Data Privacy Compliance Benefits for Organisations – A Cyber-physical Systems and Internet of Things Study

Ntsako Baloyi[1,2][0000-0002-5690-9115] and Paula Kotzé [2][0000-0003-1610-2776]

[1] Council for Scientific and Industrial Research, South Africa
[2] Department of Informatics, University of Pretoria, South Africa
nbaloyi11@gmail.com, paula.kotze@gmail.com

Abstract. The protection of people's privacy is both a legal requirement and a key factor for doing business in many jurisdictions. Organisations thus have a legal obligation to get their privacy compliance in order as a matter of business importance. This applies not only to organisations' day-to-day business operations, but also to the information technology systems they use, develop or deploy. However, privacy compliance, like any other legal compliance requirements, is often seen as an extra burden that is both unnecessary and costly. Such a view of compliance can result in negative consequences and lost opportunities for organisations. This paper seeks to position data privacy compliance as a value proposition for organisations by focusing on the benefits that can be derived from data privacy compliance as it applies to a particular subset of information technology systems, namely cyber-physical systems and Internet of Things technologies. A baseline list of data privacy compliance benefits, contextualised for CPSs and IoT with the South African legal landscape is proposed.

Keywords: Internet of Things, cyber-physical systems, data privacy, privacy compliance benefits, POPI Act.

1 Introduction

Privacy is a multi-dimensional and multi-discipline concept that is not always easy to define. This paper focuses on a specific form of privacy, which is information or data privacy, also referred to as privacy of personal information [1]. In this paper, data privacy refers to control over one's personal information [2, 3]. Such control allows one to decide what may or may not be done with your personal information in cases where the law does not place any restrictions on such control.

Worldwide, organisations are under siege from regulatory authorities for violations of people's privacy [4, 5]. The increased focus on data privacy and the enactment of the General Data Protection Regulation (GDPR) [6] by the European Union (EU) has led to a worldwide rush of enacting data privacy legislation [7]. South Africa is among the countries that have enacted privacy legislation in the form of the Protection of Personal Information Act 4 of 2013 (POPI Act) [8]. The significance of privacy as

an important area of focus for organisations can therefore hardly be challenged. Ignoring data privacy can have dire consequences for organisations.

An earlier study [9] found that organisational readiness for data privacy compliance in South Africa was still a concern. Organisations should ensure their compliance to data privacy laws by leveraging organisational processes and structures to create an environment for data privacy to thrive. However, data privacy need not only be seen as a problem, but should also be seen as a value adding tool or opportunity for an organisation and its stakeholders.

Furthermore, technologies that process personal information are privacy prone, thereby affecting organisations that own or use them. Data privacy compliance is therefore also an important consideration for the processing of personal information through modern information technologies. This paper specifically focuses on cyber-physical systems (CPSs) and Internet of Things (IoT) technologies that collect and process personal information (and excludes those that do not). One of the strengths of CPSs and IoT technologies is their ability to capture or record vast amounts of information, some of which may be personal information. This strength is a double-edged sword as it is also a source of possible privacy risks and concerns. Data privacy has therefore been identified as one of the challenges that have to be addressed for CPSs [10] and IoT [11], since these technologies could have peculiar privacy risks and concerns, not typical of traditional information technology systems. These privacy concerns are due to data collection and processing methods that involve the use of sensors and advanced data processing (e.g. data mining) techniques or algorithms. The uniqueness of privacy concerns is also as a result of the possible covert nature of data collection, which may not involve meaningful data subject participation or informed consent.

Organisations are core to the advancement of data privacy in CPSs and IoT technologies. However, privacy compliance for organisations, like any other compliance requirements, is often seen as an extra burden that is both unnecessary and costly. Such a view of compliance can result in negative consequences and lost opportunities for organisations. Cavoukian and Dixon [12] have proposed the identification of information security and privacy compliance benefits as a useful exercise for justifying investment.

Privacy compliance benefits, however, is an area that that remains largely unexplored. There are many publications that focus on benefits or applications of data, CPSs and IoT for individuals, organisations and nations [13-21]. It is customary to focus on the value that technologies themselves can bring, as has been evidenced and is further corroborated by the work of Carroll [22] on cloud computing and virtualization benefits. The value of data as well as technologies like CPSs and IoT is significant and well-articulated. Interestingly, not much literature exist that focus on value that could result from compliance in general, and privacy compliance specifically. Such a position does not provide organisations with much incentive for compliance other than being legally abiding and responsible corporate citizens.

Contextualised within the South African legal landscape, this paper focuses on such privacy compliance benefits, with a view to bring to light the value that organisations can derive as a result of data privacy compliance, specifically as it relates to

CPSs and IoT. The list of baseline privacy compliance benefits for organisations are not necessarily limited to CPSs and IoT, but could also find relevance for other technologies and domains with privacy implications.

Section 2 provides background on CPSs, IoT and privacy. Section 3 outlines the research methodology followed in compiling the list of benefits. Section 4 discusses the findings and presents a proposed list of privacy compliance benefits. Section 5 comments on the use of the benefits while section 6 concludes the paper.

2 Background

2.1 Cyber-physical Systems and Internet of Things

There are no standard definitions for both CPSs and IoT. This paper views a CPS as highly automated physical systems or processes with computing and networking [14]. An alternative definition views CPSs as electronic control systems that control physical machines, such as, controlling motors and valves in an industrial plant [23]. The typical characteristic of CPSs are physical component cyber-capability, multi-scale networking, dynamic reorganisation, self-configuration, high automation, cyber-physical adaptation, self-management and dependable operation [24].

Two distinctions are made to the definition of IoT, namely, small and large IoT deployments or applications [25]. The Institute for Electrical and Electronics Engineers (IEEE) definition for small deployments of IoT focuses on the interconnectedness of things to the Internet and their remote management [25]. The IEEE's definition for large deployments of IoT focuses on complex systems that possess self-adaptive, high-automation and physical-to-digital capabilities. Large IoT deployments are sometimes referred to as Industrial Internet of Things (IIoT) [26]. In this paper, IoT shall refer to the interconnection of things to the Internet and the ability to remotely manage them, in line with the definition for small scale deployments. The large-scale deployment of IoT, i.e. IIoT, shall be referred to under the umbrella concept of CPSs.

Examples of IoT applications include an individual's interconnected devices, smart homes, etc. [18]. CPSs' applications areas could include power grids, vehicular transportation, smart buildings, eHealth, smart manufacturing, etc. [14, 19].

2.2 Privacy and the Protection of Personal Data

At least 108 countries and regions were reported to have enacted data privacy legislation by 2016 [27]. South Africa has enacted privacy legislation in the form of the POPI Act [8] to address privacy for both natural and juristic persons. Examples of privacy legal instruments enacted by other countries and regions include the European Union's GDPR [6], United Kingdom's Data Protection Act [28] and the African Union's Convention on Cybersecurity and Personal Data Protection [29].

Privacy legal instruments are underpinned by principles or conditions for the lawful processing of personal information. These principles or conditions are largely a variation of the five fair information practices (FIPs) introduced by the United States

Department of Health, Education and Welfare in 1973 [30]. The FIPs are transparency, use limitation, access and correction, data quality and security.

The POPI Act [8] is premised on the right to privacy which is provided for in section 14 of the Constitution of the Republic of South Africa of 1996 [31]. The POPI Act is concerned with regulating the processing of personal information and therefore does not only apply to CPSs and IoT but to all processing of personal information. Processing is an all-encompassing term that covers anything that can be done with personal information, including collection, retrieval, storage, alteration, destruction, transmission, etc. [8].

The POPI Act [8], however, does not define the term privacy. Data privacy in this paper refers to privacy over personal information, giving data subjects control over their personal information [2, 3]. Personal data is defined as information relating to an identifiable, living natural person or existing juristic person [8, 32]. A data subject is a person whose identifying personal data is the subject of collection or processing [8].

Sections 8-25 of the POPI Act [8] lays down eight conditions for the processing of personal information, as provided in Table 1.

Table 1. Conditions for the lawful processing of personal information [8].

Privacy condition	Description
Accountability	To ensure that all the conditions and relevant provisions of the POPI Act are complied with, when processing personal information.
Processing limitation	To ensure that only minimal personal information is processed and such processing is lawful and conducted in a reasonable manner. Further that personal information is collected directly from data subjects and primarily based on informed consent, unless certain conditions apply.
Purpose specification	To specify and communicate the purpose for the processing of personal information. Responsible parties, may, in certain circumstances be required to retain or restrict the processing of personal information.
Further processing limitation	To ensure that personal information is only processed for specified or compatible purposes unless there are other valid legal grounds for further processing, such as informed consent.
Information quality	To ensure that personal information is accurate, complete, not misleading and updated where necessary.
Openness	To ensure that responsible parties maintain documentation of processing activities and communicate details relevant for data subjects to exercise their rights.
Security safeguards	To ensure that responsible parties take appropriate and reasonable technical and organisational measures to secure the integrity and confidentiality of personal information within their control or possession.
Data subject participation	To ensure that data subjects are able to request access, correction, deletion and other actions to their personal information.

3 Research Methodology

The primary objective of this paper is to assist organisations to embed data privacy into their organisational culture with an appreciation of the value that data privacy compliance can bring. The focus is specifically on privacy compliance benefits for organisations that use or develop technologies for CPSs and IoT to address the paucity of organisational data privacy compliance benefits for these technologies and empower them to view data privacy compliance as a value adding exercise.

A design science research (DSR) approach was followed to conduct the research to compile the benefits, allowing for knowledge generation and contribution through iterations or circumscriptions. The variant of DSR followed is that by Vaishnavi, Kuechler and Petter [33], with five activities, namely, awareness of the problem, suggestion for a solution, development, evaluation and conclusion. The list of privacy compliance benefits was developed in two DSR development iterations followed by a refinement process.

During the first development cycle, a literature study and content analysis (of legal instruments) were conducted to identify privacy compliance benefits with likely significance for organisations with respect to CPSs and IoT. This iteration resulted in an initial list of 14 privacy compliance benefits. The second development iteration, to review and refine the initial list of privacy compliance, included an expert review process that used interviews and questionnaires. The panel of 23 experts, with 202 years of combined experience, included specialists from eight different domains, including CPSs/IoT, data privacy law, data privacy, management, enterprise risk, human resources, information security and enterprise architecture. They were asked to review the provided benefits, suggest exclusions of any of the listed benefits and inclusion of new benefits. This cycle resulted in changes to the phrasing of some benefits and the addition of three new benefits, resulting in a total of 17 benefits.

As an evaluation exercise for factual accuracy and coverage, the 17 organisational privacy compliance benefits for CPSs and IoT were reviewed by another panel of 21 specialists from similar domains to the development panel, also with at least 202 years combined experience. The reviews were conducted in the form of interviews guided by an open-ended questionnaire. The guiding question was to determine whether the presented benefits highlight the most important benefits of data privacy compliance for organisations in relation to CPSs and IoT. The respondents were requested to substantiate their responses. The proposed list of data privacy-related benefits for organisations in the context of CPSs and IoT were found to be representative of the most important benefits that organisations can derive from privacy compliance. One additional benefit was suggested for inclusion and included in the final list of 18 benefits. The review formed part of the evaluation for a broader project focusing on developing a data privacy framework for CPSs and IoT for IT professionals [34].

The usefulness and relevance of the benefits was also demonstrated on a real-world IoT project being deployed at an organisation in South Africa [34]. Many of the benefits were found to be directly relevant to the project and the context of the project.

4 Privacy Compliance Benefits for Organisations Using or Developing CPS and IoT Technologies

Organisational data privacy compliance benefits refer to the value that an organisation can derive as a result of privacy legal compliance, with particular focus on CPSs and IoT domains. The ability to avoid, mitigate or transfer certain privacy risks can also be seen as privacy compliance benefits. Privacy compliance benefits are meant to assist organisations to appreciate the value that data privacy compliance can bring to an organisation, in order to build a case for spending resources on data privacy compliance beyond the need for legal compliance.

In total, this paper proposes a non-exhaustive list of 18 organisational privacy compliance benefits. These are potential privacy compliance benefits that organisations may derive as a result data privacy compliance for CPSs and IoT technologies. Each of these benefits are discussed in more detail in the remainder of this section.

4.1 Legal Compliance

The primary organisational benefit emanates from being able to demonstrate respect for the rule of law through legal compliance. The ability to demonstrate privacy compliance is essential not only for regulatory authorities, but for various other stakeholders as well such as data subjects, investors, etc. Data privacy compliance, in this instance, means compliance with the law (or legal obligations) [35]. In the South African context, this primarily means complying with the POPI Act [8] and secondarily with associated domestic and international privacy laws. Legal compliance is a benefit as it has the potential to protect organisations from legal sanctions and adverse public action. Data privacy compliance is an advantage for organisations in that they conduct their operations knowing that they are in compliance with the law and are providing value to their clients and other stakeholders.

4.2 Data Subject Trust and Confidence

Data subjects, as active or inactive participants in CPSs and IoT technology-related processing activities, should be able to trust the product or service and the intentions of the organisations involved, and have confidence that the organisations will treat their personal information in line with the law. However, the nature of CPSs and IoT is such that people may become data subjects without their knowledge. CPSs and IoT are often not geared for an opt-in mechanism as opt-in may sometimes be difficult to effect for these technologies. An example of this could be in a smart city environment where various types of sensors that process personal information may be deployed across a city. Sometimes data subjects may not even have full appreciation of the extent of the data collected or the data processing activities, even where such information may be readily available. In such situations, organisations responsible for the CPSs and IoT technologies have an even greater responsibility to ensure that they are data privacy compliant because of the nature of their CPSs and IoT related activities.

Data privacy compliance and respect for people's data privacy have the potential to increase levels of trust and confidence in organisations [1, 35, 36]. An effort by an organisation to comply with data privacy laws can boost people's perceptions about the organisation and their willingness to use or participate in the organisation's CPSs and IoT related activities or initiatives. Data subject trust and confidence in organisations is thus a benefit that organisations can derive from ensuring data privacy compliance when dealing with personal data, especially in areas such as CPSs and IoT.

4.3 Data Subject Retention

Data privacy breaches and an apparent lack of systems to safeguard people's privacy can result in people losing confidence in organisations and deciding to boycott their products and services [37]. It follows that evidence of data privacy protection mechanisms can contribute towards data subject retention, which is in the best interest of organisations [35]. Loss of data subjects may imply a loss of customers or important participants for CPSs and IoT initiatives, which could be detrimental to such programmes. Data subjects may be more likely to continue participating in or using CPSs and IoT related projects, systems or solutions when they are aware that there is no immediate danger to themselves as could result from data privacy violations. The value that organisations can derive could be increased data subject retention as the risk of flight would be mitigated.

4.4 Public Trust

Public trust in an organisation is important for the organisation's brand, services and financial sustainability. One of the factors that can affect an organisation's bottom line is how people perceive an organisation, which has a direct bearing on the level of trust that they apportion to that organisation. Dissatisfaction by one member of the public could result in serious consequences for an organisation due to the ease with which people can disseminate their frustrations to increased networks of people. Privacy related frustrations are not an exception and can in fact solicit even higher levels of rage from the public. Organisations therefore need to jealously and actively guard as well as manage the trust that the public has on them. Privacy is one area that organisations should ensure that they are not left vulnerable as it could result in the erosion of public trust on the entire organisation and its products or services. Data privacy protection is but one of many areas that can bring about greater public trust in organisations [38, 39], and has been posited as one of the factors that can increase confidence in organisations [35]. Public trust in organisations with CPSs and IoT technologies has the potential to encourage or enable CPSs and IoT technology uptake and confidence by the public.

4.5 Consumer Trust and Confidence

The strength and sustainability of any commercial organisation hinges on its customer base, natural or juristic. Organisational customer trust and confidence, or lack thereof,

can have serious financial implications. Consumer trust and confidence also have a direct impact on customer perceptions of the organisation's brand and may influence how customers speak about the organisation to others [1, 36]. Consumers who trust or have confidence in organisations or particular brands often remain loyal customers and can confidently introduce others to the same organisation or brand. This makes consumer trust and confidence in organisations and their brands an essential element for their growth and survival. Consumer action and public outrage has proven to be effective in getting organisations to review practices detrimental to consumers [40].

Consumer trust and confidence is an area that could have a bearing on customer satisfaction and continued willingness to engage with the organisation, or its services and products, especially those most likely to affect their privacy. All the organisation's stakeholders, including customers and employees, should have confidence in how the organisation handles data privacy. Customer trust (including that of employees) over an organisation's data privacy practices and processes is essential for CPSs and IoT project buy-in and support [35].

4.6 Respect for Consumer Privacy

Organisations are often criticised for pursuing profits at the expense of human rights abuses and other societal effects [41]. Data privacy compliance can be one way to practically demonstrate that an organisation are is concerned about and does have respect for consumers, their privacy and by extension their human rights [36]. This is one way to demonstrate organisational customer-centricity, especially for potentially invasive technologies like CPSs and IoT.

4.7 Improved Service Provision

Access to personal information is important for the provision of services to individuals and is beneficial for statistical and research purposes. CPSs and IoT sensors can be great sources for personal information related to service provision. Lawful processing of personal information by organisations can benefit both organisations and data subjects as it can result in better service provision [35]. Compliance with data privacy laws empowers organisations to legally process personal information in the furtherance of their objectives, which could in turn result in improved service provision for the organisation's clients.

4.8 Reducing Organisational Reputational Risk

An organisation's reputation affects its ability to do business in an optimal manner. Data privacy violations, or lack of data privacy compliance, can be a contributing factor to an organisations' reputational damage. Data privacy compliance can, therefore, reduce the exposure of the organisation to reputational risks resulting from CPSs and IoT operations [38, 39]. Organisations can in turn be spared from data privacy-related law suits, prosecutions, public outcry, regulatory sanctions, etc. A good name remains one of the important attributes that organisations need and anything, includ-

ing privacy-related risks, that could adversely affect it has the potential to threaten their very existence.

4.9 Improved Risk Management

Incorporating privacy into an organisation's risk management processes strengthens an organisation's internal risk controls. Conducting a privacy risk assessment is a legal requirement in terms of sections 19(2) and 109(3)(g) of the POPI Act [8]. Organisations can improve their risk management procedures by incorporating personal data related risks, specifically those relating to CPSs or IoT. This would result in them satisfying the requirement for risk assessments of personal information and consequently be making inroads toward data privacy compliance. Data privacy compliance can strengthen internal risk management in organisations [1].

4.10 Data Privacy Risk Minimisation

Organisations are increasingly exposed to privacy-related risks, especially in the form of data breaches. Data privacy breaches could include information security breaches, unlawful processing, inability to provide data subject access to personal information where applicable, etc. The minimisation of data privacy risk is an advantage as it reduces an organisation's risk exposure. The volume and sensitivity of personal information that organisations manage increase their risk of data breaches. Putting systems in place to ensure that an organisation is data privacy compliant can greatly minimise potential data privacy breaches [38]. Compliance with the eight conditions for the lawful processing of personal information [8] (see Table 1) could minimise organisations' exposure to data privacy-related risks. CPSs and IoT devices have particularly been identified as high-risk targets for information security breaches and likewise data privacy breaches [10, 11].

4.11 Reduction of Complaints and Disputes

It is in the best interest of any organisation to ensure that there is minimal stakeholder dissent or dissatisfaction resulting from the use of CPSs and IoT to process personal information. With section 24 of the POPI Act [8] empowering data subjects to dispute the accuracy of collected personal information or lawfulness of the processing and request its correction or deletion, organisations need to be privacy compliant and prepared to support data subjects. Furthermore, section 74 of the POPI Act empowers any person to lay a complaint with the Information Regulator [42] where they feel that there has been interference with their right to protection of personal information.

Compliance with data privacy laws can greatly reduce privacy-related complaints or disputes and/or assist with their speedy resolution [38, 39]. Data privacy compliance may also reduce the risk of infringement by organisations and enforcement action by the Information Regulator [39]. Reduced data privacy-related complaints and disputes may save an organisation valuable resources and increase confidence [39].

4.12 Public Perception of Transparent Practices

In business, just as in life, perceptions are everything. Organisations need to be seen to be transparent with people's personal information by being open and clear about their CPSs or IoT data processing activities. Demonstrating that an organisation is transparent can boost its image in society and with its customers, which can in turn result in greater public confidence [35, 43]. Automated decision-making (section 71 of the POPI Act [8]) and data subject access (sections 18 and 23 of the POPI Act) are some of the areas where data subjects can witness an organisation's transparency or lack thereof. In terms of sections 17-18 of the POPI Act, the openness condition stipulates that organisations or responsible parties should document details about their processing operations and disclose certain information to data subjects. Organisations therefore need to ensure that they are favourably perceived by the public as this can improve their reputation. Privacy compliant practices can aid with this purpose.

4.13 Reduced Risk of Collateral Intrusion

CPSs and IoT technologies present a risk of capturing large amounts of information about people indiscriminately. This risk is known as collateral intrusion as data subjects other than those targeted can be affected, and even those targeted may not have consented to the processing of their personal information. CPSs and IoT could lead to the collection and processing of vast amounts of personal information that could result in adverse inferences towards data subjects. Compliance with data privacy conditions or principles may reduce the risk of collateral intrusion [44]. This is made possible through mechanisms such as data minimisation, de-identification and others. The perceived reduced risk of collateral intrusion is a benefit as it could lead to better acceptance of CPSs and IoT technologies and a reduced likelihood of legal action as a result of data privacy breaches.

4.14 Regulated Data Sharing

Data is central to the benefits associated with CPSs and IoT. It is also the main focus of privacy laws. Organisations have a need to process data, some of which may be personal information. It may also be in the nature of an organisation's business to have to share personal data. Compliance with personal data privacy laws can be an enabler for lawful sharing, whilst the opposite may directly limit an organisation's operations. Information may be lawfully shared in compliance with the POPI Act's [8] eight conditions for lawful processing of personal information (see Table 1). It may also be shared by relying on the further processing limitation condition, as per section 15 of the POPI Act. Transborder transfer or sharing is regulated by section 72 of the POPI Act. Requests for access to personal information, which results in the sharing of personal information, may also emanate from the process as set out in the Promotion of Access to Information Act 2 of 2000 [45].

Data privacy compliance can, therefore, enable data sharing where the conditions set out in the POPI Act [8] are met. Data sharing can be one of the advantages that

organisations that comply with data privacy laws can legally enjoy, and shared data can accordingly be afforded appropriate protection [39]. Data transfers may be difficult to avoid in CPSs and IoT technologies and should, therefore, be done in privacy compliant ways. It is difficult for organisations to control or monitor what is done with personal information once shared. As a consequence, being able to show that an organisation took all reasonable measures/precautions before sharing personal information can save organisations from liability or reduce their liability.

4.15 Better Data Security/Protection

Information security is very important for CPSs and IoT environments, more so when dealing with personal information of natural and juristic persons. In terms of sections 19-21 of the POPI Act [8], one of the data privacy conditions or principles (see Table 1) is security safeguards. The security safeguards principle requires organisations to take appropriate technical and organisational measures to protect personal information. A focus on information security measures for personal data, in terms of section 19 of the POPI Act, can help strengthen an organisation's information security. Information security is very important for CPSs and IoT environments, more so when dealing with personal information of natural and juristic persons.

Many privacy breaches are likely to be as a result of information security breaches. Adequate focus on information security is an advantage with respect to both information security and privacy. Organisations would be less likely to be exposed to privacy breaches, which would in turn expose all their operations to scrutiny. Information security is important to protect the organisation and data subjects, and also to ensure that CPSs and IoT technologies are not hijacked to be used for nefarious purposes.

4.16 Encourage Adoption of CPSs and IoT

Privacy has been identified as one of the challenges that plagues CPSs and IoT technologies and could affect their effective adoption [10, 11]. Data subjects and the public at large are likely to be more amenable to CPSs and IoT technologies when they perceive a level of transparency, are given adequate control over their personal information and realise that an organisation takes their data privacy seriously [46].

This benefit is closely related to consumer trust, since buy-in would not exist where there is no trust. Employee technology buy-in, as a result of clear data privacy respecting practices, was identified as a benefit by some human resource specialists during the development of the benefits. Privacy compliance can therefore support a more enabling environment for the adoption of CPSs and IoT technologies.

4.17 Improved Trade Relations and Investment

Data privacy compliance has been identified as an area that can open up opportunities in the trade space, especially from a transborder perspective, as certain regions or countries prohibit trade when inadequate protection of personal information is pre-

sent. For example, Article 43 of the GDPR [6] and section 72 of the POPI Act [8] prohibit the transfer of personal information to third countries or international organisations where there are no appropriate safeguards or adequate levels of protection in place. Having appropriate safeguards or adequate levels of protection could therefore eliminate barriers for organisations doing business across borders, at least relating to data privacy, and may consequently attract investment.

An increase in investment opportunities and investor confidence regarding CPSs and IoT is a possible benefit that could accrue to organisations as a result of data privacy compliance, especially in the age of the fourth industrial revolution, for which these technologies are enablers. Proving that a particular device, product, service, solution or project is data privacy compliant may, together with other factors, inspire investor confidence. It would highlight competitive and compliance aspects that can draw investor support and, thus, investment opportunities for CPSs and IoT initiatives. The opposite could negatively affect investment even for transactions unrelated to personal information; a single area that exposes the organisation to risks can affect unrelated investments.

4.18 Organisational Management Efficiency

An organisation that follows a proper privacy risk management process empowers its management to effectively oversee the implementation of data privacy compliance. A risk assessment report can provide management with a quick overview of what to expect for data privacy compliance, without the need for them to be experts in privacy law. This increased ability to provide more informed oversight is in the best interest of privacy in general and organisations responsible for CPSs and IoT technologies in particular.

5 Using the Benefits

This paper focuses on privacy compliance benefits, with a view to highlight the value that organisations can derive as a result of data privacy compliance in relation to CPSs and IoT. To effectively use the benefits provided, it is necessary to understand organisational strategic priorities and the project scope. The project scope should then lead to the identification of the value that the organisation can derive from the technology and the risks associated with the project. With the understanding of the project scope, technological value, potential privacy risks and the organisation's strategic priorities, one can then identify data privacy benefits relevant for the CPSs or IoT project and the organisation. The benefits can be based on the list of benefits provided for in this paper or could be completely new benefits. This paper simply seeks to stimulate thoughts (consideration) of benefits directly linked to privacy compliance. The use and applicability of the benefits were demonstrated in a proof of concept exercise on an IoT project at a South African organisation [34] and were found to be representative of the benefits that would result from privacy compliance.

6 Conclusion

This paper advocates for the protection of personal information as a human right to privacy and as an exercise that can have potential value for organisations. Organisations are important stakeholders in the data privacy value chain. They therefore cannot remain on the periphery of the privacy discourse and act as mere implementing agents of the law through compliance. Their role has to be a form of active citizenry that respects humanity, the rule of law and people's right to privacy and self-determination. As organisations take on a more active role in the privacy landscape, there is inherent tangible and intangible value that accrues to such organisations. In a world where organisations may be seen as being merely interested in profits, they have a role to play in re-writing the narrative by actively taking steps to protect and show respect for data subjects and thereby protect their own interests and standing in society.

This paper presented a list of 18 data privacy compliance benefits for CPSs and IoT technologies with the aim to highlight the value that organisations can derive from data privacy compliance. The benefit-focused approach followed in this paper goes beyond viewing privacy as a legal compliance obligation into demonstrating the value that an organisation could derive as a result of privacy compliance. The list of data privacy compliance benefits provided is not exhaustive and serves only as guidance to locating the value for organisations through data privacy compliance. It is also clear that many benefits from the list presented are quite generic and could reasonably apply to any technology or data processing initiative.

Future work opportunities include further refinement and testing of the benefits. A closer focus on data subjects and privacy regulatory authorities is another area worth exploring.

References

1. ICO: Privacy impact assessment and risk management. Information Commissioner's Office, Wilmslow (2013).
2. Westin, A.F.: Privacy and freedom. Washington and Lee Law Review **25**, 166 - 170 (1968)
3. Solove, D.J.: Conceptualizing privacy. California Law Review **90**, 1087 - 1155 (2002)
4. Erickson, K., Howard, P.N.: A case of mistaken identity? News accounts of hacker, consumer, and organizational responsibility for compromised digital records. Journal of Computer-Mediated Communication **12**, 1229 - 1247 (2007)
5. Cole, D.D.: Assessing the leakers: criminal or heroes. Journal of National Security Law & Policy **8**, 107 - 118 (2015)
6. European Union. GDPR Portal: Site Overview. https://www.eugdpr.org/eugdpr.org.html.
7. Baloyi, N., Kotzé, P.: A data privacy model based on Internet of Things and cyber-physical systems reference architectures. In: Proceedings of the Annual conference of The South African Institute of Computer Scientists and Information Technologists: SAICSIT 2018 – Technology for Change, 258 - 268. ACM (2018). https://doi.org/10.1145/3278681.3278712

8. Government of South Africa. Protection of Personal Information Act 4 of 2013. Government Printing Works (2013). www.justice.gov.za/legislation/acts/2013-004.pdf.
9. Baloyi, N., Kotźe, P.: Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? In: Cunningham, P., Cunningham, M. (eds.): IST-Africa 2017 Conference, 1 - 11. IEEE (2017).
10. Babiceanu, R.F., Seker, R.: Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in Industry **81**, 128 - 137 (2016) https://doi.org/10.1016/j.compind.2016.02.004
11. Internet Society: The Internet of Things: An Overview (2015).
12. Cavoukian, A., Dixon, M.: Privacy and Security by Design: An Enterprise Architecture Approach, Information and Privacy Commissioner, Ontario, Canada (2013).
13. Aktypi, A., Nurse, J.R.C., Goldsmith, M.: Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In: Proceedings of the 2017 on Multimedia Privacy and Security 1 - 11. ACM, New York (2017). https://doi.org/10.1145/3137616.3137617
14. Lee, E.A., Seshia, S.A.: Introduction to Embedded Systems, A Cyber-Physical Systems Approach. MIT Press (2017).
15. Lee, J., Bagheri, B., Kao, H.: A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters **3**, 18 - 23 (2015)
16. Thinakaran, K., Dhillon, J.S., Gunasekaran, S.S., Chen, L.F.: A conceptual privacy framework for privacy-aware IoT health applications. In: 6th International Conference on Computing and Informatics, 175 - 183. Kuala Lumpur (2017).
17. Torre, H., Koceva, F., Sanchez, O.R., Adorni, G.: A framework for personal data protection in the loT. In: Internet Technology and Secured Transactions (ICITST), 384 - 391. IEEE (2016). https://doi.org/10.1109/ICITST.2016.7856735
18. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey. Computer Networks **54**, 2787 – 2805 (2010) https://doi.org/10.1016/j.comnet.2010.05.010
19. Khaitan, S.K., McCalley, J.D.: Design techniques and applications of cyberphysical systems: A survey. IEEE Systems Journal **9**, 350 - 365 (2015) https://doi.org/10.1109/JSYST.2014.2322503
20. Stankovic, J.A.: Research directions for the Internet of Things. IEEE Internet Things Journal **1**, 3 - 9 (2014)
21. Wood, A.D., Stankovic, J.A., Virone, G., Selavo, L., He, Z., Cao, Q., Doan, T., Wu, Y., Fang, L., Stoleru, R.: Context-aware wireless sensor networks for assisted living and residential monitoring. IEEE Network **July/August 2018**, 26 – 33 (2008)
22. Carroll, M.: A Risk and Control Framework for Cloud Computing and Virtualization, University of South Africa, Pretoria (2012).
23. Colbert, E.: Security of Cyber-Physical Systems. Journal of Cyber Security and Information Systems **5**, (2017)
24. Miclea, L., Sanislav, T.: About dependability in cyber-physical systems. In: EWDTS, 17 - 21. (2011).
25. Minerva, R., Biru, A., Rotondi, D.: Towards a Definition of the Internet of Things (IoT), IEEE (2015).
26. Lin, S., Miller, B., Durand, J., Bleakley, G., Chigani, A., Martin, R., Murphy, B., Crawford, M.: The Industrial Internet of Things Volume G1: Reference Architecture, Industrial Internet Consortium (2017).
27. Tesfachew, T.: Key challenges in the development and implementation of data protection laws. In: Data Protection Regulations and International Data Flows: Implications for Trade and Development, 7 - 22. United Nations, Geneva (2016).

28. Government of the United Kingdom. Data Protection Act 29 of 1998. Government of the United Kingdom (1998). www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf.
29. African Union: African Union Convention on Cyber Security and Personal Data Protection, African Union (2014).
30. Cate, F.H.: The failure of fair information practice principles. In: Winn, J.K. (ed.): Consumer Protection in the Age of the "Information Economy.". Ashgate Publishing, Hampshire, UK (2006).
31. Government of South Africa. Constitution of the Republic of South Africa. (ISBN 978-0-621-39063-6). Government of South Africa, (1996). www.justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf.
32. OECD: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).
33. Vaishnavi, V., Kuechler, W., Petter, S. Design Science Research in Information Systems. http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf.
34. Baloyi, N.: A Data Privacy Framework for Cyber-physical Systems and Internet of Things for Information Technology Professionals, University of Pretoria, Pretoria (2019).
35. ICO: Subject Access Code of Practice Information Commissioner's Office, Wilmslow (2014).
36. Weinberg, B.D., Milne, G.R., Andonova, Y.G., Hajjat, F.M.: Internet of Things: Convenience vs. privacy and secrecy. Business Horizons **58**, 615 - 624 (2015) https://doi.org/10.1016/j.bushor.2015.06.005
37. Reuters. Musk Deletes Facebook Pages of Tesla, SpaceX After Challenged on Twitter. https://www.reuters.com/article/us-spacex-musk/musk-deletes-facebook-pages-of-tesla-spacex-after-challenged-on-twitter-idUSKBN1GZ2MZ.
38. ICO: Anonymisation: Managing Data Protection Risk Code of Practice, Information Commissioner's Office, Wilmslow (2012).
39. ICO: Data Sharing Code of Practice, Information Commissioner's Office, Wilmslow (2011).
40. Head, T. Momentum agree to R2.4m payout for Nathan Ganas' family. https://www.thesouthafrican.com/momentum-agree-pay-ganas-family-why/.
41. Baloyi, N., Kotźe, P.: Do users know or care about what is done with their personal data: A South African study. In: Cunningham, P., Cunningham, M. (eds.): IST-Africa 2017 Conference Proceedings, 1 - 11. IEEE (2017).
42. Kula, S. Appointment of the Information Regulator for POPI and PAIA. https://www.michalsons.com/blog/appointment-of-the-information-regulator/20059.
43. ICO: The Guide to Data Protection, Information Commissioner's Office, Wilmslow (2017).
44. ICO: In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information Information Commissioner's Office, Wilmslow (2015).
45. Government of South Africa. Promotion of Access to Information Act 2 of 2000. Government of South Africa, (2000). www.justice.gov.za/legislation/acts/2000-002.pdf.
46. Sinclair, M., Siemieniuch, C., Palmer, P.: The identification of knowledge gaps in the technologies of cyber-physical systems with recommendations for closing these gaps. Systems Engineering **22**, 3 - 19 (2019)