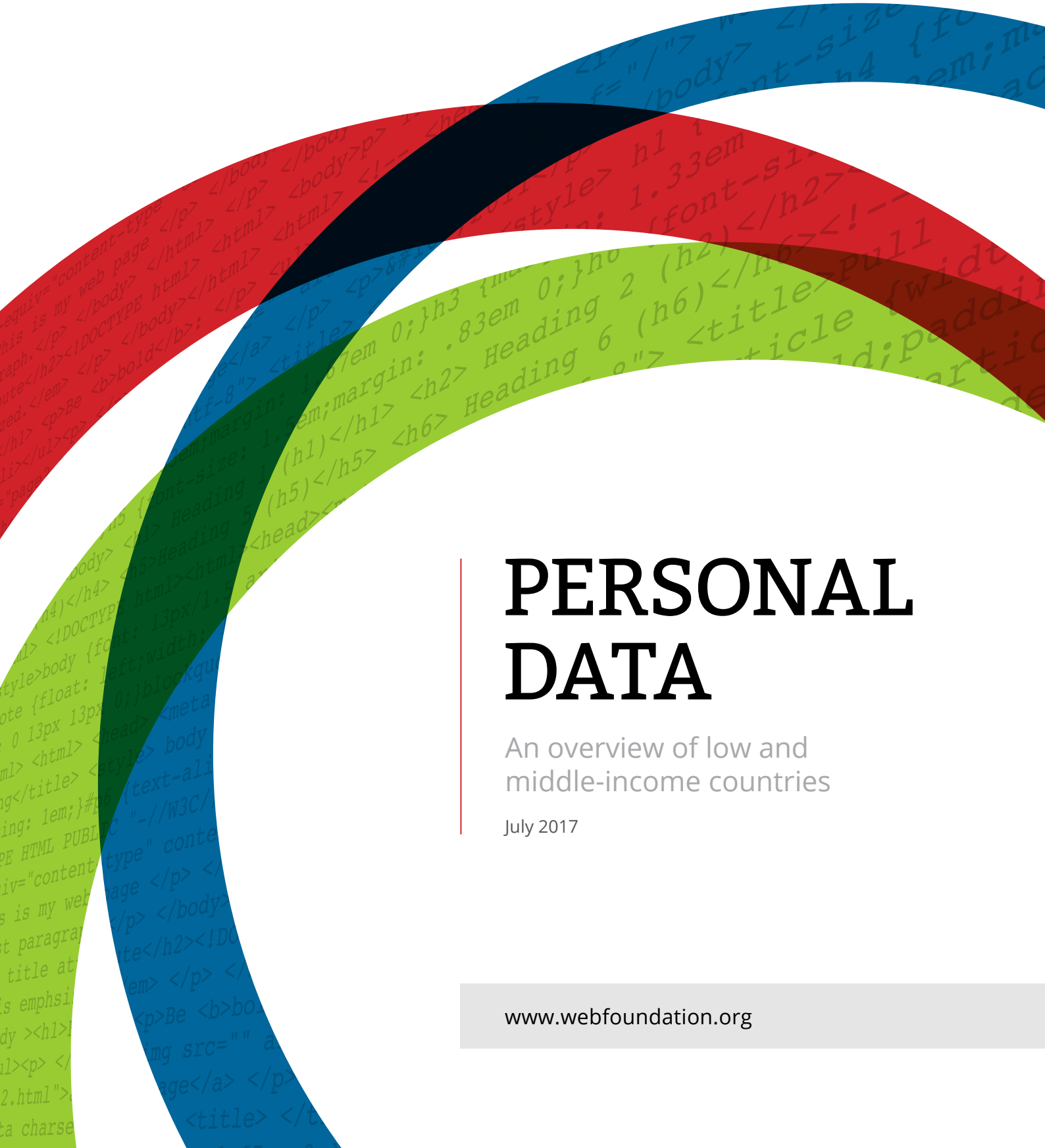
WORLD WIDE WEB FOUNDATION

A SMART WEB FOR A MORE EQUAL FUTURE

A series focused on identifying the challenges and opportunities ahead and ways to address them



PERSONAL DATA

An overview of low and middle-income countries

July 2017

www.webfoundation.org

CONTENTS

WORLD WIDE WEB FOUNDATION

The Web Foundation was established in 2009 by Sir Tim Berners-Lee, inventor of the World Wide Web. Our mission is to establish the open web as a public good and a basic right.

This paper has been adapted by the Web Foundation from a draft report commissioned to Claude Migisha and Musoni Fabrice.

This research was funded by a grant from the Ford Foundation.

FOREWORD

"To achieve this vision, we must keep an eye on the trends, technologies and forces shaping the web of tomorrow, and the policy interventions that will be required to ensure digital equality becomes a reality."

Welcome to this new series of policy white papers, produced by the World Wide Web Foundation.

The Web Foundation was established in 2009 by Sir Tim Berners-Lee, inventor of the World Wide Web. Our mission is to establish the open web as a public good and a basic right. Our five-year strategy – developed in 2016 – is to deliver digital equality – a world where everyone has the same rights and opportunities online. To achieve this vision, we must keep an eye on the trends, technologies and forces shaping the web of tomorrow, and the policy interventions that will be required to ensure digital equality becomes a reality.

On the web's 28th birthday in March 2017, Sir Tim Berners-Lee penned a letter on what he believed to be the biggest challenges facing the web today. The challenges he outlined are threefold: we've lost control over our personal data; misinformation spreads too easily online; and we need more transparency and understanding of digital political advertising.

Since then we have been discussing ways in which we could and should tackle these issues. We understood that these could be early warning signals of deeper problems, and set out to distil these in search of their most basic components. We landed upon data, algorithms and artificial intelligence, and the way these interact with existing socio-legal frameworks. These three issues are interdependent – data feed algorithms that are increasingly being used to make critical decisions, algorithms are the bedrock of artificial intelligence, and data gathered by AI and algorithms feed back into the system.

This is one of the three white papers we commissioned to begin to understand more about these issues. All too often, research, debate and discussion on these areas is focused on the US, UK and Europe, while actors from outside these countries are seldom being included as critical actors in thinking through policies at the global level. Our objective was to gain initial insights how each component is currently playing out in low and middle-income countries, and what some of the future risks and opportunities are.

An important step towards enabling collaboration and solving the challenges the web faces is increasing public and key stakeholder understanding of how the individual components of the system work. We hope that these papers make a small contribution towards this goal, including in countries too often ignored in these debates. We will now be using these papers to refine our thinking and set our work agenda in the years ahead. We are sharing them openly in the hopes that they benefit others working towards our goals.

We hope you enjoy the read, and we welcome your feedback. Let's work together to build a more open web for a more equal world.

Craig Fagan
Director of Policy, Web Foundation
June 2017

INTRODUCTION

In an era of fast paced technological advancements, issues related to control and use of personal data are taking centre stage. Personal data is often referred to as "the new oil of the Internet and the new currency of the digital world".[1] Moreover, the distinction between public and personal data is often blurry, begging the question: who uses and controls our personal data?

We now spend much of our lives online, and our online activities - from shopping to socialising, entertainment to information searching and gathering - have created an unprecedented number of data points. But these data bring risks. Once mined or breached, they reveal intimate details about our income, race, ethnicity, religion, and more. When governments opt to use these data for surveillance purposes, even when claimed to be for the public good, such data points can be used against us. Companies, meanwhile, can use this data in unethical or illegal ways, with impacts ranging from the relatively benign (such as unwanted ads) to the very harmful (unwarranted denial of credit or health insurance).

There is a clear indication that the datafication of our personal information will continue to be fostered by powerful companies, resulting in a data imbalance between the data haves (government and large corporations) and have nots. Furthermore, the very asymmetry of power around who controls personal data is fostering practices such as data commodification, identity theft, surveillance, and profiling, which are putting the lives of individuals at risk.

These general trends are evident across the globe, although different regions and countries are responding in different ways. In industrialised countries, initiatives are being led by the European Union (EU) and the Organisation for Economic Co-operation and Development (OECD) to shape legislation around personal data protection. Regional bodies elsewhere are beginning to follow suit with initiatives of their own. Yet the landscape for emerging economies is mixed. Among countries analysed for this study - Brazil, Dominican Republic, India, Indonesia, Mexico, the Philippines and South Africa - most have constitutional provisions protecting individual privacy. However, only Mexico, the Philippines, and South Africa have enacted data protection laws and empowered regulatory bodies to provide monitoring and enforcement mechanisms - as well as legal redress - for citizens who are victims of a data privacy violation.

1 Kuneva, M. (2009, March 31). Keynote Speech presented at The European Commission Roundtable on Online Data Collection, Targeting and Profiling in Belgium, Brussels.

Those interviewed in compiling this study point to several factors to explain why many countries have no data protection regulations (or ineffective ones).[2] First, there is a combination of government failure to prioritise the enactment of data protection laws, and a lack of public interest and trust in governments' ability to protect their personal data. Second, these laws fail to adequately address issues emerging from cross-border data transfers. This is significant when considering the high-level of interconnectedness of countries (through commercial and social interactions) and the fact that many low and middle-income countries lack the infrastructure to house their data locally.[3] Third, the lack of government oversight of intrusive surveillance means that regulatory bodies have encountered issues when trying to protect the personal data rights of consumers.

Currently, there is a dearth of surveys conducted in low and middle-income countries on consumer concerns around the use of their personal data. Still, trends about consumers perceptions and their personal data in high-income countries can allow for some extrapolation, particularly as connectivity and online activities continue to rise globally. First, there is a general misconception or lack of awareness regarding how entities collect and use personal information. Second, there is a growing mistrust among consumers in the ability of companies or institutions to protect their personal information. Consumers feel that these third parties benefit the most from customer data sharing. Third, though consumers understand the value of their personal data, they bemoan the lack of a trusted entity that allows them control over their own personal data, or appropriate advice regarding how to protect these data.

These findings suggest that the existing model of data protection is being challenged at its very core. The traditional approach, which has emphasised the consent of the individual at the time of collection of information and protecting the individual from all risks, no longer reflects modern day technologies and the risks posed to personal data. New approaches advocate for a model of protections that are either data-centric, or context-specific and adaptive. The focus is more on types of data use and/or technical approaches to empower individuals.

However, is "privacy self-management" possible given current data protection regimes? Are the current levels of protection in low and middle-income countries sufficient?

This paper aims to look at these questions, addressing a topic area that is under-researched.[4]

2 For full list of interviewees and those identified for consulting, see: https://docs.google.com/spreadsheets/d/1CAuact_YhzlcIftk7eMfvMU9oBh1Ir_m5KBm67aHz2I/edit#gid=0. Consulted here means, the authors reached out but were unable to schedule an interview. The authors then referred to their scholarship on the subject matter.

3 For figures on the number of secure servers in these countries, see: http://data.worldbank.org/indicator/IT.NET.SECR.P6?locations=XP-XM-XD.

4 Although privacy concerns such as cybercrimes, surveillance, and identity schemes are discussed in the paper, the scope of the paper is limited to data protection. These topics two topics are extensively covered by other organisations whose work has been highlighted in the country perspective section of the paper.

01

THE OPPORTUNITIES

1.1 The growth of data and data commodification

Globally, IBM estimates that 90 percent of the data in existence today has been created in the last two years.[5] A 2016 global survey of 600 companies shows that businesses collect massive volumes of personal data from individuals to then use the data to personalise customer offerings, innovate products and diversify into new markets.[6] Personal data is increasingly being seen as personal property.[7] As such, individuals are finding ways to obtain greater benefits from allowing companies to use their data. Three out of five companies surveyed in a global study believe that their customers are taking steps to actively monetise their own data.[8]

These developments signal the surging phenomenon known as data commodification. While still a nascent phenomenon, this is predominantly happening where robust legal, policy, and institutional frameworks are efficient and functional - such as in the US, UK and the EU. The scenario in most low and middle-income countries is different due to varying levels of internet access and weak or quasi-inexistent personal data protection mechanisms. In addition, individuals unwittingly may give up their personal data or have to cede it in order to access state services (such as through the large scale biometric ID systems seen in Brazil, India, Nigeria and elsewhere).

5 IBM (2017) 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations, IBM, http://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN

6 This is from findings which include Brazil and India. See: Cooper, T. and LaSalle, R. (2016), Guarding and Growing Personal Data Value. Accenture Institute of High Performance, https://www.accenture.com/t20160929T010202__w__/us-en/_acnmedia/PDF-32/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf

7 Lazaro, C., & Le Métayer, D. (2015). Control over Personal Data: True Remedy or Fairy Tale? SCRIPTed,12(1). doi:10.2966/scrip.120115.3

8 Cooper, T. and LaSalle, R. (2016), Guarding and Growing Personal Data Value. Accenture Institute of High Performance, https://www.accenture.com/t20160929T010202__w__/us-en/_acnmedia/PDF-32/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf

PERSONAL DATA CONTROL, PROTECTION, PRIVACY AND USE:

Understanding the Connections

It is important to clearly define the terms at play and how they related to each other:

- Control over personal data is the right of individuals to determine what information about themselves is collected, to determine what information is made available to third parties, and to access and potentially correct their personal data.[9]
- Data protection is "a key solution to the problems raised by personal data processing technologies",[10] and a remedy to challenges posed by these technologies that process - collect, use, store, transfer, disclose and destroy - personal data.
- Privacy is a type of "control over personal information".[11]
- Use refers to relying on personal information to make a decision or an assessment regarding an individual (such as through the employment of algorithms, artificial intelligence, etc.) or a group (such as through aggregating individual profiles). The dissemination and disclosure of personal data also fall under this definition of use.[12]

1.2 A new approach to data protections?

According to the World Economic Forum[13] the traditional approach to data protection needs to be revised to reflect recent technological evolutions that have given way to the era of Big Data. The traditional approach focuses on the individual's consent at the time of collection and is appropriate when the collected data was used for a specific purpose, and deleted when no longer needed. This approach to data collection fails to account for unforeseen uses of data long after the time of collection, and relies on unrealistic expectations regarding the data subject's ability to protect their privacy.

Against this backdrop, one approach has been to argue that personal data policies must be flexible and adaptive enough to foster innovation, but also they must protect the rights of individuals.[14] Given rapid technological advancements, it has been argued that the emphasis should be on how data is used rather than how it is collected. The belief is that empowering individuals to control how their data is used is better than solely protecting their data. Still, an argument could be made whether there is a sufficient balance of essential personal data protections and control mechanisms.[15] The Open Data Institute has attempted to address both sets of issues by elaborating seven principles on the control and use of personal data.[16] For data use, these principles call on organisations to be open and ensure that people are clear about what data about them is being collected, used, and shared. Data literacy is seen as a way to help people understand the terms and implications of sharing their data and better control it.

9 Lazaro, C., & Le Métayer, D. (2015). Control over Personal Data: True Remedy or Fairy Tale? SCRIPTed,12(1). doi:10.2966/scrip.120115.3

10 Ibid

11 Solove, D. J. (2008). Understanding Privacy (Chapter One)[PDF]. Cambridge, MA: Harvard University Press

12 Cate, F. H., Cullen, P., & Mayer-Schönberger, V. (2014, May). Data Protection Principles for the 21st Century: Revising the 1980 OECD Guideline[PDF].

13 Unlocking the Value of Personal Data: From Collection to Usage[PDF]. (2013, February). Geneva: World Economic Forum & Boston Consulting Group.

14 Unlocking the Value of Personal Data: From Collection to Usage[PDF]. (2013, February). Geneva: World Economic Forum & Boston Consulting Group.

15 Kearney, A. (2014, May). Rethinking Personal Data: A New Lens for Strengthening Trust[PDF]. Geneva: World Economic Forum.

16 Broad, E. (2016, March 2). Bringing together privacy and openness: the ODI shares draft personal data principles | News. Retrieved February 16, 2017. Available at http://bit.ly/24DXiBs (last accessed 6/5/2017)

1.3 Global and regional efforts

There is growing interest among global and regional institutions to address these exact issues of the control and use of personal data. This is occurring globally, regionally and nationally where governments and regional/international bodies are drawing on fair information practices (FIPs), which began being adopted in the 1970s, as the basis for their data privacy policies.

Globally, efforts have been taken up by the United Nations General Assembly, which adopted a new resolution in 2016 on the right to privacy in the digital age.[17] In response to multiple re-sales of personal data without the explicit and informed consent of concerned individuals, this resolution was seen to call on governments and companies to develop preventative measures, sanctions and remedies to inform consumers of policies infringing on their right to privacy. The resolution comes four years after the adoption of the UN Resolution on Digital Rights,[18] and the appointment, in July 2015, of a Special Rapporteur on the right to privacy.[19]

Within different country blocs, a series of initiatives have been targeted at personal data protections. In 2016, the European Union (EU) adopted a Directive on General Data Protection Regulation (GDPR),[20] which is to be transferred into law by May 2018. The GDPR requires organisations that process personal data for EU citizens to be compliant with the regulation within two years. Currently, this is seen as one of the better standards that merits replication. The G20 and OECD also have increasingly taken on more prominent roles on the issue. Under Germany's leadership of the G20, a focus has been created on digital economies and specifically around the digital rights of consumers (Argentina is the next G20 chair and has committed to carrying forward the agenda). It is believed that the G20 will delegate to the OECD to continue work on privacy norms and principles, which have been recently revised.[21] Meanwhile, the Commonwealth of Nations has recommended relevant model laws — the Privacy Bill and the Protection of Personal Information Bill — for adoption or adaptation as national legislation of member countries to address issues related to information privacy.[22]

Regionally, good practice principles for personal data protections are being advanced although more binding commitments have had mixed success. In Asia, the Asia-Pacific Economic Cooperation (APEC) has developed several data protection initiatives (2017) including common APEC Privacy Principles.[23] In Africa, the African Union adopted in June 2014 a Convention on Cyber-security and Personal Data protection, but as of June 2017, only Senegal had ratified its commitment.[24] The Economic Community of West African States (ECOWAS), through the ECOWAS Supplementary Act A/SA.1/01/10 on data protection, has seen the establishment of a data protection authority in seven of its member states. The East African Community (EAC) Framework for Cyberlaws approved in 2010 is another regional framework that recommends the establishment of a regulatory regime for data protection but the EAC does not make any specific recommendations.[25]

The overall focus on data protection of these different frameworks shows there is a growing consensus on the need to safeguard personal data in the current context of growing "datafication" and the commodification of personal data. It also signals the recognition that current frameworks — such as within the UN or OECD — need updating in order to protect people adequately (see box). The range of initiatives also helps to begin to reveal to what extent there has been an alignment between some of the key features needed to protect personal data and how they are addressing (or not) the balance between protecting, using and controlling personal data.

17 The right to privacy in the digital age[PDF]. (2016, November 16). New York: United Nations General Assembly.

18 The promotion, protection and enjoyment of human rights on the Internet. (2012, July 15). New York: United Nations General Assembly.

19 Data protection regulations and international data flows: Implications for trade and development. (2016, April). Geneva: United Nations Conference on Trade and Development.

20 EU Parliament and Council Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016). Official Journal of the European Union L 119/89

21 These were last updated in 2013: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

22 UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. New York and Geneva. Available at http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 Last accessed 6/7/2017)

23 The APEC principles are seen by some as a rival approach to the EU's position since the APEC principles are based on holding data controllers accountable for breaches ex-post instead of regulating ex-ante.The three key APEC (2017) initiatives are: 1) the development of a set of common APEC Privacy Principles; 2) the development of a system for coordinating complaints that involve more than one APEC jurisdiction; and 3) the development of the Cross-Border Privacy Rules system (CBRPs).

24 List of countries which have signed/ratified/acceded to the Convention on Cybersecurity and Personal Data Protection (updated 15 June, 2017), African Union. Available at https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_.pdf (last accessed 7/7/2017)

25 Robert Achieng, R. (2015) Regional Case Study: Cyberlaw Reform in the EAC. UNCTAD. Available at http://unctad.org/meetings/en/Presentation/CII_EM5_P_RAchieng_en.pdf (last accessed 7/7/2017)

SETTING GLOBAL DEFINITIONS AND PRINCIPLES:

The Role of the OECD

In the 1980 guidelines governing the protection of privacy and transborder flows of personal data, the OECD laid out two relevant principles which help explain current thinking on data use: purpose specification,[26] and use limitation.[27] In a bid to address the challenge of balancing individual privacy with valuable uses of data in 21st century, the OECD set up a group of experts in the beginning of 2010 to re-examine the guidelines in light of significant changes, in particular the volume of personal data collection, use and storage, and the value of the societal and economic benefits enabled by new technologies and responsible data uses.[28] The OECD Expert Groups recommended updating the guidelines without changing the basic principles. Under the auspices of Microsoft and the Oxford Internet Institute, a working group of senior leaders reviewed OECD Guidelines,[29] and recommended to "shift responsibility for data protection away from individuals, and to focus on data use rather than data collection".

26 The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. See: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (1980). Retrieved February 17, 2017, from http://bit.ly/1gaZQzY .

27 Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance except: a) with the consent of the data subject; or b) by the authority of law (OECD, 1980).

28 Cate, F. H., Cullen, P., & Mayer-Schönberger, V. (2014, May). Data Protection Principles for the 21st Century: Revising the 1980 OECD Guideline[PDF].

29 Ibid

02

THE RISKS

If the opportunities outlined above are to be harnessed, a number of risks and barriers will need to be overcome. These include the challenges of weak legislation, growing public mistrust of how personal data is being used, more widespread surveillance, increased collection of personal data by governments, and low levels of company transparency and accountability on data policies.

2.1 Weak legislation

The growing number of frameworks is a positive signal of global, regional and national responses to increased concerns around the use and control of personal data. However, many of these frameworks, particularly in the Global South, do not offer a strong level of protections in either policy or practice.

The following table presents an overview of how some of these regional measures currently stand-up against different areas of data protection.

As seen across the board, only the EU GDPR stands out for being assessed as strong or moderate on all the assessed fronts. The AU is seen to be strong in addressing gaps in coverage due to its comprehensive membership. However, AU-led initiatives are new and do not have political support at this stage, hence why the continental framework is not yet capable of strengthening the enforcement of data protection laws and addressing new technologies that impact personal data use. As a regional framework, ECOWAS could play a role in managing cross-border data transfer restrictions and compliance burden in West Africa. Lastly, the APEC framework is relatively new and has limitations in many aspects that are related to balancing surveillance and data protections; enforcement; and determining jurisdiction.

Table 1 — Strengths and limitations of the main regional frameworks for data protection

	VERY WEAK	WEAK	MODERATE	STRONG
ADDRESSING GAPS IN COVERAGE	Trade Agreements	OECD	EU Directive	EU GDPR
		APEC	ECOWAS	AU
		Commonwealth		
ADDRESSING NEW TECHNOLOGIES		APEC	OECD	
		Commonwealth	Trade Agreements	
		AU	EU Directive	
		ECOWAS	EU GDPR	
MANAGING CROSS BORDER DATA TRANSFER RESTRICTIONS		OECD	EU Directive	EU GDPR
		Commonwealth	Trade Agreements	
			APEC	
			AU	
			ECOWAS	
BALANCING SURVEILLANCE AND DATA PROTECTION	APEC	OECD		Trade Agreements
	Commonwealth	AU		EU Directive
		ACOWAS		EU GDPR
STRENGTHENING ENFORCEMENT	APEC	AU	EU Directive	EU GDPR
	OECD	ECOWAS		
	Commonwealth			
	Trade Agreements			
DETERMINING JURISDICTION	APEC	Trade Agreements	EU Directive	EU GDPR
	OECD	ECOWAS	AU	
	Commonwealth			
MANAGING THE COMPLIANCE BURDEN	Commonwealth	APEC	OECD	Trade Agreements
		EU Directive	AU	
		EU GDPR	ECOWAS	

Source UNCTAD, 2016[30]

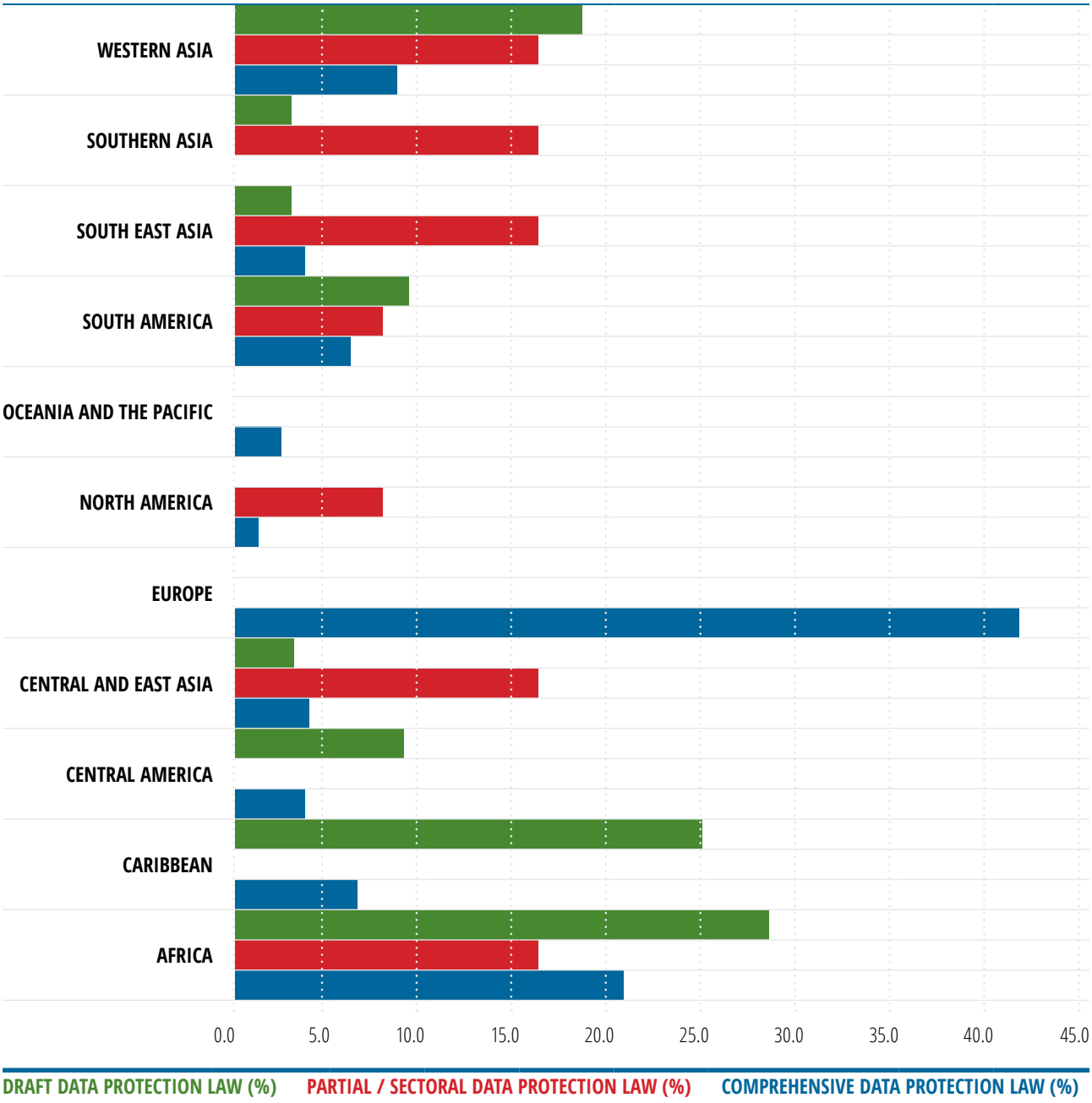
In many cases, regional-level measures have been used as a springboard for developing national legal frameworks. However, the reality is that there are generally weaker data protections in low and middle-income countries, leaving their citizens at risk. Figure 1 offers relevant regional insights on the current state of national legislation and the share of that region in the overall number of existing data protection laws (draft, partial/sectoral or comprehensive) across the world. Excluding Europe, less than 30 percent of all countries across all regions have adopted comprehensive data protection legislation. Out of the countries of focus in this study, only Mexico, the Philippines and South Africa currently have stand-alone data protection laws. Brazil, Indonesia, India and Nigeria have draft laws that have yet to be adopted. In the other countries like the Dominican Republic, the laws tend to be piecemeal and sectoral.

A survey of government representatives in 48 countries in Africa, Asia, Latin America and the Caribbean helps to point to some of the reasons why low and middle-income countries are not enacting and enforcing data protections. The survey, completed by UNCTAD in 2016[31], reveals that more than 60 percent of the representatives reported difficulties in understanding legal issues related to data protection and privacy. Similarly, 43 percent of them noted that a lack of understanding among parliamentarians and 47 percent among police or law-enforcement bodies. These findings suggest institutional impediments that could delay the adoption and enforcement of data protection laws.

30 UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. UNCTAD. New York and Geneva. Available at http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 Last accessed 6/7/2017)

31 Ibid

Figure 1 — Global Percentage of comprehensive, partial/sectoral approaches, and draft data protection laws



Source UNCTAD, 2016[32]

32 UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. New York and Geneva. Available at http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 Last accessed 6/7/2017)

2.2 Growing public mistrust

Across all countries, people do not always understand how their personal data will be used once they give "notice and consent". There is also an increased feeling of mistrust towards companies capturing their personal information, regarding how their data is being used and protected.[33]

According to one report, a large percentage of the US population often does not have the basic knowledge to make informed cost-benefit choices about the ways marketers use their information.[34] In Europe, a separate study has revealed that European consumers have a growing mistrust of different organisations' ability to protect personal data.[35] Another study focused on the UK shows that only one in four British consumers report they understand how companies collect their personal information while nearly nine out of every 10 British consumers avoid using companies that they believe don't protect their privacy.[36]

In low and middle-income countries, public opinion surveys on these related questions have been very limited. An Ipsos MORI survey of 20 countries — including many middle-income countries like Brazil, India, Indonesia and South Africa — shows that there is an increasing tension emerging between the push by companies to use data and the need to respect an individual's data privacy and personal control over the data.[37] Other surveys have shown that most internet users do not feel fully aware of the types of personal information that is collected about them, as seen in Brazil (76%) and South Africa (82%). Surveyed internet users also seem to feel that technology is affecting their privacy, according to the findings for Brazil (54%), South Africa (59%), and Indonesia (30%).[38] This may be related to the fact that figures show that people tend not to read terms and conditions or user agreements on websites, such as in Brazil, India and South Africa where such numbers are above 80 percent.[39] As all the findings are based on self-reporting, the actual percentages are likely higher.

These findings across various countries would suggest that consumers need a trusted entity who can help them make the most of the value of their personal data and to advise them on how to protect their personal information.

2.3 Increased surveillance

Companies and governments are increasingly seen as using the personal data they capture to profile people in the name of "personalised services" and/or "national security".[40]

Companies like Google and Yahoo have applied ad scanners to emails that are received by users of their services. While Google changed this policy in June 2017, it had previously come under fire for its terms of service agreements, which stated: "Our automated systems analyze your content (including e-mails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."[41]

Governments continue to blur the line between national security and personal data privacy. Kenya is seen by many to have weakened the country's privacy rights as a result of overly harsh security laws that have opened the door for broad state surveillance practices with scant oversight.[42] In Mexico, the Federal Law of Telecommunications and Broadcasting of 2014 (i.e. the Telecom law[43]) allows the store of metadata and personal data for two years and originally permitted national authorities (such as prosecutors, Navy, federal police and army) access to this data without judicial authorisation. In 2016 the Supreme Court ruled a judicial authorisation was necessary to access such data, which should only be made accessible to prosecutors.[44]

In Brazil, there have been clashes between the private and public sector over requests to access personal data for law enforcement purposes. In 2016, for instance, the Brazilian police arrested Facebook's Vice President for Latin America following a dispute over a court's order that the company provide data from its WhatsApp messaging service to aid in a secretive drug-trafficking investigation. Facebook deplored the "extreme and disproportionate measure," in what some argue is becoming a growing trend of governments using companies to spy on users.[45]

In order to harness the benefits available from greater amounts of personal data, people will need to be reassured that neither companies nor governments are leveraging this data for unwarranted surveillance.

33 Ibid
34 Turow, J., Hennessy, M., & Draper, N. (2015, June). The Trade Off Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation[PDF]. Philadelphia: The Annenberg School for Communication University of Pennsylvania.
35 The future of digital trust: A European study on the nature of consumer trust and personal data[PDF]. (2014, February). London: Orange & LoudHouse
36 The TRUSTe/National Cyber Security Alliance GB Consumer Privacy Index. http://www.prnewswire.com/news-releases/study-finds-more-british-internet-users-concerned-about-data-privacy-than-losing-their-income-300211205.html
37 Ipsos Mori. (2014). Global Trends 2014. Available at http://bit.ly/1kyZ3XA (Last accessed 03/03/2017)
38 All figures cited are from: Penn, M. (2015, January). Views from around the Globe: 2nd annual poll on how personal technology is changing our lives[PPT]. Davos: Microsoft.
39 Ipsos Mori (2014). Op. Cit.
40 Lauterbach, C. (2017, March 2), Tracking the global state of surveillance. Privacy International, https://www.privacyinternational.org/node/773(accessed on 6 July 2017)
41 Note that this policy for emails has changed as of June 2017;_r=0 . See: Wakabayashi, D. (2017, June 23) Google Will No Longer Scan Gmail for Ad Targeting. New York Times. Available at https://www.nytimes.com/2017/06/23/technology/gmail-ads.html? (last accessed 7/7/2017)
42 Privacy International (2016, March 3). State of Surveillance: Kenya. Privacy International. Available at .https://www.privacyinternational.org/node/783 (last accessed 4/5/2017)
43 Congress of Mexico (2014). Federal Law of Telecommunications, Art 190. Available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_270117.pdf (last accessed 4/5/2017)
44 Freedom of the Net 2016 (2016). Freedom House. Available at https://freedomhouse.org/report/freedom-net/2016/mexico (last accessed 4/5/2017)
45 Haynes, B. (2016, March 1). Facebook executive jailed in Brazil as court seeks WhatsApp data. Reuters. Available at http://reut.rs/1OOnH3U (Last accessed 3/3/2017)

2.4 Growth in government data collection

In conjunction with the expansion of surveillance activities, there has been a generalised increase in the amount of personal data that governments are collecting on their citizens. For example, the rise of digital identification schemes has opened up a new front of vulnerabilities and worries about individual data protections.

In India, the Aadhaar digital ID system is hugely controversial. It is one of the key pillars of the 'Digital India' — the government's flagship digital policy — and is by far the largest biometrics based identification system in the world. Since 2010, some 1.11 billion Aadhaar cards have been generated, covering 92% of all Indians.[46] Aadhaar is de facto mandatory to access subsidies and services, as well as to file taxes. People have gone to court to express concerns that Aadhaar is a tool for surveillance and in violation of their privacy.

Brazil, Indonesia, Nigeria, the Philippines and South Africa are among a group of countries that are moving to adopt similar digital ID systems or biometric IDs. Non-compliance brings the risk of being left out from accessing financial services, voting privileges, and passports, among other state services.

In Brazil, there are on-going plans to introduce a biometric ID card system that has facial and fingerprint capabilities.[47] Moreover, the 27 regional identity registries are to be consolidated into one single federal registry. Additionally, SIM card registration requires, at a minimum, the collection of one's name, ID card number and taxpayer number which are then shared with the government (a similar scheme is being considered in the Philippines).

In Nigeria, the National Identity Management Commission (NIMC) has adopted a policy to implement a digital ID as of 2014, but there are serious concerns about its impact on data protection and privacy.[48] First, there are no provisions for the protection of citizens whose data is collected and stored. Second, without a comprehensive data protection law in Nigeria, there is an increased risk of personal data abuse and misuse and there is no legal recourse in the event of the violation of an individual right to privacy and personal data breaches. Currently, there is no penalty for loss or misuse of personal data by an agency or agencies with authorised access to the personal data of Nigerians.

It is critical that legal frameworks are able to strike a balance to allow governments to collect and use the data they need to enhance service delivery and the quality of life for their people, but also to ensure robust personal data protection.

46 Karnik, M. (2017, March 16) World Bank's top economist says India's controversial ID program should be a model for other nations. Quartz. Available at https://qz.com/933907/paul-romer-on-aadhaar-world-banks-top-economist-says-indias-controversial-id-program-should-be-a-model-for-other-nations/ (Last accessed 7/7/2017)

47 Doneda, D., & Varon, J. (2017, March 14). State of Privacy Brazil. Privacy International. Available at http://bit.ly/2nHZhXb (Last accessed 7/7/2017)

48 Nkum, K., Bikwa, O., & Ogbodo, C. (2016). Nigeria's Urgent Data Privacy Law Need [PDF]. Lagos: Paradigm Initiative Nigeria.

DATA BREACHES ON THE RISE

In light of recent hacking cases of companies' customer databases[49] or government data files,[50] there is increased concern in certain countries (primarily the UK, US and EU) about how personal data is being safeguarded. Yet such breaches are certainly not limited to high-income nations.

In Brazil, security failures led to a leak of personal data records from the database of the Municipality of São Paulo — including identification, address, phone number and even medical information — of 650,000 patients and civil servants.[51]

In the Philippines, the information of over 55 million registered Filipino voters was leaked following a breach on the Commission on Elections' (COMELEC) database, also dubbed "Comeleak".[52] The National Privacy Commission, set up to handle data protection matters, was a mere two weeks old and the high profile data breach was its first case. The leak illustrated both the extent of personal information being collected and held by government authorities as well as gaps in securing such information.

49 See:Thielman, S. (2016, July 17) Yahoo hack: 1bn accounts compromised by biggest data breach in history. The Guardian. https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached (Last accessed 7/7/2017)

50 See: Vijayan, J. (2016, November 15)The 7 Most Significant Government Data Breaches. Dark Reading. Available at http://www.darkreading.com/attacks-breaches/the-7-most-significant-government-data-breaches/d/d-id/1327468 (Last accessed 7/7/2017); and Press Association (2016, September 13). Government breached personal data security 9,000 times in a year. The Guardian. Available at https://www.theguardian.com/uk-news/2016/sep/14/government-breached-personal-data-security-9000-times-in-a-year-nao-watchdog-reveals. (Last accessed 7/7/2017)

51 Privacy International (Last Modified, 2017, July 17) State of Privacy in Brazil. Privacy International. Available at https://www.privacyinternational.org/node/979 (Last accessed 7/7/2017)

52 Foundation for Media Alternatives. (2017, March 28). COMELeak: A Year Hence. FMA. Available at http://www.fma.ph/?p=1016 (last accessed 7/7/2017)

2.5 Low levels of company transparency and accountability on data policies

Global assessments suggest that ICT companies have a low level of transparency regarding data protections and related policies. Ranking Digital Rights ranks 22 of the most powerful telecom, internet and mobile companies across the globe that collectively offer products and services to half of the world's 3.7 billion internet users. This study shows that most companies are getting a failing grade on disclosing commitments and policies affecting one's freedom of expression and data privacy. Across the board, the average score is 33 percent. One of the key findings shows that a particular problem area is around the handling of user information and disclosing how user information is processed and shared.[53] For example, according to this study, the Mexican telecom giant América Móvil discloses little about what types of user information it collects, shares, why, and how long it retains user information. Moreover, América Móvil provided practically no information regarding how it handles requests from governments and private parties to share user information.

This links to concerns about data collection policies that are covered under a company's Terms of Service (ToS) agreements. These tend to be long and contain terminology that is hard to grasp for the average citizen. At the same time, the agreements tend to be a take-it or leave-it affair: either you accept them, or you don't access the service (see box).

53 See: Ranking Digital Rights Website, available at rankingdigitalrights.org (Last accessed 7/7/2017)

TERMS OF SERVICE AND DATA PROTECTIONS

A Crossroad

Across some of the countries included in this study, domestic laws require that ToS cover matters related to data protection.

- In the Dominican Republic, the Dominican Institute for the Protection of Consumer Rights (PROCONSUMIDOR) has been reviewing ToS agreements of e-commerce websites to verify that there are no abusive clauses in them. As part of the review process, the institute requires that sites ensure the protection of data privacy in their ToS.
- In India, the private sector, tech and telecom companies must provide provisions for privacy policy in their Terms of Service (ToS) agreements as required by the IT Rules on Reasonable Security Practices, 2011. The rules stress the need for a clear and accessible privacy policy.
- In Mexico, the terms of service (ToS) agreements are not specifically covered by the major legislation on personal data protection for the public and private sector. Nevertheless, there are provisions to obtain consent for sensitive personal information and requirements, which are similar to European ones, for entities collecting data to issue privacy notice to individuals sharing their data.[54]

Still, in the countries of focus for this study, experts interviewed tended to agree that there is a general lack of awareness among consumers around Terms of Service agreements, which are often hidden and difficult to understand.[55] This will need to be addressed.

54 Web Foundation Research: Interview with Isabel Davara [Online survey]. (2017, March 20).

55 Web Foundation Research: Interview with Maria Solange Maqueo Ramirez [Skype interview]. (2017, March 23) Web Foundation Research: Interview with Peter Ayeni [Skype interview] (2017, March 8)

03

A WAY FORWARD

Similar to how an idea of justice is needed in order to establish the rule of law, an idea of data justice is paramount to determine how best to deal ethically and legally with a world that is quickly commodifying data. One proposed approach to achieving data justice comprises three key elements:[56]

- Everyone should be free from greater government infringement on their (data) privacy;
- Everyone should be free to create and use a "digital identity";
- Everyone should have the right to identify and challenge when their personal data is used to discriminate against them.

It is believed that data justice, once operationalised, can empower individuals by allowing them to participate in decisions and markets related to their data, access data affecting them and gaining knowledge about data-related technologies.

To ensure data justice, there is a need to counter data-driven initiatives which raise the risks of abuse and misuse of personal data — which could lead to discrimination, surveillance, cybercrime or worse. This means ensuring that the collection and holding of a tremendous amount of personal data is done with proper oversight and legal recourses available to citizens in the event of privacy violations. Legal and institutional frameworks must be in place to allow citizens to hold accountable their governments and companies for their policies and action. As such, to effectively engage with technology, citizens must have control over the terms of engagement with those controlling their data.

The following are some potential areas for action to take forward this work in low and medium-income countries.

56 Taylor, L. (2017). What Is Data Justice? The Case for Connecting Digital Rights and Freedoms on the Global Level.

POTENTIAL AREAS FOR ACTION

1. Ensure a comprehensive data protection law and supporting frameworks are in place.

- Draw on good practice models where useful, such as the EU GDPR.
- Reignite efforts to pass good draft data laws which are currently stuck.
- Work in coalitions to overcome the considerable impediments towards enacting comprehensive data protection legislation, such as those in Brazil, India, Indonesia and Nigeria.

2. Pressure governments to implement effective legal mechanisms to regulate the control and use of personal data.

- Streamline and integrate piecemeal and sectoral regulations that address data protections and privacy to achieve a "whole of government" approach to the issue.
- Adjust policy incentives and penalties to promote compliance with laws.
- Provide adequate resources to institutions implementing and overseeing the implementation of data protection regimes, including for outreach to the general public about their rights.

3. Mobilise civil society actors to push a public discussion on why data protection matters:

- Use innovative campaigns and outreach to make people aware and concerned about the use and control of their personal data.
- Partner with other concerned actors — from companies to academia — to raise awareness and take joint legal action when needed.
- Leverage the good work of consumer rights groups to push a consumer digital rights agenda.

4. Work with companies to be more transparent and accountable to regain consumer trust.

- Collaborate with and advocate companies to make terms of service agreements more open and understandable to the public.
- Create spaces for consumers to provide feedback on and shape company data privacy policies.
- Design a forward-looking plan to roll-out the necessary investments in infrastructure, enabling users to choose to host data locally, and afford the protections included in local laws and regulations when they are stronger.

04

CASE EXAMPLE: COUNTRY LEGISLATION

This section provides a regulatory snapshot of what data protections are currently in place and the main actors involved in upholding them. The countries covered include a sample of nations from across all regions: Brazil, Dominican Republic, India, Indonesia, Mexico, Nigeria, the Philippines and South Africa.

4.1 Brazil

Although privacy and consumer data rights are safeguarded in the 1988 Constitution, Brazil does not currently have comprehensive data protection legislation.

In Brazil, observers argue that current legislation is sectoral and regulates specific issues ranging from consumer protection, internet, and telecom services. There are, however, encouraging attempts to move towards a comprehensive data protection law.

First, a Draft Bill for the Protection of Personal Data was released in January 2015. The bill requires explicit consent to transfer personal data — with limited exceptions — while restricting the transfer of personal data to countries that provide an equivalent level of data protection to Brazil.[57] Though the draft bill has been influenced by the EU directive on data protection, there is currently no regulatory authority in Brazil to oversee compliance.

Second, there is the Consumer Protection Law of 1990, which provides enforceable privacy rules between a consumer and supplier, but this law only applies within Brazil.

Third, the Brazilian Internet Civil Rights Law of 2014 (Federal Law No. 12965/2014), also known as “Marco Civil” and which took six years to enact into law, provides Brazilian citizens and Internet users additional statutory protections of privacy as well as protections around the collection and sharing of personal data online. The Marco Civil calls for, "clear and complete information on the collection, use, storage, processing and protection of users' personal data, which may only be used for the purposes...(that) a) justify its collection; b) are not prohibited by law; and c) are specified in the agreements of services or in the terms of use of the Internet application."[58] The retention or disclosure of personal data, the Marco Civil dictates, must comply with the protection of privacy of the parties directly or indirectly involved. Only under a judicial court order can personal data be disclosed. The law's coverage is nationwide and applies to entities that provide services to the Brazilian public, even when these companies might be based outside of Brazil. In the case of non-compliance, Marco Civil prescribes a fine worth 10 percent of the gross economic activity of the entity, a temporary suspension of its activities, and the requirement to halt its activities. However, the Marco Civil does not provide for a regulatory authority and current legislation does not place restrictions on the cross-border transfer of data.[59] As such, the Brazilian Institute for Consumers has called for more norms and institutional structures to govern international data flows.

In spite of the fact that Brazil is pushing the envelope on the global agenda around privacy protection, the lack of a comprehensive legislative and regulatory framework poses risks of misuse and abuse of the personal data of Brazilian citizens.

---

57 UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. New York and Geneva. Available at http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 Last accessed 6/7/2017)

58 For translation and full law, see Internet Management Committee of Brasil's Website, at: https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/18 (last accessed 7/7/2017)

59 UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. UNCTAD. New York and Geneva. Available at http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 Last accessed 6/7/2017)

4.2 Dominican Republic

There is no comprehensive personal data protection legislation or regulatory authority in the Dominican Republic. However, the Dominican Republic has adopted a sectoral approach, similar to Brazil. The closest law to a comprehensive data protection legislation is Law No. 172-13 on the Protection of Personal Data that was passed in 2013.[60] The law regulates the treatment of personal information in public or private archives, records, data banks or any other technical means intended to provide public or private reports.[61] Moreover, the protection of privacy is enshrined in the Constitution (Article 44) with provisions on compensation to individuals whose privacy has been violated. Furthermore, any person or information owner, through a habeas data constitutional remedy, can submit a claim to the database owner to update, contrast, rectify or destroy information. In addition to personal data protection legislation, there are laws regulating specific sectors with data protection and privacy provisions, including for banks, telecoms and health (such as HIV status and other health data).[62]

With regards to the existence of enforcement mechanisms, Law 24-97, which amends Art. 337 of the Criminal Code, punishes the violation of privacy with between six months and one year imprisonment and fines from 25,000-50,000 Dominican pesos (roughly USD 530 to 1,061). The Criminal Code understands a violation of privacy has occurred whenever a person captures, records, or transmits to third parties words, images, and documents produced in the private sphere, without the consent of the affected. In addition, the Law 200-04 on Free Access to Public Information provides grounds for the rejection of information requested under "prevailing private interests". In other words, the disclosure of personal data constitutes an invasion of the person's privacy unless the information requested is of public interest.

The relevant regulatory authority on these matters is the Dominican Institute of Telecommunications (INDOTEL) It was established by Resolution No. 55-66 and Law 126-02 on Electronic Commerce, Digital Documents and Signatures. INDOTEL regulates the treatment of personal data of subscribers and users of certification and digital signature services, such as ensuring the confidentiality of data and information on telephone services.[63]

The way forward on broader personal data protection and privacy in the country requires enacting comprehensive data protection legislation with a regulatory authority to implement and enforce compliance with the law. In fact, the Open Government Partnership (OGP) Action Plan for the Dominican Republic contains a commitment to creating a legal framework for the protection of personal data, both in the public and private domain.[64]

4.3 India

India has adopted a partial approach to data protection based on a combination of statutes, rules and guidelines. As such, India does not have comprehensive privacy legislation and the Constitution does not specifically guarantee a right to privacy unless privacy is interpreted under the right to life and liberty.[65] Choudary[66] claims that the question of whether privacy is a fundamental right is pending before the Supreme Court of India. With regards to sensitive personal data or information (i.e. a data subject's password, financial information, health, sexual orientation, medical records, and biometric information), the Information Technology Act (2000), as amended by the Information Technology Amendment Act (2008) addresses reasonable security practices and procedures and is complemented by the 2011 Information Technology Rules. According to Choudhary,[67] these rules stress security measures required while handling or dealing with personal information, including sensitive information by a corporate body or any person acting on its behalf. The IT Act and Rules is the strongest legal protection provided for personal data information.

The rules also require all corporate bodies to establish a privacy policy for all information providers and obtain expressed consent from information providers prior to the collection, use, and disclosure of sensitive personal information.[68] In addition, individuals must be informed of the collection, the purpose of collection, the intended recipients, the name and the address of the agency collecting, and the agency that will retain sensitive personal information. Furthermore, individuals should have the option to opt in or out of services prior to the collection of sensitive personal information and should have the ability to withdraw consent at any point in time. While companies must obtain consent from the individual who the information belongs before it is used, service use contracts or legal requirements and requests from a mandated governmental agency are grounds for disclosing sensitive personal information to a third party.

In the case of data breaches, the IT Act provides legal recourse in the form of compensation by a corporate entity for failing to protect personal and sensitive data or information as a result of negligence, and a penalty for breach of confidentiality and privacy by any person.[69] The IT Act also prescribes punishment to any person for disclosure of information in breach of contract. The Consumer Protection Act of 2015 offers an additional source of redress in the event of abuse and misuse of sensitive personal information by commercial entities. With respect to the transfer of sensitive data offshore, data can be transferred only to a country where it is clear that the sensitive data will be adequately protected.

The provisions are, however, limited in scope as they only apply to sensitive personal information, are restricted to corporate entities undertaking the automated processing of data, and consumers are only able to take enforcement action in relation to a small subset of the provisions.

60 See: https://www.privaworks.com/Details/AlertReference/~/media/Files/DOM_REPUBLIC_LAW.ashx (in Spanish).
61 Pellerano, L., & Pellerano, M. (2016, November 1). Doing business in Dominican Republic. Thompson Reuters Available at http://tmsnrt.rs/2nON3w8 (last accessed 7/7/2017)
62 Web Foundation Research: Interview with César Moline [Online survey]. (2017, March 13). See: Law No. 183-02, which establishes the Monetary and Financial System; Law No. 153-98 on Telecommunications sector; Law No. 55-93 protects the confidentiality of HIV-positive employees; and the General Health Law No. 42-01.
63 Web Foundation Research: Interview with César Moline [Online survey]. (2017, March 13).
64 Open Government Partnership (n.d.). Dominican Republic. Open Government Partnership https://www.opengovpartnership.org/countries/dominican-republic (last accessed 7/7/2017)
65 Privacy International & CIS (2017), State of Privacy India. Privacy International. Available at https://www.privacyinternational.org/node/975#toc-5 (last accessed on 6/7/2017).
66 Web Foundation Research: Interview with Mishi Choudhary [Online survey]. (2017, March 21).
67 Ibid
68 Privacy International & CIS (2017), Op. Cit.
69 Ibid

Due to the lack of comprehensive privacy legislation, India is faced with challenges to ensure the protection of the personal data of its citizens. The obstacles also include the lack of a data protection standard for the public sector and legal recourse in cases of privacy violations, limited public awareness around issues related to the treatment of personal data, and a lack of comprehensive and technically appropriate consent mechanisms. A proposed Right to Privacy Law, which had drafts released in 2011 and 2014, is still under consideration and is viewed as an attempt to address some of these problems. If enacted, such a law would recognise the right to privacy as a fundamental right under the Indian Constitution, create a Data Protection Authority, and provide mechanisms to resolve disputes between individuals and entities handling their data.[70]

4.4 Indonesia

The right to privacy is alluded to in Indonesia's 1945 Constitution through the right to "feel secure" and the right to dignity.[71] Moreover, a 2010 Constitutional Court decision[72] and a 1999 Law on Human Rights[73] affirmed the right to privacy. At the time of writing, Indonesia lacks a comprehensive framework for the protection of personal data even though there are 30 different laws that relate to data privacy. The government has taken steps to correct this through some recent legislative actions but critics claim these changes could threaten to violate freedom of expression and reduce the protections of internet users against criminal prosecution.[74]

The Electronic Information and Transactions Law (Law No. 11 of 2008), which was amended by Law No. 19 of 2016 (the "EIT Law") requires the consent of individuals to use their personal data that has been acquired through electronic media. It also prohibits any individual without the valid rights from attempting to do so or to destroy electronic information that is not his or her personal data.[75] Online companies and platforms (Electronic System Provider, "ESP") must remove content when requested by the person owning the data when done through a court ruling.

In addition, the Ministry of Communication and Informatics (MOCI) submitted the Regulation on Personal Data Protection in Electronic Systems (Data Protection Regulation - DPR, Regulation No. 20 of 2016) in December 2016. This regulation serves to define personal data[76] in relation to the EIT Law and it outlines the scope of the protections provided. Under the DPR, individuals have the right to submit complaints when an ESP does not protect their personal data. These are provided to the MOCI through its Director General of Informatics Application.[77] Individuals can request to see, change and destroy their personal data that is held — giving them control over the use of their personal data.[78] The DPR also requires operators to promptly notify — in less than 14 days — data owners of data breaches with an explanation of causes of the breach. The DPR prescribes administrative sanctions[79] in the event of non-compliance with any of these provisions.

The DPR serves to implement the EIT Law as well as Government Regulation No. 82 of 2012 (GR 82).[80] There is a two-year period to comply with the Data Protection Regulation (DPR) and MOCI will use this transitional period to prepare its implementation and provide further clarification on the new provisions and processes.[81] The coverage of the Data Protection Regulation is international by virtue of implementing the EIT Law, which also extends in coverage beyond Indonesia.

Interviewees and local organisations have suggested the forthcoming data protection law must adhere to international human rights and standards. There are concerns that the current draft laws proposed to implement the DPR may create vulnerabilities and reduced protections for internet users rather than to serve as a legal umbrella to help to better regulate the Internet in Indonesia.

4.5 Mexico

Mexico is among the few countries covered in this study to have a general data protection framework and a designated data protection authority. According to a 2017 briefing on the state of privacy by Privacy International (PI) and Red en Defensa de los Derechos Digitales (R3D), the Federal Law for Protection of Personal Data held by Private Parties (FLPPD or LFPDPPP in Spanish), enacted in 2010, outlines rules, requirements and obligation for companies to ensure the proper treatment of personal data. The law designates the National Institute for Transparency, Access to Information and Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 'INAI') as the authority in charge of oversight and enforcement mechanisms. According to Davara,[82] INAI is known more for data protection than access to information in the public eye. In the event of non-compliance, INAI offers progressive sanctions in the form of warnings and fines. Under the law, data owners have the right to access, rectify, cancel, and object to the processing of their personal information.

The law's coverage is limited to private entities and to the processing of the personal data of Mexican residents by companies operating inside of Mexico.[83] The law does not, however, extend to the processing of data of Mexican residents by companies operating outside of Mexico. Additionally, the Mexican Constitution of 1917 covers the right to privacy and gives Congress the power to protect

70 Privacy International (2017), State of Privacy India. Privacy International. Available at https://www.privacyinternational.org/node/975#toc-5 (last accessed on 6/7/2017).
71 Privacy International and The Institute for Policy Research and Advocacy (ELSAM). (2017, March 14). State of Privacy Indonesia. Privacy International. https://www.privacyinternational.org/node/974 (Last accessed 3/14/2017)
72 in Judgement No. 5/PUU-VII/2010
73 Law no. 39 of 1999 on Human Rights
74 See: http://elsam.or.id/2017/01/amendment-draft-law-on-information-and-electronic-transaction-law-violates-freedom-of-expression/
75 See: http://blog.ssek.com/index.php/2017/02/data-protection-in-indonesia/
76 The Data Protection Regulation defines personal data as "certain individual data which is stored, maintained and kept accurate and the confidentiality of which is protected." "Certain individual data" is defined as "true and actual information that is attached to and identifiable towards, directly or indirectly, an individual."
77 See: http://blog.ssek.com/index.php/2017/02/data-protection-in-indonesia/
78 The Data Protection Regulation defines use as "namely acquiring and collecting, processing and analysing, storing, displaying, announcing, transmitting, disseminating and/or providing access to, and/or deleting personal data".
79 Sanctions include "verbal warnings, warning letters, temporary suspension of business activities, and announcement on online website".
80 Innis, M. (2017, January 25) Indonesia: New Regulation on Personal Data Protection. Global Compliance News. Available at https://globalcompliancenews.com/argentina-regulation-personal-data-protection-20170125/ (last accessed 6/7/2017)
81 Ibid
82 Web Foundation Research: Interview with Isabel Davara [Online survey]. (2017, March 20).
83 Privacy International and R3D (Last modified 2017, June 28). State of Privacy Mexico. Privacy International . Available at https://www.privacyinternational.org/node/972 . Last accessed (7/7/2017)

and regulate the use of personal data held by private entities. Lastly, LFPDPPP incorporates data protection principles that were adopted from the International Standards on Data Protection and Privacy, which are 2009 guidelines approved by the World Anti-Doping Organisation to deal with the handling of personal information.[84]

In a bid to address gaps in LFPDPPP and as part of Constitutional reforms, Mexico now has a new Federal Law on Data Protection for the public sector. According to Recio[85], the General Law on Data Protection Held by Obligated Parties (in Spanish, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados) entered into force in January 2017. It requires that current federal and state laws align with the general law within six months.[86] The enactment of the general law, which follows current international standards and is inspired by the European model, means that the level of protection is on equal footing for the public and private sector. The general law also requires obligated parties to submit data protection impact assessments (DPIA)[87] to INAI, which in turn will issue non-binding recommendations within a period of 30 days.

Though the inadequacy of current surveillance legislation leaves citizens at serious risk of violating their right to privacy (as noted in Risks, above), Mexico is relatively advanced in terms of data protection legislation. The challenge is how to put this better into practice and ensure Mexicans are informed of and leveraging their rights.

4.6 Nigeria

From a legal standpoint, the 1999 Nigerian Constitution safeguards the right to privacy.[88] However, as is the case in Indonesia, there is no comprehensive legislation pertaining to data privacy or personal information protection law. The Digital Rights and Freedom Bill of 2016 is the most recent attempt at such legislation. With respect to data privacy, the bill seeks to "accord data privacy more priority and thus safeguarding citizen sensitive data currently being held by numerous government and private institutions." The bill has gone through a second reading at the House of Representatives and will need to reach a third hearing to be fully passed by the House, and then approved by the Senate and the President to become a law.

Other recent attempts at a comprehensive personal data protection legislation include a draft Personal Information and Data Protection Bill, which was proposed by the National Identity Management Commission (NIMC) in February 2013 and is still pending in the National Assembly. Although the bill has been hailed as a welcome step in protecting citizens against threats posed by modern technologies, the draft bill has several flaws, including its lack of coverage of government agencies, exemptions and some inconsistent provisions.[89]

In the absence of comprehensive data protection legislation, there are industry-specific measures. One such industry-specific regulation is the Consumer Code of Practice Regulations of 2007 issued by the Nigerian Communications Commission ("NCC") - the regulator of the telecommunications industry in Nigeria. According to Udoma & Belo-Osagie,[90] the NCC regulations require that all licences protect customer information against "improper and accidental disclosure" and ensure that such information is securely stored".

The National Information Technology Development Agency (NITDA) has also issued guidelines on minimum data protection requirements for the public and private sectors[91] The NITDA Guidelines, are however, not mandatory and only act as a reference, which is a significant drawback as it leaves open the opportunity for abuse and misuse of personal data.[92]

As the Nigerian telecommunications sector regulator, the Nigerian Communications Commission issued in 2011 the Registration of Telephone Subscribers Regulation (RTS Regulation). The RTS Regulation attempts to protect personal data collected, collated, and managed by telecom companies and relevant independent entities, including the use of fines (up to over US$3,000) for non-compliance. A major concern is that the RTS Regulation, as Oluranti[93] notes, does not treat breaches in data protection measures as a violation of the individual subscriber's right. This in turn, along with fairly limited enforcement mechanism diminishes the data protection potency of the RTS Regulation.

4.7 The Philippines

The Philippines joins Mexico as one of the countries to have dedicated data protection legislation and a regulatory authority. The 1987 Constitution of the Philippines protects individuals against unreasonable searches and seizures, and renders inviolable the privacy of their communication and correspondence.[94] Enacted in 2012, the Data Privacy Act (DPA) established the general rule that

84 World Anti Doping Agency (2015, January) International Standard for the Protection of Privacy and Personal Information. WADA. Available at https://www.wada-ama.org/sites/default/files/resources/files/WADA-2015-ISPPPI-Final-EN.pdf (Last accessed 7/7/2017)

85 Recio, M. (2014, March 14). Mexico's new public-sector data protection law. International Association of Privacy Professionals. Available at https://iapp.org/news/a/mexicos-new-public-sector-data-protection-law/ (Last accessed 7/7/2017)

86 Web Foundation Research: Interview with Maria Solange Maqueo Ramirez [Skype interview]. (2017, March 23)

87 A Data Protection Impact Assessment is defined, in Article 3.XVI of the law, as a "document by which obligated parties who intend to put into operation or modify public policies, programs, systems or computer platforms, electronic applications or any other technology that involves the intensive or relevant processing of personal data, assess the real impacts with respect to a given processing of personal data, in order to identify and mitigate possible risks related to the principles, duties and rights of the data subjects, as well as the duties of the data controllers and processor, provided for in the applicable regulations."

88 Section 37 of the Nigerian Constitution (1999) states: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected," according to Constitution of the Federal Republic of Nigeria (Promulgation) Act, Chapter C23, Laws of the Federation of Nigeria 2004 (as amended).

89 A legal analysis conducted by Article 19 (2013) highlights that the draft bill should be structured in a way to make it more understandable and implementable law; extend in its application to government agencies in addition to targeting the private sector; and clarify how it relates to social media when information is provided for personal purposes as well exemption on the collection, use and disclosure of personal information for journalistic, artistic and literary purposes. See: Article 19 (2013, February 13). Nigeria: Personal Information and Data Protection Bill. Article 19. Available at https://www.article19.org/resources.php/resource/3683/en/nigeria:-personal-information-and-data-protection-bill (Last accessed 7/7/2017)

90 Udoma, U., & Osagie, B. (2017). Data Privacy Protection in Nigeria [PDF]. Lagos.

91 The NITDA Guidelines define "personal data" as: "any information relating to an identified or identifiable natural person (data subject); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address". "NITDA Guidelines", September 2013.

92 Jemilohun, B. O., & Akomolede, T. I. (2015). Regulations or Legislation for Data Protection in Nigeria ? A Call for a clear legislative Framework. Global Journal of Politics and Law Research, 3(4), 1-16.

93 Oluranti, D. (2016, February 9). DATA & PRIVACY LAWS IN NIGERIA. Retrieved March 20, 2017, from http://bit.ly/2lbttcX

94 Privacy International and Foundation for Media Alternatives. (Last updated 2017, March 14). State of Privacy Philippines. Privacy International. Available at https://www.privacyinternational.org/node/969 (Last accessed 3/14/2017)

the processing[95] of privileged information is a prohibited activity unless all parties have given consent prior to the processing.[96] The DPA was put into effect in 2016.

The National Privacy Commission (NPC), which is the agency tasked to administer and implement the law, was appointed in March 2016 following the law's promulgation. According to Commissioner Liboro,[97] the DPA applies to public and private sector bodies. In addition to implementing and enforcing the law, the NPC is tasked with rulemaking, to assist lawmakers in the crafting of privacy related laws (for instance laws around identification), and provides advisory services to ensure compliance from data controllers on issues related to data privacy.

This means that prior to the appointment of the NPC in 2016, there was no government mechanism in place to regulate, monitor and protect data privacy. As a result, data collected by public bodies were subject to weak security measures, which made possible several data breaches over the years.

Looking ahead, the momentum generated by the DPA and a highly ambitious NPC needs to be sustained for continued progress in personal data and privacy protection. As such, the government must ensure that the NPC enjoys full independence and adequate resources to conduct its functions, especially its grievance and accountability mechanisms.

4.8 South Africa

South Africa leads the way on the African continent with a comprehensive privacy law, the Protection of Personal Information (POPI) Act 2013, enacted in August 2013.[98] Moreover, the right to privacy is entrenched in the South African Constitution. According to its preamble, the purpose of POPI, which has been largely modeled on the EU data protection directive, is to regulate "the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests."[99]

However, there has been a lengthy delay in fully implementing POPI. This delay is unfortunate, as it raises serious privacy protection risks. The provisions relating to the establishment of the Office of the Information Regulator, an independent body with national jurisdiction tasked with overseeing and enforcing POPI, are amongst the few provisions that have come into force, and enabled steps to be taken to set up the office. The Information Regulator performs a dual function — it regulates privacy, while also serving as an internal appeal mechanism for access to information requests. In this regard, the Information Regulator's duties include monitoring and enforcing compliance, and handling complaints. Singh[100] suggests that resourcing concerns raised by the state have been partly responsible for inducing the delay, and members of the government have requested that training be provided before POPI is brought into force. The dependence that the Information Regulator currently has on the Department of Justice and Constitutional Development for the allocation of its funding raises doubts about the budgetary independence that the Office of the Information Regulator will be able to enjoy.

The bulk of POPI's provisions, most notably the conditions for lawful processing of personal information, are yet to be brought into force.[101] Though the five members of the Office of the Information Regulator were appointed in October 2016,[102] and the office bearers took office on 1 December 2016, it remains unclear when the remaining provisions of POPI will be brought into force. Once POPI has been brought into force, section 114 still provides for a one-year grace period before POPI needs to be complied with, which may be extended to up to three years. Once POPI is in force, one of the key provisions is that cross-border transfers are prohibited unless the responsible party satisfies certain requirements, such as consent from the data subject, or that the recipient of the information is subject to law, binding corporate rules or a binding agreement that provides an adequate level of protection that is substantially similar to the protections under POPI.

Besides POPI, there are several other pieces of legislation worth noting. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (2002, RICA) is intended to set out a legal process for intercepting communications, including the timing and conditions under which requisite judicial authorisation must be obtained.[103] In such cases, there are concerns about how it properly addresses data protections and privacy. The law imposes a mandatory retention of communication data, and mandatory SIM card registration; users are not notified that their communications have been intercepted, even after the interception activities have been concluded; and service providers are prohibited under RICA from providing information about interception directions.[104] Singh[105] notes that RICA has been heavily, and repeatedly, criticised for being out of date, and for failing to adequately protect users. In April 2017, a court case was brought to challenge the constitutionality of various provisions of RICA, and the Department of Justice has undertaken a review of RICA. Also of relevance is the Cybercrimes and Cybersecurity Bill, which if enacted will also undermine the right to privacy.

The way forward for South Africa with regards to privacy and data protection entails fast-tracking the full operationalisation of the POPI to eliminate gaps in the areas related to privacy and personal data protection.

95 Processing is defined as referring to "any operation/set of operations performed upon personal information including, but not limited to, the collection, recording, organisation, storage, updating, or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data"

96 This held true when the processing is lawful and compliant with existing regulation, the processing is necessary to achieve lawful and non-commercial objectives of the public organisation and their associations, when the processing is necessary for the purposes of medical treatment and ensures an adequate level of protection, when the processing concerns sensitive personal information which is necessary for--the protection of lawful rights and interests of natural and legal persons in court proceedings or the establishment, exercise or defense of legal claims, and when the sensitive personal information is to be provided to the government or public authority (PI & FMA, 2017. Op. Cit.).

97 Web Foundation Research: Interview with Raymund Liboro [Skype interview]. (2017, March 15).

98 UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. New York and Geneva. Available at http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 Last accessed 6/7/2017)

99 Government Gazzette of the Republic of South Africa (2013) Protection of Personal Information (POPI) Act. Cape Town. Available at http://www.gov.za/sites/www.gov.za/files/37067_26-11_Act4of2013ProtectionOfPersonalInfor_correct.pdf (last accessed 6/6/2017)

100 Web Foundation Research: Interview with Singh [Skype interview]. (2017, March 10).

101 Privacy International and R2K (2017, March 14). State of Privacy South Africa. Privacy International. https://www.privacyinternational.org/node/968 (Last accessed 3/14/2017)

102 Ibid

103 Government Gazzette of the Republic of South Africa (2002). Cape Town. http://www.justice.gov.za/legislation/acts/2002-070.pdf (last accessed 6/7/2017)

104 Privacy International and R2K (2017, March 14). State of Privacy South Africa. Privacy International. https://www.privacyinternational.org/node/968 (Last accessed 3/14/2017)

105 Web Foundation Research: Interview with Singh [Skype interview]. (2017, March 10).

05

REFERENCES

- 2016 ID-IGF DIALOGUE. (n.d.). Retrieved March 20, 2017, from http://igf.id/2016-id-igf-dialogue/
- 2017 Corporate Accountability Index. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2nY56Oz
- About Right2Know. (2016, October 03). Retrieved March 20, 2017, from http://www.r2k.org.za/about/
- Adopted Resolutions. (2016, October). Retrieved February 20, 2017, from http://bit.ly/2oH2gNq
- Areas and Projects – Coding Rights. (n.d.). Retrieved March 17, 2017, from http://bit.ly/2nOFMMR
- Asia-Pacific Economic Cooperation. (n.d.). Retrieved February 16, 2017, from http://bit.ly/2nr7IUo
- Broad, E. (2016, March 2). Bringing together privacy and openness: the ODI shares draft personal data principles | News. Retrieved February 16, 2017, from http://bit.ly/24DXiBs
- Brown, D. (2, November 22). New UN resolution on the right to privacy in the digital age: crucial and timely. Retrieved February 19, 2017, from http://bit.ly/2ohnx3E
- Cate, F. H., Cullen, P., & Mayer-Schönberger, V. (2014, May). Data Protection Principles for the 21st Century: Revising the 1980 OECD Guideline[PDF].
- Cavoukian, A., Ph.D. (2012, October). Privacy by Design and the Emerging Personal Data Ecosystem[PDF]. Ontario: Information and Privacy Commissioner.
- Concern over Mexican Constitutional Revisions on Right to Information. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2nzQymU
- Conference Report : The Sustainable Development Goals Center for Africa Conference Expediting the Implementation of Africa's 2030 Agenda [PDF]. (2017, March 13). Kigali: The Sustainable Development Goals Center for Africa.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (1981). Retrieved February 21, 2017, from http://bit.ly/295qEFw
- Cooper , T., & LaSalle, R. (2016, September). Guarding and growing personal data value[PDF]. Accenture.
- Data protection regulations and international data flows: Implications for trade and development. (2016, April). Geneva: United Nations Conference on Trade and Development.
- Digital Equality: An open web for a more equal world [PDF]. (2017). Washington, D.C.: World Wide Web Foundation.
- Digital Rights and Freedom Bill, 2016 [PDF]. (2017, March 20). Lagos: Paradigm Initiative Nigeria.
- Djafar, W., Sumigar, B. R., & Setianti, B. L. (2016). Protection of Personal Data in Indonesia: A Proposal for Policy Institutionalisation from the Human Rights Perspective [PDF]. Jakarta: The Institute for Policy Research and Advocacy (ELSAM).
- Dominican Republic's Community Technology Centers Fight Digital Poverty. (2014, January 20). Retrieved March 19, 2017, from http://bit.ly/2oNXtcW

- Doneda, D., & Varon, J. (2017, March 14). State of Privacy Brazil. Retrieved March 18, 2017, from http://bit.ly/2nHZhXb
- Features of Aadhaar (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oUNOlb
- Focus areas. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2nYco6S
- Gellman, R. (n.d.). Fair Information Practices: A Basic History. SSRN Electronic Journal. doi:10.2139/ssrn.2415020
- Freedom on the Net 2016: Nigeria Country Profile. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oxA03R
- Goodman, B., & Flaxman, S. (2016, June). EU regulations on algorithmic decision-making and a "right to explanation". In ICML Workshop on Human Interpretability in Machine Learning (WHI 2016).
- Gumbus, A., & Grodzinsky, F. (2016). Era of big data. ACM SIGCAS Computers and Society, 45(3), 118-125. doi:10.1145/2874239.2874256
- Indonesia - New Regulation On Personal Data Protection. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oxtvy6
- Jemilohun, B. O., & Akomolede, T. I. (2015). Regulations or Legislation for Data Protection in Nigeria? A Call for a clear legislative Framework. Global Journal of Politics and Law Research, 3(4), 1-16.
- Haynes, B. (2016, March 1). Facebook executive jailed in Brazil as court seeks WhatsApp data. Reuters. Retrieved March 18, 2017, from http://reut.rs/1OOnH3U
- Institute for Technology and Society of Rio de Janeiro (ITS Rio). (n.d.). Retrieved March 19, 2017, from http://bit.ly/2oy0xKS
- Ipsos Mori. (2014). Global Trends 2014. Retrieved March 03, 2017, from http://bit.ly/1kyZ3XA
- Kearney, A. (2014, May). Rethinking Personal Data: A New Lens for Strengthening Trust[PDF]. Geneva: World Economic Forum.
- Kuneva, M. (2009, March 31). Keynote Speech presented at The European Commission Roundtable on Online Data Collection, Targeting and Profiling in Belgium, Brussels.
- Kochi, E. (2016, December 10). How innovation in data generation can contribute to social good. Retrieved March 17, 2017, from http://bit.ly/2ntVh9B
- Lazaro, C., & Le Métayer, D. (2015). Control over Personal Data: True Remedy or Fairy Tale? SCRIPTed,12(1). doi:10.2966/scrip.120115.3Leahy, J. (2015, May 20). Marco Civil hailed as step forward by rights activists. Financial Times. Retrieved March 17, 2017, from http://on.ft.com/2o03MNo
- Ley Telecom. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2nzMxyG
- Marco Civil English Version. (2014, May 27). Retrieved March 15, 2017, from http://bit.ly/1K7dvle
- Martens, C. (n.d.). Legal Resources Centre - [Event] Openness and Accountability Workshop. Retrieved March 20, 2017, from http://bit.ly/2nTanHt
- McKinley, D. T., Dr. (2016, December). New Terrains of Privacy in South Africa [PDF]. Cape Town: Right2Know Campaign and the Media Policy & Democracy Project.
- Media Rights Agenda. Promoting and Protecting Press Freedom and Freedom of Expression in Nigeria. (n.d.). Retrieved March 20, 2017, from http://www.mediarightsagenda.org/activities.html
- Mercurio, R. (2017, April 04). Globe names new IT security head. PhilStar Global. Retrieved April 04, 2017, from http://bit.ly/2nFIR0p
- National Digital Literacy Mission. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oy2yd6.
- National Identity Management Commission. (n.d.). Retrieved March 20, 2017, from http://www.nimc.gov.ng/
- Nigeria: Personal Information and Data Protection Bill. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2nA2tRx
- Nkum, K., Bikwa, O., & Ogbodo, C. (2016). Nigeria's Urgent Data Privacy Law Need [PDF]. Lagos: Paradigm Initiative Nigeria.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (1980). Retrieved February 17, 2017, from http://bit.ly/1gaZQzY
- Official Website of the National Privacy Commission. (n.d.). Retrieved March 20, 2017, from https://privacy.gov.ph/
- Oluranti, D. (2016, February 9). DATA & PRIVACY LAWS IN NIGERIA. Retrieved March 20, 2017, from http://bit.ly/2lbttcX
- Online Privacy. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2n76WQd
- Paradigm Initiative Nigeria. (n.d.). Retrieved March 20, 2017, from https://pinigeria.org/
- Pellerano, L., & Pellerano, M. (2016, November 1). Doing business in Dominican Republic. Retrieved March 18, 2017, from http://tmsnrt.rs/2nON3w8
- Penn, M. (2015, January). Views from around the Globe: 2nd annual poll on how personal technology is changing our lives[PPT]. Davos: Microsoft.
- Policies and Guidelines. (2017, January 09). Retrieved March 20, 2017, from http://bit.ly/2nYeiEA
- Privacy. (n.d.). Retrieved March 20, 2017, from http://fma.ph/
- Promoting a culture of good governance and public accountability in Nigeria. (n.d.). Retrieved March 20, 2017, from http://eie.ng/
- Protection of personal data. (n.d.). Retrieved February 25, 2017, from http://bit.ly/1nN50Ah
- Ramanathan, U. (2016, March 17). Aadhaar bill: With no respect for the law. IndianExpress. Retrieved March 20, 2017, from http://bit.ly/2nzIKS5
- Recio, M. (2014, March 14). Mexico's new public-sector data protection law. Retrieved March 23, 2017, from http://bit.ly/2n76CAX
- Research Projects. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2nY4Gtn

- Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 3(2), 74-87. doi:10.1093/idpl/ips036.
- Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma.[PDF]. Cambridge, MA: Harvard Law Review.
- Solove, D. J. (2008). Understanding Privacy (Chapter One)[PDF]. Cambridge, MA: Harvard University Press.
- Stakeholder Report Universal Periodic Review 27th Session – Brazil: The Right to Privacy in Brazil[PDF]. (2016, September). London: Privacy International, Coding Rights & PrivacyLatAm.
- Stakeholder Report Universal Periodic Review 27th Session – India: The Right to Privacy in India [PDF]. (2016, October). London: Centre for Internet and Society India and Privacy International.
- Stakeholder Report Universal Periodic Review 27th Session – Indonesia: The Right to Privacy in the Indonesia [PDF]. (2016, September). London: Institute for Policy Research and Advocacy (ELSAM) and Privacy International.
- Stakeholder Report Universal Periodic Review 17th Session - Mexico: The Right to Privacy in Mexico [PDF]. (2013, March). London: Privacy International.
- Stakeholder Report Universal Periodic Review 27th Session – Philippines: The Right to Privacy in the Philippines [PDF]. (2016, September). London: Foundational for Media Alternatives and Privacy International.
- State of Privacy India. (2017, March 14). Retrieved March 23, 2017, from http://bit.ly/2nXxNNC
- State of Privacy Indonesia. (2017, March 14). Retrieved March 23, 2017, from http://bit.ly/2o57vcv
- State of Privacy Mexico. (2017, March 14). Retrieved March 23, 2017, from http://bit.ly/2oE4Jcl
- State of Privacy South Africa. (2017, March 14). Retrieved March 23, 2017, from http://bit.ly/2n6JQt3
- State of Privacy Philippines. (2017, March 14). Retrieved March 23, 2017, from http://bit.ly/2iZthLV
- Survey on Data Protection Regime. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oxWwt1
- Taylor, L. (2017). What Is Data Justice? The Case for Connecting Digital Rights and Freedoms on the Global Level.
- The Dominican Republic committed to enact the law on personal data protection as part of its OGP Action Plan. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oUV6oU
- The future of digital trust: A European study on the nature of consumer trust and personal data[PDF]. (2014, February). London: Orange & LoudHouse.
- The right to privacy in the digital age[PDF]. (2016, November 16). New York: United Nations General Assembly.
- Types of Research Methods[PDF]. (2008). Greensboro: The SERVE Center at the University of North Carolina.
- Turow, J., Hennessy, M., & Draper, N. (2015, June). The Trade Off Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation[PDF]. Philadelphia: The Annenberg School for Communication University of Pennsylvania.
- Udoma, U., & Osagie, B. (2017). Data Privacy Protection in Nigeria [PDF]. Lagos.
- Unlocking the Value of Personal Data: From Collection to Usage[PDF]. (2013, February). Geneva: World Economic Forum & Boston Consulting Group.
- Wagner, K. (2015, June 29). Facebook Is Opening Its First Office in Africa. Retrieved March 20, 2017, from http://bit.ly/2n7aGBu
- What we do. (n.d.). Retrieved March 20, 2017, from http://bit.ly/2oy9PK1
- Wells, P. (2016, January 28). Data Privacy Day: can we stop informed consent from being an illusion? | News. Retrieved February 17, 2017, from http://bit.ly/1PDk8hR
- We believe the Internet.. (n.d.). Retrieved March 20, 2017, from http://ictwatch.id/
- Web Foundation Research: Interview with Franklin Akinsuyi [Skype interview] (2017, March 13)
- Web Foundation Research: Interview with Enmanuel Alcántara [Online survey]. (2017, March 21)
- Web Foundation Research: Interview with Peter Ayeni [Skype interview] (2017, March 8)
- Web Foundation Research: Interview with Sam Ayode [Online survey] (2017, March 8)
- Web Foundation Research: Interview with Mishi Choudhary [Online survey]. (2017, March 21)
- Web Foundation Research: Interview with Isabel Davara [Online survey]. (2017, March 20).
- Web Foundation Research: Interview with Wahyudi Djafar [Online survey]. (2017, March 16)
- Web Foundation Research: Interview with Raymund Liboro [Skype interview]. (2017, March 15)
- Web Foundation Research: Interview with Eduardo Magrani [Skype interview]. (2017, March 16)
- Web Foundation Research: Interview with César Moline [Online survey]. (2017, March 13)
- Web Foundation Research: Interview with Jessamine Pacis [Skype interview]. (2017, March 8)
- Web Foundation Research: Interview with Maria Solange Maqueo Ramirez [Skype interview]. (2017, March 23)
- Web Foundation Research: Interview with Gbenga Sesan [Skype interview] (2017, March 8)
- Web Foundation Research: Interview with Avani Singh [Skype interview]. (2017, March 10)
- Web Foundation Research: Interview with Parminder Jeet Singh [Skype interview]. (2017, March 16)
- Web Foundation Research: Interview with Alison Tilley [Whatsapp interview] (2017, March 23)

WORLD WIDE WEB
FOUNDATION

World Wide Web Foundation, 1110 Vermont Ave
NW, Suite 500, Washington DC 20005, USA

www.webfoundation.org | Twitter: @webfoundation