnational Law* 1011.
211. Brenner, W. Susan and Clarke, L. Leo 'Should commercial misuse of private data be a crime?' Available at SSRN: https://ssrn.com/abstract=845845 or http://dx.doi.org/10.2139/ssrn.845845.
212. Brenner, W. Susan and Clarke, L. Leo 'Civilians in cyberwarfare: Casualties' (2010) 13 *Science and Technology Law Review* 249.
213. Brenner, W. Susan 'Nanocrime' (2011) 39 *University of Illinois Journal of Law, Technology Policy* 39.
214. Brenner, W. Susan and Clarke, L. Leo 'Fourth Amendment protection for shared privacy rights in stored transactional data' (2005) 14 *Journal of Law* 211.
215. Brenner, W. Susan 'Cybercrime jurisdiction' (2006) 46 *Crime, Law, Social Change* 189.
216. Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve; and Da, Chen 'Crime in cyberspace: Offenders and the role of organised crime groups' 2013 Australian National University Cybercrime Observatory Working Paper 1.
217. Brotman, N Stuart 'Multistakeholder internet governance: A pathway completed, the road ahead' (2015) *Center for Technology Innovation at Brookings*.
218. Brown, Steven David 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2019) ERA Forum.
219. Buys, Reinhardt 'Love Hurts' 2000 De Rebus 33.
220. Cachalia Firoz and Klaaren Jonathan 'Digitalisation, the 'Fourth Industrial Revolution' and the Constitutional law of privacy in South Africa: Towards a public law perspective on constitutional privacy in the era of digitalisation' (2021) 14 Digital Pathways Oxford Paper Series 1.
221. Cai, Tianji and Du, Li and Xin, Yanyu and Chang, Y.C. Lennon 'Characteristics of cybercrimes: evidence from Chinese judgement documents' (2018) Police Practice and Research 582.
222. Calcara, Giulio 'Rethinking legal research on matters of international police cooperation: Issues, methods and raison d'tre' (2019) 40 *Liverpool Law Review* 95.
223. Cassim, Fawzia 'Formulating adequate legislation to address cyber-bullying: Has the law kept pace with advancing technology?' (2013) SACJ 1
224. Cassim, Fawzia 'Addressing the spectre of phishing: Are adequate measures in place to protect victims of phishing' (2014) 47 Comparative & International Law Journal of Southern Africa 401.

225. Cassim, Fawzia 'Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players' (2011) 44 Comparative International Law Journal of South Africa 123.
226. Cassim, Fawzia 'Addressing the challenges posed by cybercrime: A South African perspective' (2010) 5 *Journal of International Commercial Law and Technology* 118.
227. Cassim, Fawzia 'Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study' (2009) 12 Potchefstroom Electronic Law Journal 36.
228. Cassim, Fawzia 'Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?' 2015 (18) *Potchefstroom Electronic Law Journal* 69.
229. Celestine, M Carol 'Cloudy skies, bright futures: In defense of a private regulatory scheme for policing cloud computing' (2013) University of Illinois Journal of Law, Technology & Policy 141.
230. Chaudhari, Nehaa and Prasad, Krishna Smitha 'Carpenter v United States: State Surveillance and Citizen Privacy" (2019) 13 *NALSAR Student Law Review* 129.
231. Chandarman, Rajesh and & Brett van Nierkerk, Brett 'Students' cybersecurity awareness at a private tertiary educational institution' 2017 The African Journal of Information and Communication 133.
232. Chander, Anupam 'Is data localization a solution for Schrems II?' (2020) 23 Journal of International Economic Law 771.
233. Chander, Anupam and Le, P. Uyen 'Data Nationalism' (2015) 64 Emory Law Journal 677.
234. Chawki Mohammed and Okike Uzor Ezekiel 'Fighting cybercrime: Issues for the future' (2009) African Journal of Crime and Criminal Justice 1.
235. Chawki Mohamed, Darwish Ashraf, Khan Ayoub Mohammad and Tyagi Sapna Cybercrime, Digital Forensics and Jurisdiction 2015 Springer International Publishing 1.
236. Chen, Jiahong "Data localisation law and policy: The EU Data Protection International Transfers Restriction through a cloud computing lens" (2020) 17 SCRIPTed: A Journal of Law, Technology and Society 152 .
237. Chimuka Andrea Tarisayi and Mashumba-Paki Lesedi 'Understanding cyber scams: An assessment of the challenges of law enforcement in Botswana' 2016 Journal of Sustainable Development in Africa 111.
238. Cohen, Bret and Hall, Britanie and Wood, Charlie 'Data localization laws and their impact on privacy, data security and the global economy' (2017) 32 Antitrust 107.
239. Cong, Wanshu 'China's 2015 Counterterrorism Law' (2016) 11 Journal of Comparative Law 381.

240. Corn, P Gary and Taylor, Robert 'Sovereignty in the age of cyber' (2017 – 2018) 111 AJIL – UNBOUND 207.
241. Clopton, D. Zachary 'Data institutionalism: A reply to Andrew Woods' (2016 -2017) 69 Stanford Law Review Online 9.
242. Clough, Jonathan 'Cybercrime' (2011) 37 Commonwealth Law Bulletin 671.
243. Clough, Jonathan 'The Council of Europe Convention on Cybercrime: Defining 'Crime' in a digital world' (2012) 13 Criminal Law Forum 363.
244. Clough, Jonathan 'Cybercrime' (2011) 37 Commonwealth Law Bulletin 671.
245. Clough, Jonathan 'A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation' Monash University Law Review 698.
246. Clough, Jonathan 'Data theft? Cybercrime and the increasing criminalization of access to data' (2011) 22 Criminal Law Forum 145.
247. Clough, Jonathan 'Now you see it, now you don't: Digital images and the meaning of 'possession' (2008) Criminal Law Forum 205.
248. Currie, J Robert 'Cross border evidence gathering in transitional criminal investigation: Is the Microsoft Ireland case the next frontier?' (2016) 54 Canadian Yearbook of International Law 63.
249. Daskal, Jennifer 'Access to data across borders: The critical role for Congress to play now' (2017) Advance: The Journal of the ACS Issue Briefs 45.
250. Daskal, Jennifer 'Privacy and security across borders' (2018-2019) 128 Yale Law Journal Forum 1029.
251. Daskal, Jennifer 'Transnational government hacking' (2020) Journal of National Security Law and Policy 677.
252. Daskal, Jennifer 'Borders and Bits' (2018) 71 Vanderbilt Law Review 179.
253. Daskal, Jennifer 'The un-territoriality of data' (2015) The Yale Law Journal 125.
254. Daskal, Jennifer 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0.' (2018-2019) 71 Stanford Law Review Online 9.
255. Dauterman, Walter C Jnr 'Internet Regulation: Foreign Actors and Local Harms – at the Crossroads of Pornography, Hate Speech and Freedom of Expression' (2002) 28 North Carolina Journal of International Law and Commercial Regulation 177.
256. Daultrey Sally 'Cybercrime: Invisible problems, imperfect solutions' 2017 https://dx.doi.org/10.2139/ssrn.3803735.
257. De Caria, Riccardo 'Old is sometimes better: The case for using existing law to face the challenges of the digital age' (2019) 4 Cambridge Law Review 68.

258. Decroos, J.L. Matthieu ‘Criminal jurisdiction over transnational speech offences – from unilateralism to the application of foreign public law by the national courts’ (2005) 3 *European Journal of Crime, Criminal Law and Criminal Justice* 365.
259. De Hert, Paul and Kopcheva, Monika ‘International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! Case’ (2011) 27 *Computer Law & Security Review* 291.
260. Didenko, Anton ‘Regulating fintech: Lessons from Africa’ (2018) 19 San Diego International Law Journal 311.
261. Dove, S. Edward and McMillian, Catriona ‘Looking back, looking forward’ (2016) 13 SCRIPTed: Journal of Law, Technology and Society 232.
262. Efremov, A.A. ‘Formation of the concept of information sovereignty of the state’ (2017) Journal of the Higher School of Economics 201.
263. Eichesehr, E Kristen ‘Data extraterritoriality’ (2017) 95 Texas Law Review 145.
264. Farinpour, Ramin ‘The evolving face of European criminal justice in an ever-changing world’ (2016) 17 ERA Forum 279.
265. Fehr, Caroline and LiCalzi, Christine and Oates, Thomas ‘Çomputer Crimes’ (2016) 53 *American Criminal Law Review: Annual Survey of White Collar Crime* 977.
266. Flanagan, Anne ‘The law and computer crime: Reading the script of reform’ (2005) 13 *International Journal of Law and Information Technology* 98.
267. Flint, David ‘Law shaping technology: Technology shaping the law’ (2009) 23 *International Review of Law, Computers & Technology* 5.
268. Fraser, Erica ‘Data localisation and the balkanisation of the internet” (2016) SCRIPTed: A Journal of Law, Technology and Society 359.
269. Garrie, Daniel and Byhovsky, Irene ‘Privacy and data protection in Russia’ (2017) Journal of Law & Cyber Warfare 235.
270. Gasson, N Mark and Koops Bert-Jaap ‘Attacking Human Implants: A New Generation of Cybercrime’ (2013) 5 Law, Innovation & Technology 248.
271. Geldenhuys, Kotie ‘Bilateral tools for fighting transnational organised crime’ 2019 Servamus 32.
272. Gercke, Marco ‘Europe’s legal approaches to cybercrime’ (2009) 10 ERA Forum 409.
273. Gillespie, A. Alisdair and Samantha Magor, Samantha ‘Tackling online fraud’ (2019) ERA Forum
274. Gillespie, A. Alisdair ‘Child pornography’ (2018) 27 Information and Communications Technology Law 30.
275. Gillespie, A. Alisdair “Jurisdictional issues concerning online child pornography” (2012) 20 International Journal of Law and Information Technology 151.

276. Girgenti, Elkin ‘Computer crimes’ (2018) 4 *American Criminal Law Review – Annual Survey of White Collar Crime* 911.
277. Ghappour, Ahmed ‘Searching places unknown: Law enforcement jurisdiction on the dark web’ (2017) 69 Stanford Law Review 1075.
278. Ghappour, Ahmed ‘Tallinn, Hacking, and Customary International Law’ (2017-2018) 111 *AJIL Unbound* 224.
279. Gleeson, Niamh and Walden, Ian ‘Placing the state in the cloud: Issues of data governance and public procurement’ (2016) 32 Computer Law & Security Review 683.
280. Godoy, Jaoa ‘Computers and international criminal law: High-tech crimes and criminals’ (2000) 6 *New England International and Comparative Law Annual* 95.
281. Goldsmith, Jack ‘Sovereign difference and sovereign deference on the internet’ (2018-2019) 128 Yale Law Journal Forum 818.
282. Goicovici, Juanita ‘Provisions regarding the Consumers’ rights in Cloud Computing Service Agreements’ (2019) 2 *Romanian Review of Private Law* 399.
283. Goodman, D Marc and Brenner, W Susan ‘The emerging consensus on criminal conduct in cyberspace’ (2002) 10 *International Journal of Law and Information Technology* 139.
284. Goodwin, Morag Embracing the Challenge: Legal Scholarship in a Global Era' (2013) 4 *Transnational Legal Theory* 686.
285. Goodwin, Morag What I Talk about When I Talk about Global Law (2012) 17 *Tilburg Law Review* 269.
286. Grabosky, Peter ‘Requirements of prosecution services to deal with cyber crime’ (2007) 47 *Crime, Law, Society and Change* 201.
287. Gray, Anthony ‘Conflict of laws and the cloud’ (2013) 29 *Computer Law & Security Review* 58.
288. Greene, Hillary and Cooper, James and Ghappour, Ahmed and Lieber, David and Wu, Felix Data Collection and the Regulatory State (2017) 49 *Connecticut Law Review* 1733.
289. GSMA ‘The state of mobile internet connectivity 2022’ GSMA Report 2022.
290. Hache, C.B. Ana and Ryder, Nicholas ‘Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the web lurking to scam shoppers this Christmas: A critical analysis of the United Kingdom’s legislative provisions and policies to tackle online fraud’ (2011) 20 *Information & Communications Technology Law* 35.
291. Han, Wang Sarah and Munir, Abu Bakar ‘Information Security Technology – Personal Information Security Specification: China’s Version of the GDPR’ (2018) 4 European Data Protection Law Review 535.

292. Helberger, Natali; Borgesius Frederik Zuiderveen and Reyna Agustin 'The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54 Common Market Law Review 1309.
293. Henry, Shawn and Brantly, F. Aaron 'Countering the Cyber Threat' (2018) 3 *The Cyber Defense Review* 47.
294. Hildebrandt, Mireille 'Extraterritorial jurisdiction to enforce in cyberspace: Bodin, Schimitt, Grotius' (2013) 63 University of Toronto Law Journal 196.
295. Hildebrandt, Mireille and Koops, Bert-Jaap 'The challenges of ambient law and legal protection in the profiling era (2010) 73 Modern Law Review 428.
296. Hofmeyer, Jan, Wolf, Ndeapo Wolf and Cloete, Deon 'SADC Futures of digital geopolitics: Towards African digital sovereignty' Southern African Institute of International Affairs Occasional Paper 337.
297. Hon, W Kuan; Millard, Christopher and Walden, Ian 'The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing' (2011) International Data Privacy Law 211.
298. Hon, W Kuan; Millard, Christopher; Singh, Jatinder and Walden, Ian 'Policy, legal and regulatory implications of a Europe-Only cloud' (2016) 24 *International Journal of Law and Information Technology* 251.
299. Hon, W. Kuan and Millard, Christopher and Walden, Ian 'Negotiating cloud contracts: looking at clouds from both sides now (2012) 16 *Stanford Technology Law Review* 79.
300. Hooper, Christopher and Martini, Ben and Choo, Raymond Kim-Kwang 'Cloud Computing and Its Implications for Cybercrime Investigations in Australia' (2013) Computer Law & Security Rev 152.
301. Howell, C Jordan; Burruss, W George; Maimon, David and Sahani, Shradha 'Website defacement and routine activities: considering the importance of hackers' valuations of potential targets' (2019) *Journal of Crime and Justice* 1.
302. Huang, Jeanne Jie, 'Personal jurisdiction based on the location of a server: Chinese territorialism in the internet era? (2016) 36 *Wisconsin International Law Journal* 87.
303. Hunt, John 'The new frontier of money laundering: how terrorist organisations use cyberlaundering to fund their activities, and how governments are trying to stop them' (2011) 20 Information & Communications Technology Law 133.
304. Hurwitz, Roger 'Depleted Trust in the Cyber Commons' (2012) 6 *Strategic Studies Quarterly* 20.
305. Hussain, Shakir Wisam and Ibrahim, Jalel Nebras 'A survey of cybercrimes, investigations and penal laws imposed on the criminals' (2019) *International Journal of Computer Science and Mobile Computing* 131.

306. Jamil, Zahid ‘Global fight against cybercrime: undoing the paralysis’ (2012) *Georgetown Journal of International Affairs, International Engagement on Cyber* 109.
307. Jiow Jhee Hee ‘Cyber crime in Singapore: An analysis of regulation based on Lessig’s four modalities of constraint’ 2013 International Journal of Cyber Criminology 1.
308. Johnson, R David and Post, David Laws and Borders – The Rise of Law in Cyberspace (1996) 48 *Stanford Law Review* 1367.
309. Johnson, Maureen and Rogers, M. Kevin ‘The Fraud Act 2006: The e-crime prosecutor’s champion or the creator of a new inchoate offence?’ (2007) 21 *International Review of Law Computers and Technology* 295.
310. Jong-Chen, Jing de ‘Data sovereignty, cybersecurity, and challenges for globalization’ (2015) 16 *Georgetown Journal of International Affairs* 112.
311. Judy, L. Henry and Satola, David ‘Business interests under attack in cyberspace: Is international regulation the right response?’ (2011) *Business Law Today* 1.
312. Kadlecova Lucie ‘Russian-speaking cyber crime: Reasons behind its success’ 2015 The European Review of Organised Crime 104.
313. Kahvedzic, Damir ‘Cybercrime investigations of mobile phone devices and the cloud in the light of EU safe harbour rulings’ (2016) ERA Forum 355.
314. Kang, Robert ‘Lessons from Hollywood cybercrimes: Combatting online predators’ (2018) 7 Berkeley Journal of Entertainment and Sports Law 1.
315. Kesan, Jay P and Bashir, N Masooda ‘Privacy in the cloud: Going beyond the contractarian paradigm’ 1.
316. Kempen, Annalise ‘Digital forensic evidence and investigations’ (2021) 114 Servanus Community-based Safety and Security Magazine 38.
317. Kilovaty, Ido ‘Freedom to hack’ (2019) 80 *Ohio State Law Journal* 455.
318. Kirkpatrick, Keith ‘Borders in the cloud’ (2018) 61 Communications of the ACM 19.
319. Klumpp, Jordan A ‘International impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations’ (2020) 48 *Georgia Journal of International and Comparative Law* 613.
320. Leenes, Ronald and Koops, Bert-Jaap ‘Code: Privacy's death or saviour’ (2005) 19 *International Review Law, Computers and Technology* 329.
321. Koops, Bert-Jaap ‘Technology and the crime society: Rethinking legal protection’ (2009) 93 *Law, Innovation & Technology* 93.
322. Koops, Bert-Jaap and Leenes, Ronald ‘Code and the slow erosion of privacy’ (2005) 12 *Michigan Telecommunications & Technology Law Review* 115.

323. Koops, Bert-Jaap and Prinsen, M. Merel 'Houses of glass, transparent bodies: How new technologies affect inviolability of the home and bodily integrity in the Dutch Constitution' (2007) 16 *Information & Communication Technology Law* 177.

324. Koops, Bert-Jaap and Newell Clayton Bryce and Skorvanek, Ivan 'Location tracking by police: The regulation of tireless and absolute surveillance (2019) 9 *UC Irvine Law Review* 635.

325. Koops, Bert-Jaap 'Criminal law and cyberspace as a challenge for legal research' (2012) *SCRIPTed Journal of Law, Technology and Society* 354.

326. Kulesza Joanna 'New technologies and the need of a uniform legal system' 2007 https://dx.doi.org/10.2139/ssrn.1446768 accessed 12 October 2022.

327. Kuner, Christopher 'Data nationalism and its discontents' (2014-2015) 64 *Emory Law Journal Online* 2089.

328. Kumar, K. Satish 'Data localization bane for digital economic growth!' (2019) 49 International In-House Counsel Journal 1.

329. Kramer, Franklin and Markoff, Michelle and Butler, Robert and Lewis, James and Fei, Gao and Klimburg, Alexander 'National and global strategies for managing cyberspace and security' (2011) *Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity* 75.

330. Kremer, Jens 'Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace' (2014) 23 *Information & Communications Technology Law* 220.

331. Lachmayer Konrad and Witzleb Normann 'The challenge to privacy from ever increasing state surivellance: A comparative perspective' (2014) *UNSW Law Journal* 748.

332. Levy, EC Karen 'Book-smart, not street-smart: Blockchain-based smart contracts and the social workings of law' (2017) 3 Engaging Science, Technology, and Society 1.

333. Leukfeldt, Rutger Eric and Notte, R.J. Raoul and Malshc, M. Marijke 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes' (2019) Victims & Offenders: An international journal of evidence based research, policy and practice.

334. Laubscher, M and Van Vollenhoven, WJ 'Cyberbullying: Should schools choose between safety and privacy?' (2015) PER /PELJ 2219.

335. Li, Xiaofeng 'A dangerous game: China's big data advantage and how the US should respond' (2020) University of Illinois Journal of Law, Technology and Policy 253.

336. Lips, Miriam and Koops, Bert-Jaap 'Who regulates and manages the internet infrastructure? Democratic and legal risks in shadow global governance' 2005 (10) *Information Policy* 117.

337. Lochner, Hennie; Benson, Bernadine and Horne, Juanida 'Making the invisible visible: the presentation of electronic (cell phone) evidence as real evidence in a court of law' (2012) Acta Criminologica: African Journal of Criminology & Victimology 69.

338. Lloyd, Chris ‘The crime of sexting: a deconstructive approach’ (2018) Information & Communications Technology Law 55.
339. Mabunda, Sagwadi ‘Is it cyberfraud or good ol’offline fraud: A look at section 8 of the South African Cybercrimes Bill’ (2018) 2 *Journal of Anti-Corruption Law* 58.
340. Macagno, Fabrizio ‘Definition in law’ (2010) *Swiss Bulletin of Applied Linguistics* 197.
341. Mason, Stephen ‘Electronic evidence: dealing with encrypted data and understanding software, logic and proof’ (2014) 15 *ERA Forum Journal of the Academy of European Law* 25.
342. Makulilo B Alex ‘Myth and reality of harmonisation of data privacy policies in Africa’ (2015) *Computer Law & Security Review* 78.
343. Matania, Eviatar and Yoffe, Lior and Mashkautsan, Michael ‘A three-layer framework for a comprehensive national cyber-security strategy’ (2016) 17 *Georgetown Journal of International Affairs* 77.
344. McGruer, Jonathan ‘Emerging privacy legislation in the international landscape: Strategy and analysis for compliance’ (2020) 15 *Washington Journal of Law, Technology & Arts* 120.
345. McKenna, Matthew ‘Up in the cloud: Finding common ground in providing for law enforcement access to data held by cloud computing service providers’ (2016) 49 *Vanderbilt Journal of Transnational Law* 1417.
346. Mills, Alex ‘Rethinking Jurisdiction in International Law’ (2014) 81 (1) *BYBIL* 187.
347. Mishra, Neha ’Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows’ (2019) 52 *Vanderbilt Journal of Transnational Law* 463.
348. Mothibi, Kholofelo and Amali, Ewaoda Sadiq ‘Curbing cybercrime at institutions of higher learning: A case study of the information communication technology unit (ICT) at selected South African Universities’ (2018) Acta Criminologica: Southern African Journal of Criminology: Special Edition: Cybercrime 57.
349. Molokomme, Athaliah ‘Combating cybercrime in Botswana’ (2011) 13 *University of Botswana Law Journal* 55.
350. Movsisyan, Sona ‘Human trafficking in a digital age: Who should be held accountable?’ (2019) 27 Michigan State International Law Review 539.
351. Musoni, Melody ‘Is cyber search and seizure under the Cybercrimes and Cybersecurity Bill consistent with the Protection of Personal Information Act?’ (2016) 3 *Obiter Law Journal* 683.
352. Musoni, Melody ‘The criminalisation of “Revenge Porn” in South Africa’ 2019 *Obiter Law Journal* 61.
353. Muswaka, L ‘Unauthorised adaptation of computer programmes – is criminalisation a solution?’
354. Mueller, Milton ‘Will the internet fragment? Sovereignty, globalisation and cyberspace’ (2017) 42.

355. Nel, Sanette 'Problematic issues surrounding transborder cybersmear' (2010) 22 SA Merc LJ 360.

356. Nodeland, Brooke and Belshaw, Scott and Saber, Mark 'Teaching cybersecurity to criminal justice majors' (2019) Journal of Criminal Justice Education 71.

357. Njotini, Niven Mzukisi 'Anti-terrorism measures in South Africa: Suspicious transaction reporting and human rights'(2015) 15 African Human Rights Law Journal 515.

358. Nycyk Michael Computer hackers and hacking: Exploring those lurking behind the screen 2018 Michael Nycyk 1.

359. Nortje, GJ Jacobus and Myburgh, C Daniel 'The search and seizure of digital evidence by forensic investigators in South Africa' (2019) 22 *PER / PELJ* 1.

360. O'Brien Mark 'Clear and present danger? Law and the regulation of the internet' (2005) 14 *Information and Communications Technology Law* 151.

361. Odumesi, Olayemi John 'Combatting the menace of cybercrime' (2014) 3 *International Journal of Computer Science and Mobile Computing* 980.

362. O'Keeffe, Vincent 'Jurisdictional issues associated with a move to the cloud'

363. Olinger H.N. et al 'Western privacy and / or ubuntu? Some critical comments on the influences in the forthcoming data protection in South Africa' (2007) *The International Information & Library Review*.

364. Orji, Uchenna Jerome 'Regionalising data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act' (2017) *International Data Privacy Law* 179.

365. Orlova, V Alexandra 'Digital sovereignty, anonymity and freedom of expression: Russia's fight to reshape internet governance' (2020) UC Davis Journal of International Law & Policy 225.

366. Osula, Anna Maria 'Remote search and seizure in domestic criminal procedure: Estonian case study' (2016) 24 *International Journal of Law and Information Technology* 343.

367. Onuora, A.C, Uche, D.C, Ogbunude F.O., and Uwazuruike F.O., 'The challenges of cybercrime in Nigeria: An overview' (2017) *AIPFU Journal of School of Sciences* 1.

368. Panc, Daniela 'Considerations on sovereignty in cyberspace' (2015) International Conference Education and Creativity for a Knowledge-Based Society 279.

369. Payne, K Brian 'White collar cybercrime: White collar crime, cybercrime or both' (2018) 19 *Criminology, Criminal Justice, Law & Society* 16.

370. Pecoraro, Andrew 'Drawing lines in the cloud: Implications of extraterritorial limits to the Stored Communications Act' (2017) 51 *Creghton Law Review* 75.

371. Pell, K. Stephanie and Soghoian, Christopher 'Can you see me now: Toward reasonable standards for law enforcement access to location data that congress could enact'(2012) 27 Berkeley Technology Law Journal 117.

372. Perry, Barbara and Olsson, Patrick 'Cyberhate the globalisation of hate' (2009) 18 *Information & Communications Technology Law* 185.

373. Pinguelo, M Fernando and Muller, W Bradford 'Virtual crimes, real damages: A primer on cybercrimes in the United States and efforts to combat cybercriminals' (2011) 16 *Virginia Journal of Law and Technology* 116.

374. Pinto, Avila Renata 'Digital sovereignty or digital colonialism' (2018) 27 Sur-International Journal on Human Rights 15.

375. Porcedda, Grazia Maria 'Lessons from PRISM and Tempora: The self-contradictory nature of the fight against cyberspace crimes. Deep packet inspection as a case study'(2013) 25 *Neue Kriminalpolitik* 373.

376. Podgor, S. Ellen and Filler, M. Daniell 'International criminal jurisdiction in the 21st century: Rediscovering United States v Bowman' (2007) San Diego Law Review 585.

377. Porwal, Sakshi; Nair K Srijith; and Dimitrakos Theo Regulatory impact of data protection and privacy in the cloud (2011) Wakeman et al (Eds) IFIPTM, IFIP AICT 290.

378. Pradillo Carlos Ortiz Juan 'Fighting against cybercrime in Europe: The admissibility of remote searches in Spain' 2011 European Journal of Crime, Criminal Law and Criminal Justice 363.

379. Rachavelias, G Michail 'Online financial crimes and fraud committed with electronic means of payment – a general approach and case studies in Greece' (2019) 19 *ERA Forum* 339.

380. Rajesh, S; Reddy, Shylender and Kumar, T Pavan 'Security threats in cloud computing' (2012) *GJCAT* 1043.

381. Rastogi, Ishan; Chandra Adesh; Gupta Kumar Vivek and Vaish Abhishek 'Privacy issues and measurement in cloud computing: A review' (2013) *International Journal of Advanced Research in Computer Science* 81.

382. Robison, Jeremy William 'Free at what cost: Cloud computing privacy under the Stored Communications Act' (2010) 98 *Georgetown Law Journal* 1195.

383. Roscini, Marco 'Gravity in the statute of the international criminal court and cyber conduct that constitutes, instigates or facilitates international crimes' (2019) Criminal Law Forum 247.

384. Rubinstein, S. Ira and Bilyana Petkova, Bilyana 'Governing privacy in the datafied city' (2020) 47 Fordham Urban Law Journal 755.

385. Samuli Haataja, Samuli 'The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach' (2017) Law, Innovation and Technology (2) 159.

386. Sauer, Rich 'Achieving trust and compliance in the cloud' (2016) 9 *International in-House Counsel Journal* 1.

387. Saulawa, A. Mu'azu and Abubakar, M.K. 'Cybercrime in Nigeria: An overview of Cybercrime Act 2013' (2014) 32 Journal of Law, Policy and Globalization 23.

388. Selby, John ‘Data localization laws - Trade barriers or legitimate response to cybersecurity risks, or both’ (2017) 25 *International Journal of Law and Information Technology* 213.

389. Segall, Sasha ‘Jurisdictional challenges in the United States government’s move to cloud computing technology' (2012) Fordham Intellectual Property, Media & Entertainment Law Journal 1105.

390. Scassa, Teresa and Currie, J Robert ‘New first principles – assessing the internet’s challenges to jurisdiction’ (2011) 42 Georgetown Journal of International Law 1017.

391. Schomburg, Wolfgang ‘Criminal matters: transnational ne bis in idem in Europe – conflict of jurisdictions – transfer of proceedings’ (2012) ERA Forum 311.

392. Shah, Reema ‘Law enforcement and data privacy – a forward looking approach’ (2015) 125 *Yale Law Review Journal* 543.

393. Singh, Jatinder; Bacon, Jean; Crowcroft, Jon; Madhavapeddy, Anil; Pasquier, Thomas; Hon W Kuan and Millard, Christopher ‘Regional Clouds: Technical Considerations’ (2014) *Computer Laboratory, University of Cambridge Technical Report* 863.

394. Snail, Sizwe ‘Cybercrime in the context of the ECT Act’ 2008 *JBL* 63.

395. Snail, Sizwe ‘Cyber crime in South Africa – hacking, cracking, and other unlawful online activities’ (2009) Journal of Information Law & Technology 1.

396. Snail, Sizwe and Madziwa, Simbarashe ‘Hacking, cracking, and other unlawful online activities’ (2007) Without Prejudice 32.

397. Snail, Sizwe and Madziwa, Simbarashe ‘Hacking, cracking and other unlawful online activities’ (2008) Without Prejudice 30.

398. Snail, Lindelo Ka Mtuze and Matanzima, Siya ‘Cyber security in Africa’ (2014) Without Prejudice 88.

399. Snail ka Mtuze, Sizwe ‘The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013’ (2022) *Obiter Law Journal* 536.

400. Softness, Nicole ‘Terrorist communications: Are Facebook, Twitter, and Google responsible for the Islamic State’s Actions?’ (2016) 70 *Journal of International Affairs* 202.

401. Stancu, Luliana Adriana ‘Evolution of the international regulations regarding cybercrime’

402. Stanescu, Lorena Elena and Onufreiciuc, Raluca ‘Some reflections on ‘datafication’: Data governance and legal challenges’ (2020) 7 European Journal of Law and Public Administration 100.

403. Subashini, S and Kavitha, V ‘A survey on security issues in service delivery models of cloud computing’ (2010) *Journal of Network and Computer Applications* 1.

404. Schjolberg, Stein and Ghernaouti-Helie, Solange A global protocol on cybersecurity and cybercrime 2009 Cybercrimedata.

405. Schaengold, Zachary 'Personal jurisdiction over offenses committed in virtual worlds'(2012) 81 University of Cincinnati Law Review 361.
406. Sullivan, Clare 'Is identity theft really theft?' (2009) 23 *International Review of Law, Computers & Technology* 77.
407. Swales, Lee 'An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: suggestions for reform – part one' (2018) 21 *Potchefstroom Electronic Law Journal* 1.
408. Swire, Peter and Kennedy-Mayo, Debrae 'How both the EU and the U.S. are stricter than each other for privacy of government requests for information' (2017) 66 *Emory Law Journal* 617.
409. Taslitz, E. Andrew 'Cybersurveillance without restraint: The meaning and social value of the probable cause and reasonable suspicion standards in governmental access to third party electronic records' (2013) 103 *Journal of Criminal Law and Criminology* 839.
410. Terblanche, SS and Mollema, N 'Child pornography in South Africa' 2011 SACJ 283.
411. 'The private-sector ecosystem of user data in the digital age' (2019) 29 *Fordham Intellectual Property, Media & Entertainment Law Journal* 1099.
412. Tikk-Ringas, Eneken 'The implications of mandates in international cyber affairs' (2012) *Georgetown Journal of International Affairs* 41.
413. Tsosie, Rebecca 'Tribal data governance and informational privacy: Constructing indigenous data sovereignty' (2019) 80 *Montana Law Review* 229.
414. Tropina, Tatiana 'The nexus of information technologies and illicit financial flows: phenomenon and legal challenges' (2016) 17 *ERA Forum* 369.
415. Theophilopoulos, C 'The admissibility of data, data messages, and electronic documents at trial' (2015) *Journal of South African Law* 461.
416. Trautman, Lawrence 'Virtual currencies: Bitcoin and what now after liberty reserve, silk road and Mt Gox?' (2014) 20 *Richmond Journal of Law and Technology* 1.
417. Tubic, Bojana and Radojcic, Stefan 'Jurisdictional problems in international law' (2017) *Romanian Journal of Comparative Law* 200.
418. Urbas, Gregory 'Cybercrime, jurisdiction and extradition: The extended reach of cross border law enforcement' (2012) 16 Journal of Internet Law 8.
419. Vaciago, Giuseppe 'Remote forensics and cloud computing: An Italian and European Legal Overview' (2011) 8 *Digital Evidence and Electronic Signature Law Review* 124.
420. Valdes, Roma Antonio 'The mutual recognition principle in criminal matters: A review' (2015) ERA Forum 291.
421. Van Jaarsveld, Izelde 'Following the money across cyber highways: A herculean task or international challenge? Some thoughts on money laundering on the internet' 2004 *SA Merc LJ* 685.

422. Van Nierkerk, Brett 'The cybersecurity dilemma: Considerations for investigations in the dark web' (2018) Acta Criminologica: Southern African Journal of Criminology 132.
423. Vertes-Olteanu, Andrea 'Evolution of the criminal legal frameworks for preventing and combating cybercrime'(2014) 1 Journal of Eastern European Criminal Law 84.
424. Waheeda, Fathimath 'Legislating for cybercrimes in the Maldives: Challenges and prospects'(2015) 23 IIUM Law Journal 415.
425. Walden, Ian and Flanagan, Anne 'Honeypots: A sticky legal landscape' (2003) 29 *Rutgers Computer Technology Law Journal* 317.
426. Walden, Ian 'EDI: Contracting for legal security' (1992) 6 *International Yearbook of Law Computers and Technology* 23.
427. Walden, Ian 'Forensic investigations in cyberspace for civil proceedings (2004) 18 *International Review of Law, Computers & Technology* 275.
428. Walden, Ian 'Harmonising Computer Crime Laws in Europe' (2004) 12 *European Journal of Crime Criminal Law and Criminal Justice* 321.
429. Walden, Ian 'Anonymising personal data' (2002) 10 *International Journal of Law and Information Technology* 224.
430. Wall, S David 'Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime' (2008) 22 *International Review of Law Computers and Technology* 45.
431. Wall, S. David 'Policing cybercrimes: Situating the public police in networks of security within cyberspace' (2010) 8 *Police Practice & Research: An International Journal* 183.
432. Wall, S. David 'Towards a conceptualisation of cloud (cyber) crime'(2017) T.Tryfonas (Ed.) Human Aspects of Information Security, Privacy and Trust, New York Springer International 529.
433. Wang, Anqi 'Cyber sovereignty at its boldest: A Chinese perspective' (2020) 16 *Ohio State Technology Law Journal* 395.
434. Wanglai, Gao 'BRICS Cybersecurity cooperation achievements and deepening paths' (2018) 68 *China International Studies* 124.
435. Watney Murdoch 'The evolution of legal regulation of the internet to address terrorism and other crimes' (2007) *TSAR* 494.
436. Watney, Murdoch 'The criminal and procedural means of combating cybercrime (part 1)' 2003 *TSAR* 56.
437. Watney, Murdoch 'The way forward in addressing cybercrime regulation on a global level' (2012) 1 *Journal of Internet Technology and Secured Transactions* 61.
438. Watney, Murdoch 'Analysing different approaches to cross border electronic evidence data sharing in criminal matters' (2019) 14th International Conference on Cyber Warfare and Security (ICCWS2019) 484.

439. Wei, Chen Chia 'Sketching the margins of a borderless world' (2018) 30 Singapore Academy of Law Journal 833.
440. Weistein, M. Jason and Drake, L. William and Silverman, P. Nicholas 'Privacy vs Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era' (2015) 52 *American Criminal Law Review – Annual Survey of White Collar Crime* 729.
441. Weinstein, Stuart and Wild, Charles 'Lawrence Lessig's 'Bleak House': A critique of 'Free Culture: How big media uses technology and the law to lock down culture and control creativity' or 'How I learned to stop worrying and love internet law' (2005) 19 *International Review of Law Computers* 363.
442. Westmoreland, Kate and Kent, Gail 'International law enforcement access to user data: A survival guide and call for action' (2018) *Canadian Journal of Law and Technology* 225.
443. Wong, W.S. Mary 'Cyber-trespass and 'unauthorised access' as legal mechanisms of access control: Lessons from the US Experience' (2006) 15 *International Journal of Law and Information Technology* 90.
444. Woods, Andrew Keanu 'Against Data Exceptionalism' (2016) 68 *Stanford Law Review* 729.
445. Woods, Andrew Keanu 'Litigating data sovereignty' (2018) 128 *Yale Law Journal* 328.
446. Yakovleva, Svetlana and Irion, Kristina 'The best of both worlds – free trade in services and EU law on privacy and data protection' (2016) 2 *European Data Protection Law Review* 191.
447. Yar Majid 'Online crime' 2016 Oxford Research Encyclopedia of Criminology
448. Yilma Micheal Kinfe and Abraha Hailu Halefom 'The internet and regulatory responses in Ethiopia: Telecoms, cybercrimes, privacy, e-commerce and the new media' 2015 Mizan Law Review 108.
449. Yilma, Kinfe Micheal 'Developments in cybercrime law and practice in Ethiopia' (2014) *Computer Law & Security Review* 720.
450. Zheng, Weiwei 'Comparative study on the legal regulation of a cross border flow of personal data and its inspiration to China' (2020) 15 *Frontiers of Law in China* 280.
451. Zimba, Aaron and Chishimba, Mumbi 'On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems' (2019) 4 *European Journal for Security Research* 3.
452. Zaidy AL Ahmed 'Digital crimes and our society' 2022 Academia Letters Article 4884 https://doi.org/10.20935/AL4884.

Newspapers

453. '336: Trumping Schrems II' Lexology 2 November 2020.
454. Bierman, Ben 'Small business and the 4IR cyber-threats' 15 July 2018 Sunday Independent 21.
455. Dayimani, Malibongwe; Maliti, Soyiso and Quintal, Genevieve 'SA now hostage to cyber ransom' Sunday Dispatch 26 October 2019.
456. 'EU-US Privacy Shield invalid: Schrems II' Lexology 26 August 2020.

457. ‘EU personal data transmission guarantees have universal application: Schrems v Facebook’ Lexology 29 September 2020.
458. Gallagher, Ryan and Burkhardt, Paul ‘Death kitty ransomware linked to South African port attack’ 29 July 2021 Bloomberg.
459. Gauteng banks lead in countering cybercrime’ 30 November 2018 Pretoria News 16.
460. GSMA ‘The state of mobile internet connectivity 2022’.
461. GSMA ‘The state of mobile internet connectivity 2019’.
462. Israeli Privacy Regulator publishes position paper on Israeli implications of Schrems II 30 September 2020.
463. Keenan, Ted ‘Cybercrime hits property market’ 6 November 2018 Daily Dispatch 8.
464. Kenneth Propp and Peter Swire ‘After Schrems II: A proposal to meet the individual redress challenge’ Lawfare 13 August 2020.
465. Musoni, Melody ‘South Africa’s “smart cities” and cybersecurity’ iAfrikan News 27 July 2019.
466. Moyo, Admire ‘City of Johannesburg hit by cyber attack’ IT Web 25 October 2019.
467. Siphumelele Khumalo ‘SA has 3rd highest rate of cybercrime in world’ 31 January 2018 Cape Times.
468. Snide, Mike and Molina, Brett ‘Everyone wants to own the metaverse including Facebook and Microsoft. But what exactly is it?’ USA Today 10 November 2021.
469. Ngqakamba, Sesona ‘Justice department IT system brought down in ransomware attack’ News24, 9 September 2021.
470. ‘Schrems II: Implications for data transfers from the GCC’ Lexology 15 July 2020.
471. ‘Schrems II Lawful Cloud Processing’ Webinar Anonos 29 October 2020.
472. Segal, Edward ‘A crisis is averted after Amazon’s Alexa tells child about lethal viral challenge’ 28 December 2021 Forbes News.
473. Smillie Shaun ‘Hackers hold city, banks to ‘ransom’’ Saturday Star 26 October 2019.
474. Swire, Peter and Daskal, Jennifer ‘What the CLOUD Act means for privacy pros’ (2018) IAPP Blog 26 March 2018.
475. Taddese, Yamri ‘Focus: Cloud Services Create Challenges fore-discovery’ Law Times 7 December 2015.
476. ‘The crime and punishment of DDoS attacks’ Business World 17 December 2018.
477. ‘US responds to Schrems II judgment’ Lexolody 1 October 2020.
478. Zodidi, Danc ‘Cybercrime to be added to police statistics’13 September 2018 Cape Argus 3.

Conference proceedings, policy papers and theses

479. Bauer, Matthias and Lee-Makiyama, Hosuk and Van Der Marel, Erik and Verschelde, Bert ‘The costs of data localisation: Friendly fire on economic recovery’ 2014 European Centre for International Political Economy Occasional Paper No 3/2014.

480. Beyleveld, Alexander 'Data protection in Kenya, Nigeria and South Africa in the 2020s and beyond' 2021 Mandela Institute Policy Brief 1.
481. Burwell, Frances G and Propp, Kenneth 'The European Union and the search for digital sovereignty: Building "Fortress Europe" or preparing for a new world' (2020) Atlantic Council.
482. Burrows, Matthew and Mueller-Kaler, Julian 'Smart partnerships amid great power competition: AI, China, and the global quest for digital sovereignty' Atlantic Council.
483. Dalton, Wayne; Van Vuuren, Joey Jansen and Westcott Justin 'Building cybersecurity resilience in Africa' (2017) 12th International Conference on Cyber Warfare and Security 112.
484. European Parliament 'Fighting cyber crime and protecting privacy in the cloud' 2012 Policy Department C: Citizens' Rights and Constitutional Affairs.
485. Ferracane, Martina 'South Africa: Options to regulate data flows' (2018) Global Economic Governance Policy Briefing.
486. Flaig, Dorothee; Lopez-Gonzalez, Javier; Messent, James and Jouanjean, Marie-Agnez 'Modelling data localisation measures' 2016 19th Annual Conference on Global Economic Analysis 1.
487. Gebers, J and Ophoff J 'Exploring cloud computing legal and privacy issues in South Africa' 2013 15th Annual Conference on World Wide Web Applications, Cape Town.
488. Goldsmith, Jack The Internet and the Legitimacy of Remote Cross Border Searches (Chicago Public Law and Legal Theory Working Paper, Issue 16, 2001) 1.
489. Gillwald, Allison and Moyo Mpho 'The cloud over Africa' 2013 Research ICT Africa Policy Paper prepared for the United Nations Conference on Trade and Development Information Economy Report 2013.
490. Gillwald, Allison and Moyo, Mpho 'Modernising the Public Sector through the Cloud: A report commissioned by the Microsoft Foundation' 2016.
491. Guinchard, Audrey 'Criminal law in the 21st century: The demise of territoriality?' 2007 Notes for the Critical Legal Conference on Walls, 16 September 2007, Birkberk.
492. Hlomani, Hanani and Ncube, B. Caroline 'Data regulation in Africa: Free flow of data, open data regimes and cyber security' 2022 African Economic Research Consortium Policy Brief.
493. Hilbig, Sven 'Development opportunity or digital colonialism? The planned WTO e-commerce agreement' 2021 Global Governance Spotlight.
494. Hon, W Kuan, Millard Christopher and Walden Ian 'The problem of personal data in cloud computing – What information is regulated? The cloud of unknowing, part 1' (2011) Queen Mary University of London Legal Studies Research Paper 75.
495. Hussein, Ibrahim Noor and Hashem, Mervat and Li, Zhiyong 'Security migration requirements: From legacy system to cloud and from cloud to cloud'(2013) 2nd International Symposium on Computer, Communication, Control and Automation.

496. Kathuria, Rajat and Kedia, Mansi and Varma, Gangdesh and Bagchi, Kaushambi 'Economic implications of cross border data flows' 2019.
497. International Organisation for Standardization and the International Electrotechnical Commission ISO/IEC 17788 Information Technology – Overview and Vocabulary 2014.
498. International Organisation for Standardization and the International Electrotechnical Commission ISO/IEC TR 22678 Information Technology – Cloud Computing – Guidance for Policy Development 2019.
499. Jan-Jaap, Oerlemans Investigating Cybercrime (PhD thesis, Leiden University 2017).
500. Jackson, Allan Paul Legal concerns arising from the use of cloud technologies (LLD thesis, University of Pretoria, 2017).
501. Koops, Bert-Jaap 'Cybercrime legislation in the Netherlands' (2010) Country report for the 18th International Congress on Comparative Law, Washington, DC 25 – 31 July 2010, session 'Internet Crimes.
502. Koops, Bert-Jaap 'The internet and its opportunities for cybercrime' (2011) 9 Tilburg Law School Legal Studies Research Paper Series 735.
503. Koops, Bert-Jaap and Goodwin, Morag 'Cyberspace, the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law' (2014) Tilburg Law School Legal Studies Research Paper Series Issue 5.
504. Metson, Robinson 'A critical analysis on the status of cyber crimes and legal reforms in Tanzania' (2015) Master of Laws Thesis University of Mzumbe 1.
505. Minnaar, Anthony ''You've received a greeting e-card from …': The changing face of cybercrime e-mail spam scams' (2008) Acta Criminologica CRIMSA Conference 92.
506. Mitrovic, Zoran; Klaas, Ntombovuyo and Mbhele Fidel 'Benefits of introducing the cloud computing based m-government in the Western Cape: Policy Implications' 2013 7th International Conference on Theory and Practice of Electronic Governance "Beyond 2015 – Smart Governance, Smart Development"' Soul, Korea 22 – 25 October 2013.
507. Mukherjee, Arpita and Soham, Sarma and Angan, Parashar and Bharti, Nibha Sarma, and Vishwanath, Drishti 'Covid-19, data localisation and G20: Challenges, opportunities and strategies for India' 2020 Working Paper Indian Council for Research on International Economic Relations.
508. Mvelase, Promise Sthembiso; Dlamini, Innocentia Zamaswazi; Marumo, Happy Sithole and Dlodlo, Nomusa 'Towards a government public cloud model: the case of South Africa' 2013 Second International Conference "Cluster Computing" CC 3-5 June 2013 Ukraine, Lviv 149.
509. O' Flynn, Aaron Michael 'Harmonisation and Cybercrime Jurisdiction: Uneasy Bedfellows? An analysis of the jurisdictional trajectories of the Council of Europe's Cybercrime Convention' 2014 PhD Thesis Queen Mary University of London.

510. Polatin-Reuben, Dana and Wright, Joss 'An internet with BRICS characteristics: Data sovereignty and the balkanisation of the internet' 2014 4th USENIX Workshop on Free and Open Communications on the Internet.
511. Ruelens, Joke 'Universal jurisdiction: an analysis from a comparative and international law perspective. A future for universal jurisdiction over serious crimes under international law?' 2016 Master of Laws Thesis University of Gent.
512. Schultz, Beverly Charlotte 'Cybercrime: An analysis of current legislation in South Africa' LLM Thesis.
513. Spoenle, Jan 'Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?' (Strasbourg: Council of Europe, 2010).
514. Swales, Lee 'An analysis of the regulatory environment governing electronic evidence in South Africa: Suggestions for reform'(2018) Doctor of Philosophy University of Cape Town.
515. Uroki, EY Rehema 'Damage to data is devastating' (2013) Master of Laws Thesis University of Tumaini.
516. Walden, Ian 'Accessing data in the cloud: The long arm of the law enforcement agent' (Queen Mary School of Law Legal Studies Research Paper 74/2011).
517. Taddese, Yamri 'Focus: Cloud Services Create Challenges fore-discovery' Law Times) (7 December 2015).

Internet Sources

518. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-11-march-2020 accessed on 31 August 2021.
519. https://www.eff.org/cyberspace-independence accessed on 3 January 2020.
520. https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab accessed on 13 January 2020.
521. https://www.internetworldstats.com/stats.htm accessed on 25 December 2019.
522. https://www.mrdfood.com/ accessed on 25 December 2019.
523. https://www.uber.com/za/en/ accessed on 25 December 2019.
524. https://www.kaspersky.co.za/resource-center/threats/ransomware-wannacry accessed on 28 December 2019.
525. https://www.internetworldstats.com/stats.htm accessed on 1 March 2022.
526. https://www.bbc.com/news/technology-49125853 accessed on 14 September 2021.
527. https://www.gov.za/speeches/president-cyril-ramaphosa-response-debate-state-nation-address-2019-14-feb-2019-0000 accessed on 29 April 2019.
528. https://about.google/ accessed on 28 June 2021.
529. https://www.ibm.com/za-en?lnk=m accessed on 28 June 2021.
530. https://www.amazon.com/ accessed on 28 June 2021.

531. https://www.microsoft.com/en-za accessed on 28 June 2021.
532. https://en.wikipedia.org/wiki/Silk_Road_(marketplace) accessed on 22 June 2019.
533. https://www.datacenterknowledge.com/microsoft/microsoft-launches-first-cloud-data-centers-south-africa accessed on 25 June 2019.
534. https://aws.amazon.com/blogs/aws/now-open-aws-africa-cape-town-region/ accessed on 3 May 2020.
535. https://news.microsoft.com/cloudforgood/ on 28 November 2020.
536. https://www.nist.gov/ accessed on 3 May 2020.
537. https://www.google.com/gmail/about/ accessed on 10 September 2021.
538. https://www.microsoft.com/en-za/microsoft-365/what-is-microsoft-365 accessed on 10 September 2021.
539. https://www.dropbox.com/?_hp=c&landing=dbv2 accessed on 10 September 2021.
540. https://www.salesforce.com/ accessed on 11 September 2021.
541. https://advice-cloud.co.uk/ultimate-guide-gcloud/ accessed on 10 September 2021.
542. https://www.iso.org/home.html accessed on 11 September 2021.
543. https://azure.microsoft.com/en-gb/ accessed on 11 September 2021.
544. https://aws.amazon.com/?nc2=h_lg accessed on 11 September 2021.
545. https://www.microsoft.com/MEA/trustedcloud/southafrica/public-sector.aspx accessed on 14 July 2020.
546. https://www.microsoft.com/en-za/microsoft-365/what-is-microsoft-365 accessed on 12 January 2021.
547. https://d1.awsstatic.com/WWPS/pdf/Using_AWS_in_the_Context_of_South_African_Privacy_Considerations.pdf accessed on 2 June 2020.
548. https://transparency.facebook.com/content-restrictions accessed on 13 January 2021.
549. https://policies.google.com/terms accessed on 13 January 2021.
550. https://support.google.com/transparencyreport#topic=7294962 accessed on 13 January 2021.
551. https://policies.google.com/terms/information-requests accessed on 13 January 2021.
552. https://transparencyreport.google.com/user-data/overview?dlr_requests=authority:;time:Y2019H1&lu=dlr_requests accessed on 13 January 2021.
553. https://transparencyreport.google.com/user-data/enterprise accessed on 13 January 2021.
554. https://www.cnbc.com/2021/12/29/amazons-alexa-told-a-child-to-do-a-potentially-lethal-challenge.html accessed 30 December 2021.
555. https://www.businessinsider.co.za/killer-drone-hunted-down-human-target-without-being-told-un-2021-5 accessed on 4 June 2021.

556. https://www.adams.africa/intellectual-property/inventorship-age-artificial-intelligence/ accessed 26 December 2021.
557. https://www.dw.com/en/saudi-arabia-grants-citizenship-to-robot-sophia/a-41150856 accessed 26 December 2021.
558. https://www.bbc.com/news/technology-50207192 accessed on 28 December 2019.
559. https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18255&view=map accessed on 27 December 2019.
560. https://mybroadband.co.za/news/internet/329539-massive-ddos-attacks-south-african-internet-providers-crippled.html accessed on 27 December 2019.
561. https://www.itweb.co.za/content/GxwQDM1A339MlPVo accessed on 27 December 2019.
562. https://www.kaspersky.co.za/resource-center/threats/ransomware-wannacry accessed 28 December 2019.
563. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack accessed 28 December 2019.
564. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ accessed 28 December 2019.
565. https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html accessed on 28 December 2019.
566. https://www.datacenterknowledge.com/microsoft/microsoft-launches-first-cloud-data-centers-south-africa accessed 05 February 2022.
567. https://www.reuters.com/article/us-safrica-amazon-com-cloud-idUSKCN2241X3 accessed 05 February 2022.
568. https://www.huawei.com/za/news/za/2019/huawei-cloud-africa-launch-due-for-march-2019 accessed 05 February 2022.
569. https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king Vox accessed 12 June 2021.
570. https://www.bbc.com/news/business-28047877#:~:text=The%20German%20government%20has%20cancelled,giving%20data%20to%20US%20authorities.&text=The%20firm%20did%20not%20comment,bugged%20Chancellor%20Angela%20Merkel's%20phone accessed 25 April 2021.
571. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html accessed on 25 April 2021.
572. https://www2.deloitte.com/be/en/pages/risk/articles/data-localisation-requirement-russia.html accessed on 18 April 2021.
573. https://www.camara.leg.br/noticias/696533-projeto-determina-que-dados-pessoais-de-brasileiros-sejam-armazenados-no-territorio-nacional/ accessed on 18 April 2021.
574. https://www.interpol.int/en/Crimes/Cybercrime accessed 05 February 2022.

575. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime accessed 05 February 2022.