Data Privacy in the Cloud: The Position of Small, Medium and Micro Enterprises Engaged in Mobile Application Development in South Africa

Dusty-Lee Donnelly
ORCID iD: https://orcid.org/0000-0002-5574-7481

Abstract

Rapid technological development challenges the application of privacy laws. Mobile applications' development is a new and rapidly growing field in which a high number of developers are Small, Medium and Micro Enterprises (SMMEs) who may lack the resources and expertise to address privacy issues. Mobile application ecosystems are complex – typically involving use of third-party libraries and cloud-based data storage and back-end services – so creating uncertainty about legal responsibilities for lawful data processing and reporting of data breaches. Mobile applications present a high risk of privacy infringement given the vast amounts of personal data and meta-data that may be entered by application end-users or collected through on-device sensors and the huge number of application downloads. Against this background, the aim of this qualitative preliminary pilot study was to use semi-structured interviews to explore the levels of knowledge, attitudes, practices and challenges of small mobile application developers and entrepreneurs in South Africa to data privacy. This article describes the findings of the study and provides an overview of the requirements of the European General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA), and the principles of privacy by design.

Keywords: mobile applications, data privacy, privacy by design, GDPR, POPIA, SMMEs

Introduction

Mobile applications (apps) present a high risk of privacy infringement. Sophisticated on-device sensors and the huge number of app downloads mean that vast amounts of personal data, including content and meta-data, may be collected by apps and transferred to third parties who may use the data in unexpected ways, without the user's awareness or permission (Van der Sype & Maalej 2014: 25; Breaux *et al.* 2015; Cortesi *et al.* 2015; European Network & Information Security Agency (ENISA) 2018: 12; Razaghpanah *et al.* 2018: 2). The problem has reached public attention through recent data abuse scandals, such as the case of Cambridge Analytica, who used a personality app on Facebook to harvest personal data for voter-profiling and targeted political advertising in Donald Trump's 2016 United States presidential election campaign. The app's privacy policy contained deceptive, false assurances that no personal data was collected, but what truly shocked regulators and the public was the vast scale of the data collection. Approximately 250 000 Facebook users directly interacted with the app, but Cambridge Analytica gained access to the profiles of over 50 million Facebook 'friends' in those app users' social networks (Federal Trade Commission (FTC) [US] 2019: 7). A range of empirical studies have shown that many apps pose a high privacy risk as they fail to provide adequate protection of privacy (Papageorgiou *et al.* 2018: 9391) and users lack adequate understanding of the relative risks associated with the use of these apps (Van Kleek *et al.* 2017: 5208). The presence of third-party trackers was detected in 90% of Android apps, with concentrated data flows being directed to big technology companies such as Alphabet and Facebook (Binns *et al.* 2018: 5).

Mobile app ecosystems are complex – often involving the use of third-party libraries, cloud-based data storage and back-end services. There is a need to address how free and informed consent can be obtained from app users, including how app users can be made aware of parties who have access to and process their data (Office of the Privacy Commissioner (OPC [Canada]) 2012: 4). The involvement of multiple parties creates uncertainty about the legal responsibilities for lawful data processing and reporting of data breaches (ENISA 2018:12). A high number of app developers are based in Small, Medium and Micro-sized Enterprises (SMMEs) and cannot adequately address these issues, as they have 'limited resources and security/privacy expertise' (ENISA 2018:12).

The rapid development of technology and the new uses of personal data are proving a challenge to the application of privacy laws (Organisation for Economic Cooperation and Development (OECD) 2013: 66). This paper adopts the theoretical framework of 'Privacy by Design' (PbD), which is the 'concept of engineering privacy directly into the design of new technologies, business practices and networked infrastructure, in order to achieve the doubly-enabled pairing of functionality and privacy' (Cavoukian & Prosch 2010: 3). Privacy by Design underpins both the General Data Protection Regulation (2016) (GDPR) in the European Union (EU), and the Protection of Personal Information Act (POPIA) (2013) in South Africa.

In the current study, an 'app-developer-centric' approach is taken. Such an approach is described in a recent meta-study, which advocates empirical research to better understand the mobile app ecosystem and how PbD principles can be implemented in the field of mobile app development (ENISA 2018).

The study is an exploratory, qualitative case study of four SMMEs that have developed mobile app as participants at one stakeholder site, being an accelerator program for mobile app developers at an innovation hub in South Africa. The study focuses on identifying their levels of knowledge and attitudes as well as the practices and challenges, in relation to data privacy. The names of the participants, their company, the app, and the stakeholder site are excluded in order to preserve the anonymity of the participants.

This chapter will first review the requirements of the GDPR and the POPIA as well as the principles of PbD. The chapter will then set out the methodology, and results of the empirical study and present an analysis of findings, a conclusion and recommendations.

The Legal Requirements of GDPR and POPIA

In this section the key legislative provisions relevant to the objectives in the field of study are considered. The GDPR came into force on 25 May 2018 – replacing the Data Protection Directive (1995). The GDPR introduced more stringent privacy protections and large penalties for non-compliance. It has extra-territorial application and every entity processing the personal data of EU residents must ensure compliance. The privacy protection advocated for by the GDPR is thus expected to have a significant global impact (He *et al.* 2019:2). Mobile app developers in South Africa need to be aware of and to comply with

its provisions.

In addition, a draft Regulation on Privacy and Electronic Communications (2017) was released on 20 September 2018, with the intention that it will repeal the Privacy and Electronic Communications Directive (2002). The 'e-Privacy' regulation aims to particularise the general principles contained in GDPR by providing specific rules applicable to electronic communications data, which include both the content and metadata processed by mobile applications. However, it has not been adopted and its contents are still being furiously debated.

In South Africa, data privacy is regulated by the POPIA, and from 1 July 2021 app developers must comply fully with its provisions.. At the time of the data collection for this study in 2018, POPIA's commencement date had not been announced. At that time, South African data controllers could voluntarily subscribe to the less onerous privacy principles set out in Chapter VIII of the Electronic Communications and Transactions Act (2002) and only had to provide details on their website of their security procedures and privacy policy when supplying goods or services to consumers by way of an electronic transaction. The interception of the content and metadata relating to communications was (and remains) governed by the Regulation of Interception of Communications (RICA) and Provision of Communication-Related Information Act (2002).

The GDPR was selected for comparison because the legal approach to the right to data privacy is 'broadly similar' in South Africa and in the EU (Roos 2003: 20). Both the POPIA and the GDPR recognise that the protection of data privacy is a fundamental right – enshrined in section 14 of the South African Constitution and article 8 of the European Convention on Human Rights, respectively. The POPIA was drafted after a detailed report by the South African Law Reform Commission (2009) recommended an approach similar to that of the EU (De Bruyn 2014: 1316).

Furthermore, the GDPR has a global reach through its extra-territorial scope (GDPR 2016: art 3.2). Even if an organisation is not a data privacy 'establishment' in the EU (itself a wide concept), it must comply with the GDPR if it processes the 'personal data' of data subjects situated in the EU – i.e. not just EU citizens but all EU residents – in one of two contexts: either it is 'offering goods or services' to such persons (even when free) or it is monitoring the behaviour of such persons.

A South African app developer must comply with the GDPR if the app

will be downloaded by EU residents or will collect the data of EU residents for tracking, profiling or analytics by the developer or a third party. Without an establishment in the EU, such a developer cannot fulfil the provisions for investigation by a single, lead supervisory authority in art. 56 and may thus face multiple investigations by the data protection authorities of various EU member states, subject to sectorial and national legislation (European Data Protection Board (EDPB) 2018:12).

Although, the POPIA has no explicit extra-territorial scope, its provisions apply when personal data are 'entered in a record by or for a responsible party', either if that responsible party is domiciled in South Africa, or if it 'makes use of automated or non-automated means' of processing the data in South Africa (POPIA 2013: sec. 3.1). Arguably, when an app offered by a developer established in the EU is downloaded on a smartphone in South Africa, the processing of personal data by that app constitutes 'automated means' as defined by the POPIA (2013: sec. 3.4). Although the app developer in this instance will be governed by GDPR, the POPIA does not automatically defer to the GDPR, but provides that where other legislation has 'more extensive provisions', those will prevail (POPIA 2013: sec. 3.2.b).

Although similar, the provisions of the POPIA and the GDPR do have some differences that may affect how they are to be interpreted and applied, and this creates an additional layer of complexity in the mobile apps' ecosystem where:

1. legal compliance with the laws of multiple jurisdictions may be required; and
2. the complex architecture of mobile apps typically involves one or more layers of data processing, and cross-border data flows, which must now be contractually managed in a transparent manner.

Legal Responsibility of App Developers

The study sought to determine the attitude of the participants – in particular whether they regarded themselves as having any responsibility for ensuring that third parties processing data of app users do so lawfully. Although there have been numerous studies of consumer perceptions of privacy, there has been very little research on the awareness of and attitudes toward privacy legislation among data controllers (Mikkonen 2014: 191). Furthermore, although several

data protection agencies have published privacy guidelines for mobile apps (OPC [Canada] 2012; FTC [US] 2013; Article 29 Data Protection Working Party (Art.29WP) [EU] 2013; California Department of Justice 2013; Information Commissioner's Office [UK] 2014; Office of the Australian Information Commissioner [Australia] 2014), regulators appear to lack awareness of how developers perceive privacy (Hadar *et al.* 2018: 261). Studies adopting a developer-centric approach (Balebako *et al.* 2014; Jain & Lindqvist 2014; Van Der Sype & Maalej 2014; Hadar *et al.* 2018; Sy *et al.* 2018) indicate low levels of knowledge about privacy legislation, suggesting that PbD may not be a 'viable' approach (Martin & Kung 2018; Hadar *et al.* 2018:278), without informed interventions to change organisational and software engineering mindsets.

Personal data (referred to in the POPIA as 'personal information') includes any information that identifies, or could be used to identify a living, natural person, who is referred to as the data subject. The POPIA extends protection 'where applicable' to existing juristic persons. Personal data includes direct identifiers such as a person's name, an identification number or contact details and attributes about a person such as gender and race. Any information which alone, or in combination with other information, renders a specific person 'identifiable' (POPIA 2013: sec.1; GDPR 2016: art.4) falls within the scope of the legislation. Certain information such as race, ethnic origin, health status and criminal behaviour of a data subject, are treated as special data to which more stringent requirements apply (POPIA 2013: sec.26; GDPR 2016: art. 9 &10). Determining whether one is processing personal data can thus require 'elaborate analysis' – taking into account the specific context (ENISA 2018:14). The term 'processing' is also wider than how a software engineer would typically understand the term (ENISA 2018: 51), and includes collection, storage, transmission, use, linking and deletion of data (POPIA 2013: sec. 1; GDPR 2016: art. 4).

The complex relationships in the mobile app ecosystem must be analysed within the legislative framework of a relationship between responsible party/ies (data controller/s) and operator/s (data processor/s). A responsible party is defined in the POPIA to include any entity (public/private & natural/juristic person), acting alone or jointly, to determine the purpose and means for processing personal information (personal data). In the GDPR, this person is called the data controller. Under both Acts, it is possible that there could be more than one responsible party (data controller). For example, if an

app integrates with login credentials from a third party or with advertising networks, those parties may also be data controllers (ENISA 2018:16).

An operator (processor) is a person who processes personal information for, or on behalf of, a responsible party. This would include cloud service providers, although it has been argued by Kuan Hon (2016) that to classify the following service providers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and pure data storage Software as a Service (SaaS) as processors, is incompatible with the fact that cloud users are not 'instructing' or 'authorising' cloud providers to process data: the cloud service enables the cloud user to access the resources in order to process the data itself.

In accordance with the 'accountability principle', the responsible party (data controller) is responsible for ensuring that processing is carried out lawfully and is required to use contractual means to secure compliance (POPIA 2013: sec.21.1; GDPR 2016: art.28.3). Under the GDPR, a processor is required to take measures to assist the data controller to achieve and demonstrate legislative compliance (GDPR 2016: art.28.2), and to implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk' (GDPR 2016: art.32). The data controller must require 'sufficient guarantees' from the processor that such measures are in place (GDPR 2016: art.28.1). Processing must be governed by a contract binding the processor in respect of the controller (GDPR 2016: art.28.1). Under the PbD principle, controllers must engage trusted third parties – but still have to vet privacy compliance. This would require at least reading a processor's terms and conditions, or privacy policy, to ensure that it deals with the minimum requirements as set out in article 28(3)(a) – (h), including the type of data being processed, and the nature, purpose and duration of processing and the rights and obligations of the controller.

Determining the roles of the various parties is a complex exercise and must be undertaken in the context of a particular app. The literature on the implementation of controls over third-party processors is scarce (Kurtz *et al.* 2018:8). The entity that is developing the app (app provider/app owner) would be the primary responsible party (ENISA 2018: 16). This entity may develop the app in-house, or it may contract an independent app developer to do so. Whether the developer is in that instance a co-responsible party, a processor or not directly regulated, can only be determined in a specific context, having regard to the role that they perform, and whether they are themselves processing any personal data. Nevertheless, the producers of products, services

and apps that process personal data are 'encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfill their data protection obligations' (GDPR 2016: rec.78). This appears to be applicable to app developers (who are not also the app owners), app stores, operating system (OS) providers, library providers, and hardware manufacturers (ENISA 2018: 16). Privacy of personal data in this multi-party environment requires inter-operable and consistent protections to be applied by all stakeholders (Cavoukian 2012: 15).

.

The Practice of Privacy by Design Required by Law

The concept of PbD comprises seven foundational principles (see Table 1, below). The concept was first developed in Canada in the 1990s (Cavoukian 2012: 16). In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a unanimous resolution on PbD (Cavoukian 2011: 6), and the concept has continued to grow in popularity (Martin & Shilton 2016: 201). It acquires its name from the third principle, that privacy is to be embedded into the design of the system. This in turn reflects a change in approach from reactive measures to enforce legal liability after a breach, to proactive measures that consider privacy from the outset of the design process, built into the default settings of the system.

Table 1: The Seven Foundational Principles of Privacy by Design (PbD)

Principle	Description
1. ***Proactive*** not Reactive; ***Preventative*** not Remedial	The PbD approach is characterised by proactive rather than reactive measures.
2. Privacy as the ***Default Setting***	No action is required on the part of the individual to protect their privacy − it is built into the system, *by default*.
3. Privacy ***Embedded*** into Design	PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact.

4. Full Functionality – ***Positive-Sum***, not Zero-Sum	PbD seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, and not through a dated, zero-sum approach where unnecessary trade-offs are made.
5. End-to-End Security – ***Full Lifecycle Protection***	PbD, having been embedded into the system prior to the first element of information being collected, … ensures 'cradle to grave', secure lifecycle management of information, end-to-end.
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***	Its component parts and operations remain visible and transparent, to both users and providers alike.
7. ***Respect*** for User Privacy – Keep it ***User-Centric***	Above all, PbD requires architects and operators to keep the interests of the individual uppermost, by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Source: Adapted from Cavoukian and Prosch (2010: 5 - 6 (e.i.o.))

A PbD approach requires app developers to 'design new applications with privacy in mind right from the outset, and throughout the process and prototyping' (Cavoukian & Prosch 2010: 18). The concept identifies abstract high-level principles, but regulators need specific guidance on expectations in the context of mobile apps (Martin & Shilton 2016: 201), and app developers need the legal requirements to be 'translated' into concrete, context-specific development goals (ENISA 2018: 47; Hadar *et al*. 2018, Omoronyia *et al*. 2013; Sheth *et al.* 2014; Thomas *et al.* 2014).

Article 25 of the GDPR now makes explicit reference to PbD. The article requires that the data controller must 'implement appropriate technical and organizational measures such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner …'. Following a PbD approach, article 25(1) requires that such measures be implemented not only during processing, but even earlier

when the means of processing is first determined. Furthermore, article 25(2) requires that such measures must ensure that 'by default, only personal data which are necessary for each specific purpose of the processing are processed'. Senarath and Arachchilage (2018a) observed that in practice, developers face a 'dilemma' between applying the data minimisation principle and collecting more data to create additional app functionality.

Although the POPIA contains no express reference to PbD, it is apparent from a comparative analysis of the legal requirements that compliance with the POPIA also requires a PbD approach. The eight conditions for lawful processing under the POPIA reflect the same data protection principles contained in the GDPR (Botha *et al.* 2015a: 41). Table 2 (below) presents an analysis by ENISA (2018:22) of the application of GDPR principles in the context of mobile applications. Table 2 (col. 1) has been inserted to show the close correlation between the GDPR and the POPIA. Table 2 (row 8) has been included to show the accountability principle contained in the legislation.

In terms of the accountability principle in both the POPIA and the GDPR, the responsible party (data controller) is accountable for ensuring data privacy and must ensure that the conditions for lawful processing are complied with. Section 8 of the POPIA expressly records that this duty applies both 'at the time of the determination of the purpose and means of the processing and during the processing itself'. This implies a PbD approach.

Secondly, the data minimisation principle restricts how much personal data are collected, processed, stored and made accessible to third parties. Both the POPIA and the GDPR require that data collection be limited to the data that are adequate, relevant and not excessive; in other words, data that are necessary for the specified purposes of processing. Thus, by default, privacy is protected.

Lastly, both the POPIA and the GDPR require that data must be collected for a specific, explicitly defined and lawful purpose. In other words, there must be a legitimate purpose for the data collection. This requires, firstly, that the user be informed of and freely consents to this purpose, unless it is otherwise permitted by statute (POPIA 2013: sec.11; GDPR 2016: art.6), and, secondly, that further processing of data must be compatible with the purpose for which they were collected (POPIA 2013: sec.14; GDPR 2016: art.5.1.b). Aligned to this processing limitation is a storage limitation, in that data must not be kept in a form which permits identification of the data subject for longer than is necessary for achieving the purpose (POPIA 2013: sec.14; GDPR 2016: art.5.1.e). Data should therefore be deleted, or if this is not possible, de-

identified (anonymised), or at least pseudonymised as soon as possible (ENISA 2018: 50).

Table 2: An indicative example of assessing risks with regard to GDPR compliance

POPIA Condition	GDPR Principles	Indicative Privacy Risks	Indicative Requirements
Processing Limitation lawful & reasonable Sec.9 **Openness** Sec.17 & 18 **Data subject participation** Sec.23–25	Lawfulness, fairness and transparency – Art.5(1)(a)	Unlawful, excessive and incorrect processing (e.g. due to permissions to unautho-rised parties to access personal data through the app).	App providers/developers should ensure that they have a legal basis for the processing of personal data. App providers/developers should inform the data subjects properly about their data processing activities. This may help the users to understand what personal data are collected by them and why. App providers/developers should be aware of data subject rights such as rights to access, rectification, erasure, and data portability. They should implement appropriate processes to support these rights. Transparency requires the documentation of processing operations.

Purpose specification Sec.13 **Further processing limitation** Sec.15	Purpose limitation Art.5(1)(b)	Excessive collection and sharing of data (e.g. due to multiple sensors of mobile devices that are activated without need).	App providers/developers should use the data for a specific purpose that the data subjects have been made aware of, and no other without further consent. If the personal data are used for purposes other than the initial purpose, they should be anonymised or the data subjects must be notified and their consent must be re-obtained.
Processing Limitation Minimality Sec.10	Data minimisation Art.5(1)(c)	Excessive processing (e.g. due to use of third-party libraries).	The minimum amount of data for specific processing should be processed by app providers/developers. For instance, they should not store the exact location point when a generic location area is sufficient for their app functionalities.
Information quality Sec.16	Accuracy Art.5(1)(d)	Outdated data pose identity theft risks.	Rectification processes into data management should be embedded in the app design.
Processing limitation retention & restriction of records Sec.14	Storage limitation Art.5(1)(e)	Undue data disclosure (e.g. due to cloud storage services used by mobile	Personal data must not be stored longer than is necessary. App providers/developers should provide the 'right to be forgotten' to the

		app developers).	data subjects. This data must be kept only for a certain period of time for non-active users.
Security safeguards Sec.19 & 20	Integrity and confidentiality Art.5(1)(f)	Unlawful data processing, data loss, data breaches, data destruction or damage.	App providers/developers should ensure that the security requirements of the personal data and the processing systems are met. This encompasses integrity and confidentiality, as well as availability and resilience (Art. 35(1)(b) GDPR). For instance, the appropriate control access mechanisms should be embedded into the apps infrastructure, in order to detect or monitor unauthorised access to the data.
Accounta-bility Sec. 8	Accountability Art 5(2)	The responsible party/controller must ensure that the conditions for lawful processing are complied with.	Use trusted third parties, but verify that privacy policies will be respected.

Source: Col 1. & row 8 adapted from POPIA (2013), Botha *et al.* (2015a: 41); Col 2–4, rows 1–7, drawn from ENISA (2018: 22).

The POPIA and the GDPR are technologically neutral legislation, and refer only to '*appropriate* technical and organizational measures' (e.a.) (GDPR 2016: rec.78; POPIA 2013: sec.19.1). The POPIA (2013: sec.19.1) simply states that such measures must be reasonable. However, the GDPR (2016: art.25.2) sets out four factors that must be taken into account in determining and implementing such measures: 'the state of the art, the cost of implementation, the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'.

Guidelines on best practice for mobile app developers provide examples of how to obtain informed consent (Future of Privacy Forum & Center for Democracy 2011; National Telecommunications and Information Administration [US] 2013). Vague (blanket) consent does not meet the requirement of purpose specification (FTC [US] 2012: 58). Informed consent requires a 'clear affirmative act' (GDPR 2016: art.4.11) and must be preceded by disclosure of a specific, explicit and legitimate purpose (GDPR 2016: art5.1b). Blanket acceptance of general privacy terms does not meet GDPR requirements (Art.29WP [EU] 2017:16). While the challenges of communicating privacy practices on a small mobile screen are widely acknowledged, consent notifications must still be clear, prominent, and delivered at an appropriate time (FTC [US] 2012: 58; GSM Association 2016: 5).

The ability to develop secondary uses from analysis of very large data sets ('big data') presents challenges as to how core data protection principles are applied in practice (Art.29WP [EU] 2014: 2). Innovation inherently involves extracting insights from data that might lead to new uses that were not anticipated at the time of collection. There is extensive debate in the health ethics literature about the adequacy of broad (wide) consent versus blanket consent for future research use of biomedical specimens (Budin-Ljøsne *et al.* 2017:2). Dynamic consent, meaning 'personalised, online consent and communication platforms' that facilitates ongoing communication and user control (*idem* 3) may be informative for privacy researchers in the mobile ecosystem.

Although de-identified (anonymised) data are no longer *personal* data and thus not subject to data privacy laws (POPIA 2013: sec.6.1.b; GDPR 2016: rec.26), there is a blurred boundary between personally identifiable information (PII) and anonymous data (FTC [US] 2012: 2). Anonymisation is described in the literature as 'a process through which identifying information

is manipulated (concealed or deleted) to make it difficult to identify data subjects' (Esayas 2015: 4). Data can be anonymised, for example, by aggregation of data or adding 'noise' (ENISA 2018: 48). However, if there is even a possibility that data can be re-identified to link to an individual, then the law applies (Esayas 2015: 10). Data are not de-identified or anonymous if the means of re-identifying an individual by manipulating the data or linking them to other data is 'reasonably foreseeable' (POPIA 2013: sec.1) or 'reasonably likely' (GDPR 2016: rec.26).

The Regulation on Privacy and Electronic Communications (2017: art.6) requires that electronic communications data (both content and metadata) be made anonymous, unless the purpose of processing cannot be fulfilled by processing anonymous data. The POPIA (2013: sec.14.1) requires that 'data must not be kept in a form which permits identification of the data subject for longer than is necessary for achieving the purpose', for which it was collected and processed. This can be achieved by destroying, deleting or de-identifying a data record (POPIA 2013: sec.14.4).

Pseudonymisation, on the other hand, can be achieved 'by substituting direct identifiers with codes and numbers to prevent an individual being identified' (Esayas 2015: 4). Data have been pseudonymised if technical and organisational measures are implemented to ensure that additional information that could be used to attribute the data to a specific data subject is always kept separately (GDPR 2016: art4). Pseudonymisation of data is specifically encouraged under GDPR (2016: art.25.1) as a practice that can protect privacy – although this does not preclude other measures such as encryption.

Although pseudonymisation is not explicitly referred to in the POPIA, it is a PbD practice that may be used to achieve the privacy objectives of a responsible party. However, parties subject to the POPIA are considerably constrained in their ability to use pseudonymised data, by the requirement in section 14(4) that the data be deleted or de-identified (which by definition requires deletion of any information that could reasonably be used to re-identify an individual) once the responsible party is no longer authorised to retain the data. Consent to retain the data in a pseudonymised form for a longer period, would be required.

Challenges Facing SMMEs in Data Privacy Protection

Within this already complex field, this empirical study sought to examine the

challenges experienced by SMMEs. In addition, current legislation was analysed to determine whether there were any provisions that took into account the position of SMMEs.

The GDPR (2016: rec.16) encourages regulators to 'take account of the specific needs' of SMMEs. GDPR also adopts a risk-based approach to exemptions, rather than providing a blanket exemption to all SMMEs:

- An SMME with fewer than 250 employees is exempt from record-keeping requirements, unless the processing it performs is routine rather than occasional, or concerns special personal data, or is 'likely to result in *a risk* to the rights and freedoms of data subjects' (GDPR 2016: art.30.5) (e.a.).
- A privacy impact assessment is only required before processing data 'likely to result *in a high risk* to the rights and freedoms of natural persons' (GDPR 2016: art.35.1) (e.a.).
- Data breaches do not need to be reported to the supervisory authority if the data controller can show that it is 'unlikely to result in *a risk* to the rights and freedoms of natural persons' (GDPR 2016: art.33.1) (e.a.)
- Data breaches need only be reported to the data subject if it is 'likely to result in *a high risk* to the rights and freedoms of the natural person in order to enable him/her to take the necessary precautions' (GDPR 2016: art.34.1).
- A data protection officer is only required when the controller's core activities involve 'regular and systematic monitoring of the data subjects on a large scale' or the processing of special personal data 'on a large scale' (GDPR 2016: art.37.1).

Whether these provisions will achieve the desired effect of meeting the needs of SMMEs, is open to doubt. First, the terms 'a risk', 'a high risk' and 'large scale' monitoring are not defined and require expert analysis in any particular context. While presented as a cost-saving measure, in reality owners of small businesses will have to perform the same risk assessments without access to expert knowledge.

In South Africa, the POPIA applies to all entities processing personal information. The Act does not include risk-based exemptions. This makes the debate about developing a regulatory response that accommodates the position of SMMEs particularly relevant in South Africa.

Although compliance with privacy legislation is recognised as imposing a significant regulatory burden on data controllers, it also provides an opportunity to build consumer trust and thus boost business success (Mikkonen 2014: 192). In one study, apps with missing or inadequate privacy policies were found to be less popular in the Google Play Store (Papageorgiou *et al*. 2018: 9394).

Methodology

This was an exploratory (pilot), qualitative case study undertaken with ethical approval and with written gatekeeper's permission and informed consent of participants. The stakeholder site was purposively selected, because their program has had a successful, government-supported program in operation since 2012, providing entrepreneurial support focused specifically on the target population: small app developers and entrepreneurs developing a mobile application.

Using a census approach, all graduates were invited to participate. Semi-structured, in-depth interviews of approximately 60 minutes each were audio-recorded, professionally transcribed and then thematically analysed by the researcher and a co-coder – using Nvivo (version 12) software. An in-depth, semi-structured interview was also held with the CEO at the stakeholder site, as being a key informant providing insights into the stakeholder's perspectives and understanding of data privacy.

The findings were triangulated with document analysis of the participants' privacy policies and artefact analysis of the mobile app permission settings. Each app was downloaded on an Android smartphone, and a user account was created. Screenshots were taken to record the permission settings and privacy policy available to the app user. The participants were all either unwilling or unable to supply copies of contracts with third-party cloud service providers for inclusion in the analysis.

To preserve confidentiality and anonymity, the names of the participants, their businesses, and their apps, were excluded from the published findings.

Research Design and Limitations

The stakeholder site was based in Pretoria, although it accepts participants for

its accelerator program from throughout South Africa. The site was thus regarded as sufficiently representative of a cross-section of experiences of small, mobile app developers in South Africa. Study participants were based in Pretoria, Johannesburg and Cape Town.

An additional stakeholder site, a technology start-up incubator in Durban, was identified using snowball sampling but was excluded from the research findings. From nine potential participants only two were available for an interview within the study time-frame but did not meet the participation criteria. The first respondent had developed a web-based app only and this study was limited to apps for personal handheld devices such as smartphones, and available for download on the Google Play or Apple App stores. The second respondent was no longer a small business as it had grown to more than 50 employees (National Small Enterprise Act 1996: sch.1) and had moved its registration offshore.

The aim of the study was to sample to redundancy; however, the sample size was limited by a low response rate. The invitation to participate was sent to 47 start-up organisations. Representative from four start-up organisations responded indicating a willingness to participate. The response rate was 8.5%. The study findings are thus not capable of generalisation, but this was undertaken in August 2018 as a preliminary pilot study that formed part of PhD research. The expansion of the study to additional stakeholder sites, and a follow-up study employing a national survey of app developers met similarly low response rates in 2019 and could not be completed in 2020 due to the national state of emergency in response to COVID-19. A revised follow-up study is planned for 2022. As further publishable work is some years away, the results of the preliminary pilot study are regarded as important for distribution in the public domain on the eve of the commencement of the POPIA on 1 July 2021, as they highlight a critical lack of awareness around data privacy that merits immediate attention from the Information Regulator, and industry stakeholders.

The use of in-depth interviews was integral to the research design. Although it required a significant time commitment from participants, which may have reduced the response rate, it provided rich data. One-on-one interviews provided an intimate conversational setting to foster maximum trust and encourage frank disclosure by participants.

An inter-disciplinary study which subjected apps to static and dynamic analysis to identify vulnerabilities, detect communications between the app and

third parties, test the security of data transmissions, and identify the content of data packets, could provide more detailed insight into the privacy and security risks posed by the apps (Papageorgiou *et al*. 2018: 9393). It could also provide the basis for a follow-up study to determine what app developers could do differently to better protect the privacy of the personal data of app users.

Results and Discussion

This section first provides a summary of the participant demographics, business profiles and apps encountered in the study. It then presents the results of the qualitative analysis of interview transcripts and discusses those findings.

Participants' Profiles

In terms of the participation criteria for the study, participants had to be either a mobile app developer or an entrepreneur who owns a company developing a mobile app, or both. All the participants were entrepreneurs, but only one was also a mobile app developer. All were males. Three were black and one was white. Three were aged between 35 to 45 years while the fourth participant was between 25 and 35 years. . All had attained at least an undergraduate degree. However, only one participant had a formal qualification (or training) in app development. He reported that he had not covered data privacy in his studies, that he employed other developers and had not written the code for the app discussed as part of the study.

The study sought to explore the relationships between app developers and companies developing the app. The study revealed an interesting dichotomy between the views of these two types of participants. On the one extreme was an entrepreneur who took the view that the app developer was responsible for data privacy. He had outsourced the app development to an independent developer (whereas all other participants had developers as business employees or partners). He described the situation thus:

> *Because even on the app when you go to the app store, it says 'this app is developed by [Name of Developer]', So it doesn't say it's developed by [Name of Participant]. So, it means they are responsible for it.*

The same participant had almost no knowledge about what data the app was

actually collecting, saying 'the developer can tell me, I don't know'. Nor had the participant had any discussion with the developer about which third parties might have access to the data or where the data would be stored:

> *I don't know, it's just a cloud. That's what the developer told me, he said, 'no, we're using [a] cloud'.*

When probed about the issue he recalled an email from the developer listing third-party software being used in the app but added that he had 'no idea' who these people were or what their role was. When asked if he had any responsibility to ensure that these parties, if accessing the data, did so lawfully, his response indicated mixed feelings – on the one hand shifting responsibility to the developer and on the other hand expressing doubt about what steps he should take himself.

In contrast, the one participant, who was an app developer, placed responsibility for data privacy with his client, and accepted responsibility only for maintaining confidentiality in respect of data accessed by his company or employees. He did so on the basis that his company was not hosting the data and back-end application. The interview also established that he had no insight into the contracts between the client and other service providers. Nevertheless, as the party responsible for the design of the system, it was notable that when asked if he had any data privacy goals in mind when developing the app, he candidly replied: 'Not at all'. When the issue was probed further, he further added:

> *We focus on developing solutions and systems. We don't prioritise [the] privacy of our users.*

The above examples serve to illustrate the limitations of privacy risk assessments conducted by individual entities, and the need for privacy to be assessed in 'a holistic, ecosystem-wide manner if it is to be both effective and lasting' (Cavoukian 2010: 7).

Business Profiles

The study was restricted to businesses that are small enterprises, by reference to having less than 50 employees in terms of the Schedule to the National Small

Enterprise Act 102 of 1996. The businesses were all formally registered private companies but ranged in size: two employed less than five employees (including the owner), one employed six to nine employees and one employed 10 to 49 employees. In addition, all participant businesses potentially met the criteria as exempt micro enterprises, having an annual turnover of less than R10 million in terms of the amended Information and Communication Technology (ICT) Broad-based Black Economic (B-BEE) Sector Code (RSA 2016)

App Profiles

The study was further restricted to businesses developing one or more mobile apps for personal handheld devices. The study classified businesses to one of the following stages:

a. Start up – concept successfully pitched to incubator or funder;
b. Pilot – app is currently being piloted/completed pilot testing pre-market launch;
c. Commercialised – first sales after successful market launch; less than one year in operation; and
d. Scale – developed further apps, markets, or significantly increased turnover, and more than one year in operation.

All the apps had been commercialised and were available on the Google Play Store for download on Android devices, and one app was also available on the Apple App Store. However, none of the apps had reached a stage of scale – having only about 50 to 100 downloads each. The reasons for this were reported as being due to secure business partner or client buy-in.

The study did not focus on one particular app category. The stake-holder site-selected program entrants were based on the potential social impact of the app concept, but the apps involved in the study had diverse classify-cations on the app store: education, retail, government services, and social.

All the apps were available as free downloads and thus, unsurprisingly, two of the four participants planned to monetise the data itself (in anonymised form) as a revenue generating mechanism. A third participant's business model was still in its infancy, but he anticipated integrating the app directly with financial services' companies. When probed on this issue, he realised –

apparently for the first time – that this would raise concerns about whether those companies would also use the data of app users for other purposes, for example for targeted advertising. The fourth app provided government services and collected sensitive data, and for this reason it was hosted on government servers, and the privacy of the app data was controlled by requiring all employees with access to the data to sign confidentiality agreements.

Knowledge about Privacy Laws

Although all participants claimed knowledge about data privacy with varying degrees of confidence, they had no or very limited knowledge of the specific requirements of data privacy legislation. An empirical study by Botha *et al.* (2015b: 7) showed that South African SMMEs were not yet compliant with the POPIA, chiefly due to a lack of awareness.

Two participants were unaware of the existence of specific laws governing privacy and could not name the legislation – but displayed markedly different degrees of confidence in their level of knowledge. The first particularly confident response, claimed full awareness:

> *I am fully aware of it and it's a recent one anyways. But even … I mean with the recent one, it's just because of the Facebook case [involving Cambridge Analytica]. But other than that, my knowledge when it comes to data is that the guy who develops the app has the data, ok. But I think [The Stakeholder] told me that no, it will be my responsibility eventually, so I'm still trying to figure it out how am I going to own it.*

In contrast, another participant expressed considerable doubt about their knowledge of data privacy laws:

> *Um not really, not much. Not … just, just … you know, like for example, what I understand about, about the privacy is that, for example, like you … like you're not allowed to advertise to kids [minors], right? … So, I guess I will have to read … Is there an actual Act that is…?*

The other two participants knew about the existence of the legislation and some key data protection principles but claimed a lack of knowledge about the specific provisions. For example, the third participant reported that the

company intern was tasked with drafting a report on the differences between the POPIA and the GDRP – with the aim of 'trying to see what were the big differences'. However, when probed on this point, the participant admitted that they had not done anything about it:

> *No, I read quickly the notes, I just filed it for the next time. I am meeting the lawyers, uh, I didn't see anything that was really concerning for the moment; I had a look, but not properly, at it*.

Interestingly the participant recorded the rationale for this exercise to be they would implement 'the higher standard', which they assumed to be the European standard. Although there is considerable overlap as the same data privacy principles underpin the legislation, there are also differences. In some respects, the POPIA imposes a higher standard. For example, the POPIA applies to the data of juristic persons as well as natural persons. This participant's response thus brings to the fore the concern raised by several other participants and the key informant – that it is very difficult to comply with different legal standards. The GDPR has extra-territorial application, and thus a South African app developer who is processing the personal data of any resident of the EU would be governed by both the POPIA and the GDPR. This same participant said of his compliance with data privacy laws:

> *It's very easy for me to say that we [are] compliant because our terms and conditions were written by professional lawyers that know what they are talking about. I have absolutely no clue what are in the terms and conditions; I just make sure that I comply.*

What emerged from the interviews was that participants were either unclear about what a privacy policy should contain or were unaware of what their own privacy policy did contain. A document analysis of the privacy policies of the developers revealed that the terms and conditions were generic and did not comply with requirements of the legislation.

Attitudes towards Privacy Laws

All participants expressed high levels of concern about data privacy compliance and a desire to learn more about how to comply with the law.

However, their attitudes towards data privacy are best described as mixed. All participants expressed a desire to ensure users gave informed consent and a desire to learn more about how to comply with privacy laws (which were coded as positive attitudes). However, they expressed mixed feelings when discussing the importance of privacy compared with other priorities, principally the need to focus on how the app functions and the need to monetise the app. For example, one participant stated that:

> *… data is a, or at least the privacy of the data, is a big concern for us and we wanna [want to] make sure that we use it correctly, protecting the privacy of the [identified App user] that [who] are our customers, uhm, but at the same time being able to use the data to have a financially sustainable business model.*
> …
> *I mean data privacy is of course important but the latency is as important, and if my app is uh too slow, no one will use it. So, I won't even have an issue about data privacy, because I won't have any data.*

This same user raised the issue again, when discussing different cloud services:

> *Alibaba[.com] has a kind of radical view on data privacy saying that if they have the same rules as there are in Europe, your [their] service would not exist and there wouldn't be any convenience for the user.*

Some participants showed concern about the fact that the legislation may expose them to sanctions and expressed the view that as small businesses they needed to be 'protected' from the legislation. Views expressing the attitude that participants would comply with privacy laws to avoid prosecution, were also coded as mixed. Furthermore, all participants expressed mixed attitudes on the issue of whether the participants had any responsibility to ensure that third parties given access to the data only used the data for a lawful purpose. This is discussed further in relation to the practices employed in relation to privacy (below).

Practices Employed in Relation to Privacy

Privacy by Design was not a practice implemented by any of the participants.

Although all participants were already at the stage of commercialisation, the view expressed was that privacy was 'not really a concern right now' and that they could 'sort it out when the time comes'. As one participant put it:

> *No. All I wanted was to see the app working (laughter). Believe you me, all I wanted to see was the app working.*

The same view was expressed in one way or another by all the participants, and none reported undertaking a privacy impact assessment, or mapping data flows and risks of data leakage. None reported having obtained legal advice specifically related to compliance with privacy legislation; this was related to the high cost of quality legal services, which was mentioned by all participants.

The study aimed to explore which third parties might have access to the app data, but three out of the four participants could not explain clearly who would have access to the app data, and in one case, a participant was unaware of who was hosting the app and whether the data was being stored in South Africa. The term 'trust' or variants such as 'believe', were raised by all participants to describe their relationship with third parties, who might have access to app data. One participant expressed it thus:

> *To be completely honest with you, I trust them to follow the rules …. And that's why we haven't checked …*

Prompted for further disclosure, the participant indicated:

> *So, basically, I wouldn't like Google Cloud or Alibaba[.com] to access our information and then to sell this information to someone else, because that's what I'm planning to do. … But my first thought is that they [Google Cloud and Alibaba.com] are compliant with any data privacy rules.*

Another participant expressed the view that using Google and other 'big companies' was the best means of protecting app data:

> *I mean it's something that we think about. We can only hope and obviously, uhm trust that since they're a big company and they are up there with top officials, you know, of any government – uhm, it would*

> *be used to protect all our data.*

When probed as to whether he had ever checked the terms and conditions, he admitted that he had not:

> *Can I be honest? … You know we all just click, uh, without reading the terms and conditions. I don't know when the last time was [that] I read privacy policies.*

Only one participant reported reading the terms and conditions of the app store but reported that he 'wouldn't know' if app stores were able to process the content of app data, although the terms and conditions stated that the app store simply hosts the 'lining' of the application.

When prompted with the question of whether the development process includes steps to restrict data collection, it appeared that generally the opposite approach is taken. The stakeholder interview also flagged the issue:

> *We haven't come across directly where it's about the user data being sold, it's about using that data to create a hypothesis or a tool or a utility … by design, the notion is not what you need for this version, but always collect as much as you can ...*

The stakeholder is also aware of the privacy risks, and appropriate privacy practices, but reported the view that this was not how things are generally being done:

> *… by design should it [personal data] come in and immediately [you] anonymise it and you only work with that data … But I think what's happening at the moment, people are using that single raw pool of data to do things on top of it. So there's always risk. You've created a door into the data …*

Challenges Experienced in Relation to Privacy

Three challenges were reported by all participants. First, they reported challenges complying with the requirement of meaningful consent. Second, they reported that it was difficult to obtain affordable and adequate legal

advice. Last, they reported a need for education and training. The concerns facing the participants in this study related to complex challenges posed by inter-operability of systems through Application Processing Interfaces (APIs) and how to de-identify (anonymise) or pseudonymise data. A study of free education and training resources about the POPIA, which are available online, showed that while they were useful for raising awareness and general education, they did not replace the need for specific, expert advice (Botha 2015a: 49).

The requirement for user consent was experienced as challenging because of the difficulty in explaining how the data were used, and conversely because it might 'scare' users provide the full information. The challenge was linked to the lack of an adequate privacy policy, and in turn to the lack of awareness and lack of access to expert advice. Figure 1 (below) shows that although all participants claimed to have a privacy policy, some were not available to app users, and none adequately complied with the privacy legislation.

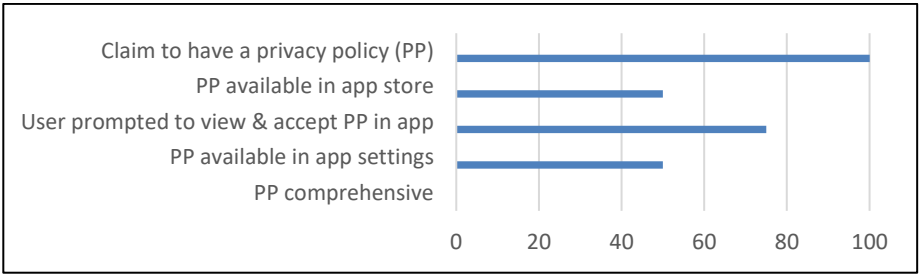

Figure 1: Participant use of privacy policies

Privacy Analysis of App 1

One participant had already resolved that because of the problems created by users reading his terms and conditions and deciding not to install the app – on the next upgrade he was going to 'hide them with that small print'. He claimed to have terms and conditions that were 'generic', but which had been drafted on a *pro bono* basis by a law firm in Sandton. Artefact analysis of the app demonstrated that the app user is required to create a profile with their name and surname (but no password) and the terms and conditions are then automatically displayed, requiring the user to scroll through several screens and mark a check box at the end to 'accept'. To complete the sign-up process,

and before using the app, the user is then required to enter especially sensitive data, including their identity number, date of birth, gender, marital status and information from which the app user's race and ethnicity can be identified.

Upon download, the app asks the app user to deny or allow the app permission to 'access photos, media and files on your device'. The app can still be used without enabling this permission, but some functions will not be available. Additional app permissions in the app info, viewable in the Play Store, indicated that the app can also access contacts, location (approximate and precise GPS location), phone (read phone status and identity, directly call phone numbers) and SMS, which have been flagged in prior research as dangerous permission settings (Papageorgiou *et al*. 2018: 9394), and should have been explained in the app's privacy policy.

When the terms and conditions of this app were reviewed, it was unsurprising that the participant reported that many potential app users had been deterred from downloading the app. The terms were poorly drafted, containing incomplete sentences, grammatical errors and repetition. To confuse matters further, the developer's privacy policy viewable in the app store had a completely different set of terms and conditions related to a different business.

Analysis of the privacy policy showed it to be completely inadequate, even for bare compliance with the legislation. Two sections referred to in-app purchases and subscriptions respectively, and links after each section for 'full disclosure' were broken and provided no additional information. The interview also clarified that both sections were inapplicable, as the app was a free download with no in-app purchases or subscriptions. The terms then contained a section on content, informing the user 'you are responsible for the content created and shared'. No details were provided of what data were collected by the app and how it was processed.

Privacy Analysis of App 2

The terms of another app's privacy policy informed the app user:

> *It is solely the responsibility of the user to protect your privacy.*

This is completely at odds with the PbD principle that a user's privacy should be protected by default – even if the app user does nothing. Not only was this statement incorrect according to the law, but the privacy policy was outdated

as it informed users that they could choose to use the app anonymously. In the interview it was established that version 1 of the app collected the user's telephone number and device details to permit the creation of a permanent identifier that would enable user interaction with the app to be tracked to a particular user – even if they uninstalled the app and downloaded it again. In version 2 of the app, anonymity was impossible as the app required registration with personal details.

This privacy policy informed users that their information might be disclosed to 'internal and external parties for the purpose of the service', but did not identify those parties or purposes. It then sets out a potentially confusing assurance that the app user data will not be sold or shared with third parties, unless requested by the app user.

The primary parties to whom the data are transmitted by the app, and the purpose of the data collection, are set out clearly in the details about the app in the app store but are not repeated in the privacy policy. The permissions listed in the app store indicate that the app has access to the device's camera, contacts, location and calendar, but this is not explained in the privacy policy. Access to the calendar states that it includes permission to read calendar events and confidential information, to modify and add events and send emails to guests without the user's knowledge.

No further information is provided in the privacy policy about further processing, or about how the transmission, storage and privacy of the data are secured. The interview also established that the data were being used for forecasting and analysis – but did not establish whether the data were de-identified. The interview also established that the data were being hosted by an external service provider, in terms of an expired contract. The developer was not privy to any contracts with third-party processors.

Privacy Analysis of App 3

The privacy policy sets out in clear and understandable language the general types of personal data collected, the purposes of collection, and how the data are secured. The policy indicates the general categories of third parties who may receive personal information, the reasons for this and alerts the user that some processing may take place outside South Africa but does not state where. As the privacy policy is a general policy applicable to the app developer's websites and products, it is a good illustration of the limitations of privacy

policies in providing specific information about an app. The policy does provide an email point of contact for further queries on the privacy policy.

The app is educational and will be used by children. The privacy policy did not deal with the issue of parental consent – stating only that the developer does 'not publish content that is targeted at children' and will 'not knowingly collect personally identifiable information from children under the age of 13 years'. In South Africa, the age of consent is 18 years (POPIA 2013: sec.1) and processing requires the prior consent of the child's parent or guardian (a 'competent person') (POPIA 2013: sec.35.1). In the EU the general age of consent is 16 years, although the member state law can lower the age of consent but not to below 13 years (GDPR 2016: art8.1). In the app, a year of birth is required to access certain 'parents' only' areas.

Furthermore, app users are assured that the developer will not sell or share their personal details with anyone, but the privacy policy later recorded that 'occasionally' data may be shared with external companies for marketing their products and services by post, unless the user opts out. Users are directed to the developer's website to update their profile and subscriptions, but no website address is provided.

Therefore, this privacy policy was not regarded as dealing comprehensively with all privacy issues.

Privacy Analysis of App 4

The fourth participant, discussing informed consent, responded that:

> *My first concern is that I respect my users; I use the data [and would like] that they are fully aware that I'm using [it] and that they feel good about it.*

In the same interview, when probed further on how informed consent would be obtained, the participant responded:

> *I think that won't be a problem because people don't read this type of thing, but I want our users to fully understand that if we give them a service that is cheap for them it's because we use the data. It's because we use the data to sell services to brands and I don't want to hide that from them. I want them to understand that it's a free service because*

> *we can sell some ads [advertisements] on it and I want them to be fully aware of that, and I want to understand if that's a problem for them or not … that's mainly our concern – how do we present that to our users [so as] not to scare them? …*

The participant indicated in the interview that their terms and conditions will be freely accessible on their app and that he would have 'no problem' sending them to the researcher. The use of future tense was not probed in the interview, but subsequent analysis of the app indicated that users installing the app must register by supplying a phone number, creating a password and checking a tick box indicating 'I have read and accept the T&Cs (terms and conditions) of use of XXX app'. However, there was, no link to the terms and conditions. The developer did not list a privacy policy in the relevant app store or anywhere in the app settings. A follow-up email to the participant enquiring about these matters went unanswered.

Conclusion and Recommendations

Although a technical study such as that by Papageorgiou *et al*. (2018) would be needed to accurately determine the risk posed by individual apps to the privacy of app users, this study did demonstrate that app developers and entrepreneurs developing mobile apps are neither sufficiently aware of, nor compliant with the legislative requirements of the GDPR and the POPIA. The key findings of the study were that all participants:

1. Had no or very limited knowledge of data privacy legislation;
2. Expressed high levels of concern about data privacy compliance, but responder bias was likely, as low overall participation rates suggest that data privacy is not a high priority for SMMEs engaged in mobile app development;
3. Reported relying on 'trust' of third-party providers and employed no measures to vet privacy compliance; and
4. Reported challenges complying with the requirement of meaningful consent.

While the study sought to investigate specific strategies and tools being employed by app developers to address privacy in the design of their mobile

apps, the participants did not report any comprehensive information on the available strategies, suggesting that they lacked sufficient knowledge about the existing technology. Likewise, where third parties were involved the participants were not taking steps to identify those third parties, to verify what data those third parties were collecting from the app, and to ensure that contract terms provided sufficient protection of the privacy of app user data. On the contrary, participants reported that they relied upon 'trust' of third parties but did not report using any strategies to verify that their trust was well-placed, such as contractual guarantees, privacy certification, privacy risk assessments or a data management plan. In short, PbD is not an approach that was being implemented by these developers. On the contrary, privacy is regarded as an issue that can be addressed after successful commercialisation of the app.

Despite all the participants being aware of the need to obtain consent from users, the findings suggest that app developers need to know more, in practical terms, about how to obtain meaningful consent from app users. At the simplest level this involves being in a position to draft appropriate privacy policy terms. However, more complex concerns involve how one deals with sensitive data, data of minors or anonymised data. The findings suggest a need for detailed guidance for app developers on these issues. These findings cannot be generalised due to the small sample size. However, they are consistent with earlier studies in other jurisdictions. The findings point to the need for a wider study of these issues in South Africa, to better understand the awareness, attitudes, practices and challenges of app developers, and to isolate issues that may be unique to SMMEs. As further publishable work will only be publishable in years to come, the results of the preliminary pilot study are important to be shared in the public domain as soon as possible, as they highlight that app developers in South Africa may have a critical lack of awareness around data privacy that merits immediate attention from the Information Regulator and industry stakeholders.

The Information Regulator (2021) published a guideline for the development of Codes of Conduct in terms of sec.65 of the POPIA. However, mobile app developers do not work in a sector with a representative regulatory oversight body that could develop such a code. Based on the findings of this study it is recommended that the Information Regulator in South Africa:

1. Introduces appropriate training and education materials for app developers on privacy requirements;

2. Develops or endorses suitable guidelines on best practice for app developers;
3. Ensures that such guidelines contain clear, explicit requirements, with steps for evaluation and appropriate software engineering techniques (Senarath & Arachchilage 2018b); and
4. Engages all stakeholders in the mobile ecosystem, including platform providers, OS providers, hardware manufacturers, advertisers and other third parties, on means to best secure the privacy of app users.

Acknowledgements
The author gratefully acknowledges the app developers and entrepreneurs who have taken part in the study to date. The financial assistance of the National Research Foundation (NRF) is hereby gratefully acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not to be attributed to the NRF.

References

Article 29 Data Protection Working Party (art29WP) [EU] 2013. *Opinion 02/2013 on Apps on Smart Devices*. WP202. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (Accessed on 17 May 2021.)

Article 29 Data Protection Working Party (art29WP) [EU] 2014. *Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of their Personal Data in the EU.* WP221. Available at: https://www.pdpjournals.com/docs/88352.pdf (Accessed on 17 May 2021.)

Article 29 Data Protection Working Party (art29WP) [EU] 2017. *Guidelines on Consent under Regulation 2016/679*. WP259. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (Accessed on 17 May 2021.)

Balebako, R. *et al 20*14. The Privacy and Security Behaviors of Smartphone App Developers. Workshop on Usable Security (USEC 2014), San Diego, 2014. Available at: https://www.researchgate.net/publication/269197012_The_Privacy_and_Security_Behaviors_of_Smartphone_App_Developers (Accessed on 17 May 2021.)

Binns, R. *et al* 2018. Third Party Tracking in the Mobile Ecosystem. Paper presented at Proceedings of the 10th ACM Conference on Web Science. Available at: https://arxiv.org/pdf/1804.03603.pdf (Accessed on 17 May 2021.)

Botha, J. *et al* 2015a. Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa. In Zaayman, J. & L. Leenan (eds.): *Proceedings of the 10th International Conference on Cyber Warfare and Security ICCWS-2015.* Reading: Academic Conferences. Available at: https://researchspace.csir.co.za/dspace/handle/10204/8299 (Accessed on 17 May 2021.)

Botha, J. *et al 20*15b. The Effects of the POPI Act on Small and Medium Enterprises in South Africa. In Venter, H.S., M. Loock & M. Coetzee *et al.* (eds.): *Proceedings of the Information Security of South Africa (ISSA) 2015 Conference*. Johannesburg: ISSA. Available at: https://doi.org/10.1109/ISSA.2015.7335054 (Accessed on 17 May 2021.)

Breaux, T D. *et al* 2015. Detecting Repurposing and Over-collection in Multi-party Privacy Requirements Specifications. Paper presented at 2015 IEEE 23rd International Requirements Engineering Conference (RE). Available at: https://doi.org/10.1109/RE.2015.7320419 (Accessed on 17 May 2021.)

Budin-Ljøsne, I. *et al* 2017. Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research. *BMC Medical Ethics* 18,4: 1 – 10. Available at: https://doi.org/10.1186/s12910-016-0162-9 (Accessed on 17 May 2021.)

California Department of Justice (CA AG) 2013. *Privacy on the Go: Recommendations for the Mobile Ecosystem*. Available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf (Accessed on 17 May 2021.)

Cavoukian, A 2011. *Privacy by Design Strong Privacy Protection – Now, and Well into the Future a Report on the State of PbD to 33rd International Conference of Data Protection and Privacy Commissioners.* Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf (Accessed on 17 May 2021.)

Cavoukian, A 2012. *Privacy by Design and the Emerging Personal Data Ecosystem*. Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-pde.pdf (Accessed on 17 May 2021.)

Cavoukian, A. & M. Prosch 2010. *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users.* Toronto, ON, Canada: Office of the Privacy Commissioner, Ontario, Canada. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-asu-mobile.pdf (Accessed on 17 May 2021.)

Cortesi, A. *et al* 2015. Datacentric Semantics for Verification of Privacy Policy Compliance by Mobile Applications. Paper presented at International Workshop on Verification, Model Checking, and Abstract Interpretation. Available at: https://doi.org/10.1007/978-3-662-46081-8_4 (Accessed on 17 May 2021.)

Data Protection Directive. 1995. Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995) 95/46/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 (Accessed on 17 May 2021.)

De Bruyn, M 2014. The Protection of Information (POPI) Act – Impact on South Africa. *International Business and Economics Research Journal* 13,6: 1315 - 1340. Available at: https://doi.org/10.19030/iber.v13i6.8922 (Accessed on 17 May 2021.)

Electronic Communications and Transactions Act (Act 25 of 2002) 2002. Available at: https://www.gov.za/documents/electronic-communications-and-transactions-act (Accessed on 17 May 2021.)

Esayas, S 2015. The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach. *European Journal of Law and Technology* 6,2: 1 - 23. Available at: https://ssrn.com/abstract=2746831 (Accessed on 17 May 2021.)

European Data Protection Board (EDPB) 2018. *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (Accessed on 17 May 2021.)

European Network and Information Security Agency (ENISA) 2018. *Privacy and Data Protection in Mobile Applications*. Heraklion, Greece: ENISA. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (Accessed on 17 May 2021.)

Federal Trade Commission (FTC) [US] 2012. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*. Available at: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (Accessed on 17 May 2021.)

Federal Trade Commission (FTC) [US] 2013. *Mobile Privacy Disclosures Building Trust Through Transparency*. Available at: www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (Accessed on 17 May 2021.)

Federal Trade Commission (FTC) [US] 2019. *Opinion of the Commission in the matter of Cambridge Analytica, LLC.* Available at: https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf (Accessed on 17 May 2021.)

Future of Privacy Forum & Center for Democracy and Technology 2011. *Best Practices for Mobile Applications Developers*. Available at: https://fpf.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf (Accessed on 17 May 2021.)

General Data Protection Regulation (GDPR) 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (Accessed on 17 May 2021.)

GSM Association 2011. *Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem.* Available at: https://www.gsma.com/publicpolicy/wp content/uploads/2016/02/GSMA2016_ Guidelines_Mobile_Privacy_Principles.pdf (Accessed on 17 May 2021.)

Hadar, I. *et al* 2018. Privacy by Designers: Software Developers' Privacy Mindset. *Empirical Software Engineering* 23,1: 259 - 289. Available at: https://doi.org/10.1007/s10664-017-9517-1 (Accessed on 17 May 2021.)

He, L. *et al* 2019. The Impact of GDPR on Global Technology Development.

Journal of Global Information Technology Management 22,1: 1 – 6. Available at: https://doi.org/10.1080/1097198X.2019.1569186 (Accessed on 17 May 2021.)

Information Commissioner's Office (ICO) [UK] 2013. *Privacy in Mobile apps: Guidance for app Developers.* Available at: https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdfhttps://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf (Accessed on 17 May 2021.)

Information Regulator [RSA] 2021. *Guidelines to Develop Codes of Conduct: Issued Under The Protection Of Personal Information Act 4 Of 2013 (POPIA).* Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-Guidelines-DevelopCodeOfConduct-22Feb2021.pdf (Accessed on 17 May 2021.)

Jain, S. & J. Lindqvist 2014. Should I Protect You? Understanding Developers' Behavior to Privacy-preserving APIs. Workshop on Usable Security (USEC'14). Available at: https://www.ndss-symposium.org/wp-content/uploads/2017/09/01_1-paper.pdf (Accessed on 17 May 2021.)

Kuan Hon, W 2016. *GDPR: Killing Cloud Quickly?* Portsmouth, NH, USA: International Association of Privacy Professionals (IAPP). Available at: https://iapp.org/news/a/gdpr-killing-cloud-quickly/ (Accessed on 17 May 2021.)

Li, H. *et al* 2019. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management* 22,1: 1 – 6. Available at: https://doi.org/10.1080/1097198X.2019.1569186 (Accessed on 17 May 2021.)

Kurtz, C. & M. Semmann 2018. Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Available at: https://aisel.aisnet.org/amcis2018/Security/Presentations/36/ (Accessed on 17 May 2021.)

Martin, K. & K. Shilton 2016. Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices. *The Information Society* 32,3: 200 - 216. Available at: https://www.tandfonline.com/doi/full/10.1080/01972243.2016.1153012 (Accessed on 17 May 2021.)

Martin, Y-S. & A. Kung 2018. Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering. Paper presented at 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Available at: https://doi.org/10.1109/EuroSPW.2018.00021 https://ieeexplore.ieee.org/document/8406568 (Accessed on 17 May 2021.)

Mikkonen, T 2014. Perceptions of Controllers on EU Data Protection Reform: A Finnish Perspective. *Computer Law and Security Review* 30: 190 - 195. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364914000284 (Accessed on 17 May 2021.)

National Small Enterprise Act (Act 102 of 1996) 1996. Available at: https://www.gov.za/documents/national-small-business-act (Accessed on 17 May 2021.)

National Telecommunications and Information Administration (NTIA) United States Department of Commerce 2013. *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*. Available at: https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf(Accessed on 17 Ma7 2021.)

Office of the Australian Information Commissioner (OAIC) 2014. *Mobile Privacy: A Better Practice Guide for Mobile App Developers*. Available at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers (Accessed on 17 May 2021.)

Office of the Privacy Commissioner (OPC) [Canada] 2012. *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*. Available at: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/ (Accessed on 17 may 2021.)

Omoronyia, I. *et al* 2013. Engineering Adaptive Privacy: On the Role of Privacy Awareness Requirements. Proceedings of the 2013 International Conference on Software Engineering. IEEE Press, 2013. Available at: https://doi.org/10.1109/ICSE.2013.6606609 (Accessed on 17 May 2021.)

Organisation for Economic Cooperation and Development (OECD) 2013. *The OECD Privacy Framework*. Paris: OECD. Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Accessed on 17 May 2021.)

Papageorgiou, A. *et al* 2018. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* 6: 9390 - 9403. Available at: https://doi.org/10.1109/ACCESS.2018.2799522 (Accessed on 17 May 2021.)

Privacy and Electronic Communications Directive 2002. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector 2002/58/EC.* Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058 (Accessed on 17 May 2021.)

Protection of Personal Information Act (Act 4 of 2013) 2013. Available at: http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf (Accessed on 17 May 2021.)

Razaghpanah, A. *et al* 2018. Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem. Available at: https://doi.org/10.14722/ndss.2018.23353 (Accessed on 17 May 2021.)

Regulation on Privacy and Electronic Communications 2017. *Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 (Accessed on 17 May 2021.)

Regulation of Interception of Communications and Provision of Communication-Related Information Act (Act 70 of 2002) 2002. Available at: http://www. gov.za/sites/default/files/gcis_document/201409/a70-02.pdf (Accessed on 17 May 2021.)

Republic of South Africa (RSA) 2016. *Information and Communication Technology (ICT) Broad-based Black Economic (B-BEE) Sector Code* (Government Gazette 40407, 7 November 2016).

Roos, A 2003. *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study*. PhD, Pretoria: UNISA. Available at: http://uir.unisa.ac.za/handle/10500/1463 (Accessed on 17 May 2021.)

Senarath, A. & N.A.G. Arachchilage 2018a. Understanding Software Developers' Approach towards Implementing Data Minimization. arXiv

preprint. Available at: https://arxiv.org/abs/1808.01479 (Accessed on 17 May 2021.)

Senarath, A. & N.A.G. Arachchilage 2018b. Why Developers cannot Embed Privacy into Software Systems? An Empirical Investigation. Paper presented at Proceedings of 22nd International Conference on Evaluation and Assessment in Software Engineering 2018, Christchurch, New Zealand. Available at: https://doi.org/10.1145/3210459.3210484; https://arxiv.org/abs/1805.09485 (Accessed on 17 May 2021.)

Sheth, S. et al 2014. Us and Them: A Study of Privacy Requirements across North America, Asia, and Europe. Proceedings of the 36th International Conference on Software Engineering. ACM, 2014. Available at: https://doi.org/10.1145/2568225.2568244; https://dl.acm.org/doi/10.1145/2568225.2568244 (Accessed on 17 May 2021.)

South African Law Reform Commission (SALRC) 2009. *Project 124 Privacy and Data Protection Report.* Pretoria: SALRC. Available at: http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf (Accessed on 17 May 2021.)

Sy, E. *et al 20*18. AppPETs: A Framework for Privacy-preserving Apps. Paper presented at Proceedings of 33rd Annual ACM Symposium on Applied Computing. Available at: https://doi.org/10.1145/3167132.3167415; https://dl.acm.org/doi/10.1145/3167132.3167415 (Accessed on 17 May 2021.)

Thomas, K. *et al* 2014. Distilling Privacy Requirements for Mobile Applications. Proceedings of 36th International Conference on Software Engineering. ACM, 2014. Available at: https://doi.org/10.1145/2568225.2568240; https://dl.acm.org/doi/10.1145/2568225.2568240 (Accessed on 17 May 2021.)

Van der Sype, Y. S. & W. Maalej 2014. On Lawful Disclosure of Personal User Data: What Should App Developers Do? 7th International Workshop on Requirements Engineering and Law (RELAW), IEEE 2014. Available at: https://doi.org/10.1109/RELAW.2014.6893479; https://ieeexplore.ieee.org/document/6893479 (Accessed on 17 May 2021.)

Van Kleek, M. *et al 20*17. Better the Devil you Know: Exposing the Data Sharing Practices of Smartphone Apps. Paper presented at Proceedings of 2017 CHI Conference on Human Factors in Computing Systems. Available at: https://doi.org/10.1145/3025453.3025556; https://people.csail.mit.edu/ilaria/papers/CHI2017.pdf (Accessed on 17 May 2021.)

Dusty-Lee Donnelly
Lecturer
School of Law
University of KwaZulu-Natal
Durban
donnelly@ukzn.ac.za