ESARBICA JOURNAL

JOURNAL OF THE EASTERN

AND SOUTHERN AFRICA

REGIONAL BRANCH OF THE

INTERNATIONAL COUNCIL ON

ARCHIVES

Volume 43
2024

ISSN 2220-6442 (Print), ISSN 2220-6450 (Online)

https://dx.doi.org/10.4314/esarjo.v43i1.2

A South African perspective on data privacy in consumer Internet of Things

Mfanasibili Ngwenya
Vodacom
mfanasibili@hotmail.com
ORCID: 0000-0002-0400-4178

Mpho Ngoepe
University of South Africa
ngoepms@unisa.ac.za
ORCID: 0000-0002-6241-161X

Received: 24 July 2024
Revised: 01 October 2024
Accepted: 09 December 2024

Abstract

The rise of the Internet of Things (IoT) raises concerns about data privacy. This qualitative study explored data privacy issues in consumer IoT using a combination of the narrative inquiry method and the Delphi technique through three rounds of interviews with experts. The study identified three levels at which personal data privacy is a concern: data collection, data transfer and data storage. Consumer data may be vulnerable at any of these stages of processing. The risks identified by the study include identity theft, financial difficulties and the unauthorised sale of personal information, location-based tracking, medical privacy and unfair discrimination due to profiling. Personally identifiable information goes beyond the consumer's known information, such as age, gender, race and other attributes. Smart devices can help consumers extend their identities. The study identified the need for legal instruments that can be used to deal with data privacy in consumer IoT in South Africa, particularly. It is concluded that IoT companies and manufacturers must be much more transparent about the data they collect and how it is processed, stored and used. It also is necessary to educate all IoT users about the dangers of using devices, which are the same as connecting to the internet.

Keywords: data privacy, consumer internet of things, personal information, data collection, data transfer, privacy legislation, data storage

Introduction and background to the study

The rise of the Internet of Things (IoT) comes with challenges concerning data privacy issues. Privacy concerns other people's ability to identify personal information based on the available data. Various smart devices that are part of the Consumer IoT (CIoT) assemblage may collect such data. In the CIoT space, personal data is shared with businesses for marketing, monitoring and evaluation of the IoT products, among other things. Consumers download mobile apps and use them without thinking twice about the kind of personal information they expose to the owners of the apps and possibly to the rest of the world. In a world where cybercriminals have

tremendously increased, people need to be aware of the benefits and dangers of these advances in IoT technology. For CIoT to succeed, safety is critical, and all the stakeholders in the IoT assemblage need to ensure the protection of consumers.

Researchers suggest that data privacy is a significant concern in the context of the CIoT in South Africa. Ngwenya and Ngoepe (2020) propose a framework to address the issues of data security, privacy and trust in the CIoT, emphasising the importance of safety and protection for consumers. Caron, Bosua, Maynard and Ahmad (2016) researched the Australian context, highlighted the challenges to individual privacy associated with data collection through IoT and argued that current privacy legislation in Australia does not adequately protect individual privacy. Perez, Zeadally and Cochran (2018) review the privacy policies and practices of six CIoT devices and find that IoT privacy policies may not be usable from the human-computer interaction perspective. Samania, Ghenniwa and Wahaishi (2015) propose a privacy protection management framework for Cooperative Distributed Systems (CDS) at the interaction level, which can be applied to CIoT. Neves, Souza, Sousa, Bonfim and Garcia (2023) provide a review of data privacy methods in the IoT, focusing on data anonymisation, and identify a lack of consensus in the field. Overall, the researchers suggest that data privacy is a significant concern in the CIoT, and there is a need for more robust privacy protection measures and legislation.

Data privacy concerns may be present at data collection, storage or transfer. The collected data may reveal personally identifiable information (PII). According to Peppet (2014), PII refers to any information that can be used to identify a person. It can consist of contact details, type of information, demographic information, historical information, biometric information, personal opinions and views, private and confidential correspondence, and views and opinions about an individual made by another individual. Ziegeldorf, Morchon and Wehrle (2014) capture the idea of informational self-determination by saying that the individual needs to:

- assess his privacy risks
- take appropriate action to protect his privacy
- be assured that the protection is enforced beyond the person's immediate sphere of control.

This qualitative study explored data privacy issues in consumer IoT using a combination of the narrative inquiry method and the Delphi technique through three rounds of interviews with experts. South Africa has some laws that seek to protect consumers such as Protection of Personal Information Act (No 4 of 2013) and Consumer Protection Act (No 68 of 2008). The POPI Act is more relevant to this study and exists to guarantee that all South African institutions responsibly behave themselves when collecting, processing, storing and sharing other people’s information. Even though the authorities enacted the POPI Act in 2013, it is only coming into effect in 2020. The enforcement of the law delayed since to allow the establishment of the regulatory bodies, that is, the Information Regulator. The Act ensures this by holding the institutions accountable should they abuse or compromise people’s data in any way. The enactment POPI Act considers personal information valuable and therefore aims to bestow upon the people certain rights concerning their data. The following summarizes the aim of the Act:

- when and how a person decides to share his or her data (requires consumer consent).
- the type and degree of data the person chooses to share (must be collected for legitimate reasons).

- transparency, responsibility and accountability on how the person's information will be utilized (restricted to the purpose) and warning if or when the information is used for the wrong reasons.
- providing the person access to their data and the right to have the personal data removed and destroyed should the person wish to do so.
- who can access the personal data, that is, there must be sufficient measures and controls set up to track access and prevent unauthorised people, even inside a similar organization, from accessing their data.
- how and where personal data is stored (there must be satisfactory measures and controls set up to shield private data from theft, or being undermined).
- the integrity and accuracy of personal data (for example, personal data must be captured correctly once collected, the institution must look after the personal information in a responsible manner).

Problem statement

Ngwenya and Ngoepe (2020; 2022) contend that CIoT raises the debate around privacy issues. Indeed, the implementation of CIoT directs the way personal data is collected, analyzed, used, and protected. In the process, consumers sometimes have to disclose personal information to receive certain benefits from service providers. Consumers often download applications and use them without mulling over the type of personal information they are exposing to the rest of the world (Ngwenya, 2020). Fong, Lam and Law (2017) state that mobile app users download and use applications without thinking about the type of personal information they expose. Some consumers are unaware that smart devices collect data and do not know their intended destination and usage. The benefits of CIoT come with privacy issues, especially when people do not correctly implement CIoT. Criminals may use one's data for illegal activities, such as compromising one's financial data and stealing identities. Palattella, Dohler, Grieco, Rizzo, Torsner, Engel and Ladid (2016) acknowledge that fitness and health tracking systems, smartwatches and sensor-rich smartphones may expose sensitive data such as someone's health status or life habits. They further state that the increase in the number of devices and the exchange of data multiplies the vulnerabilities of the systems and thus makes them more susceptible to privacy leaks and attacks from the internet.

Purpose and objectives of the study

The purpose of the study was to explore the data privacy issues faced by consumers of IoT in South Africa. It is essential to promote the safer adoption of CIoT and associated mobile apps in South Africa, as consumers of IoT continue to interact with smart things. The specific objectives were to:

- determine the technical approaches in dealing with data privacy
- analyse the dynamics and experiences of consumers of IoT concerning data privacy in the South African context.

Literature review

Privacy is a significant concern for consumers when adopting new technologies and substantially influences adoption. Alghamdi and Beloff (2014) state that consumers must feel safe about their privacy when interacting with systems such as the CIoT. Rose, Eldridge and Chapin (2015) state that the full potential of CIoT relies upon procedures that respect personal

privacy decisions over a wide range of desires. The data streams and consumer specificity afforded by CIoT devices can unlock incredible and unique value for consumers of IoT. However, concerns about privacy and potential harms might hold back the full adoption of CIoT. This stance implies that privacy rights and regard for consumer privacy expectations are integral to ensuring consumer confidence in the CIoT.

Helberger (2016) points out that profiling and targeting are usually associated with data protection laws and privacy. Consumer laws need to play an essential role in protecting the legitimate interests of consumers and guaranteeing a fair balance between consumers, providers of smart things and services, advertisers, insurance companies and other stakeholders. CIoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in opting out of specific data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of consumers. While these are significant challenges, they are not insurmountable. Rose et al. (2015) assert that IoT stakeholders should develop a strategy that respects individual privacy choices across a broad spectrum of expectations. The development of such an approach should happen while fostering innovation in new technology and services and taking advantage of the benefits of CIoT.

The fulfilment of customer privacy requirements is quite tricky. More often than not, we go on with our daily lives without thinking about personal data privacy issues. Cloud computing and the network epitomise the importance of trusting data. As much as cloud service providers reiterate that we have nothing to worry about when our data is in the cloud, it is essential to understand where the data resides if we are concerned about privacy. Can the information be leaked from that location?

Internet of Things

The IoT is about connecting everything on earth with the help of the internet. The ubiquitous connectivity and communication among the objects transform the ability to collect, analyse and distribute the data so that any stakeholder can gain insights and thus proactively perform helpful actions. Palattella et al. (2016) made a distinction between the CIoT and the industrial Internet of Things (IIoT) as below:

- **CIoT** – This is when we use IoT technology for consumer-oriented applications. In CIoT, data volumes and rates are low. It is the interconnection of consumer electronic devices and anything belonging to consumers' environments, such as homes, offices, wearables and cities.
- **IIoT** is when IoT is machine oriented, implying machine-to-machine communication with a distributed control. In essence, once implemented, IIoT does not require human intervention. It is when operational technology (OT) and information technology (IT) meet. It allows smart machines, networked sensors and data analytics to improve business-to-business (B2B) service industries. Such improvements may range from manufacturing to mining to public services. In IIoT, data volumes are very high, hence the term big data.

Data privacy concerns

This section discusses how data collection, storage and transfer affect data privacy problems. It provides a broad spectrum of recent advancements and methodologies for ensuring data privacy within IoT systems, offering valuable insights and potential frameworks to enhance

your paper on data privacy challenges in IoT. Privacy is a significant concern for consumers when adopting new technology and has a substantial influence on the adoption of technology. Yang (2022) provides an overview of current privacy-preserving solutions in IoT systems, including security protocols, network solutions, and data storage and sharing approaches. The next section explores the three areas where data privacy can be compromised.

Data collection

The first step in the IoT data lifecycle is data collection. Devices gather information from their surroundings, which can range from temperature readings to personal user information. While this data can be invaluable for improving the user experience and device functionality, it also poses significant privacy concerns. In South Africa, the POPIA governs the collection of personal data. According to the POPIA, personal data can only be collected for a specific, explicitly defined and lawful purpose, and the data subject must be aware of the purpose of the collection. (POPIA, 2013).

Moqurrab, Anjum, Tariq and Srivastava (2023) suggest instant anonymity as a lightweight semantic privacy-preservation framework that improves the usefulness of data in the IIoT by making classification more accurate and reducing the amount of time needed for computation. It does this by addressing the problems with existing privacy protection methods such as k-anonymity. Perera, Ranjan, Wang, Khan and Zomaya (2015) suggest that collecting data through IoT solutions and analysing it on a large scale can significantly benefit consumers and businesses. Furthermore, the authors state that collecting and analysing data can substantially impact society by increasing productivity and diminishing waste.

IoT technology can be used for data collection in various applications. Bojanowska (2019) discusses the potential of IoT for customer data collection in Customer Relationship Management (CRM) systems. Boualouache, Nouali, Moussaoui and Derder (2015) propose a Bluetooth Low Energy (BLE)-based data collection system for IoT, using smartphones as data collectors. Wei et al. (2022) review the scenarios and key technologies of unmanned aerial vehicles (UAV)-assisted data collection for IoT, highlighting the advantages of flexible deployment and high mobility of UAVs. Kawamoto et al. (2017) propose an efficient data collection method for location-based authentication systems as an application of industrial IoT, considering the requirements of the authentication system and regulating the network performance for data collection. In essence, IoT technology can be used for efficient and effective data collection in various applications.

Existing technologies and laws cannot support a privacy-guaranteed data management life cycle. From when the data is captured by the sensors embedded in IoT solutions to the point where there is the extraction of knowledge and permanently and securely deleting raw data, consumer privacy needs to be protected and enforced. IoT solutions can gain consumers' confidence by addressing the data management life cycle. We can solve the technological limitations through strict laws and regulations. These laws and regulations should include harsh and severe penalties for offenders and misusers. Is data collection violating consumer privacy in one way or another? Are consumers allowed to consent to data collection, or is data just collected discreetly without consumers' knowledge?

Data transfer

Once collected, the data is often transmitted to other devices or central servers for analysis. This transmission can be vulnerable to interceptions, leading to unauthorised access to sensitive information. In South Africa, the Cybercrimes Act aims to combat cybercrime by criminalising various offences related to data breaches. The Act makes it an offence to unlawfully access, intercept, or interfere with data (Cybercrimes Act, 2020).

Data transfers focus on how data transmission happens between objects, humans and analytical platforms. It also refers to how stakeholders share data with others or third parties. Is the way that shareholders share data violating privacy regulations such as the POPI Act in South Africa? Several technologies exist that can achieve information privacy goals during the transfer process. Researchers suggest that there are various technologies and protocols available for transferring data in CIoT applications. The technological approach explored technological steps that CIoT service providers can take to protect consumer data.

Guo, Chen, Chang, Hwang and Chang (2023) introduce a de-correlation neural network (DeCNN) for simultaneous estimation and privacy protection in IoT, significantly reducing the correlation coefficient between transmission and target data and thereby enhancing privacy. Wu, Peng, Tong and Li (2023) developed novel secure data transmission methods for IoT based on chaos theory and semi-tensor product compressive sensing (STP-CS), offering multilevel critical information concealment and robust privacy protection. Mary and Amalarethinam (2017) state that when a consumer outsources the data to the cloud, there is a possibility of attacking the data in transit. Hu, Chen, Yu, Meng and Duan (2022) propose a blockchain-enabled data-sharing scheme that combines edge computing and smart contracts to achieve secure and efficient data sharing. The message from these researchers is to place emphasis on the importance of innovative solutions for enhancing data privacy and security in the IoT.

Lysogor, Voskov, Rolich and Efremov (2019) present an architecture for a hybrid IoT-satellite network that uses a long-range low-power wide area network (LPWAN) terrestrial network for data collection and an Iridium satellite system for backhaul connectivity. Mämmelä, Karhula, and Mäkelä (2019) analyse the scalability of data transfer in massive IoT applications and suggest that more information brokers or gateway nodes are needed in the network as the sensor node population grows. Keophilavong, Widyawan and Rizal (2019) review different data transmission protocols for IoT applications, such as Message Queuing Telemetry (MQTT), Constrained Application Protocol (CoAP), Advanced Message Queuing Protocol (AMQP), Data Distribution Service (DDS) and Extensible Messaging and Present Protocol (XMPP) and propose an implementation model to evaluate the quality of the protocols when operating machine-to-machine communication. Overall, these researchers suggest that there are various approaches to transferring data for CIoT, and the choice of technology or protocol depends on the specific application and its requirements. Collectively, these studies underline the diversity of data transfer approaches in the IoT, emphasising that the choice of technology or protocol should be tailored to specific application needs and scalability requirements.

Weber (2010) talks about technologies that protect privacy, like virtual private networks (VPN), transport layer security (TLS), DNS security extensions (DNSSEC), onion routing and private information retrieval (PIR) systems. These are some of the technologies that CIoT service providers can use to send and receive data. These technologies form part of the proposed framework and tackle the technology part of the structure. Rewagad and Pawar (2013) believe that to induce trust when transferring data, the system should be able to perform

authentication, verification and encrypted data transfer, thus maintaining data confidentiality. The authors mention eavesdropping, tampering, man-in-the-middle attacks and identity spoofing as undesirable incidents that may happen to data in transit. They summarise these as follows.

- **Eavesdropping** – Zhang and Qu (2013) agree with Rewagad and Pawar (2013), who opine that eavesdropping is a severe concern for data in transit. For eavesdropping, the attacker gains access to the data path and the ability to monitor and read the messages. These risks are associated with the physical or perception layer.
- **Tampering** – Rewagad and Pawar (2013) state that data tampering can happen when the data is in transit. In this attack, the attacker may alter information while transiting to cloud storage. The same may happen once the data is in storage. When data tampering happens during transmission or at the destination, there is a compromise in the integrity of the data. Assembling a system such as a CIoT should be able to catch the threat of data tampering to avoid any potential damage to consumers.
- **Man-in-the-middle attack** – Zhang and Qu (2013) mention that this type of attack is common at the network layer. Data in transit happens at the network layer too. Rewagad and Pawar (2013) state that this type of attack occurs when an attacker infiltrates the communication channel to monitor the communication and modify the messages for malicious purposes.
- **Identity spoofing** – This attack happens when an attacker impersonates the user as the message's originator to gain network access. This occurs when the data is in transit.

All these researchers suggest that data should be encrypted or masked when it is in transit and are suggesting various methods to achieve the privacy of the data being transmitted.

Data storage

After transmission, the data is stored for further analysis and future use. The storage phase is crucial, as it presents opportunities for data breaches, especially if the data is stored in an unencrypted format. POPIA mandates that responsible parties must secure the integrity and confidentiality of personal information by taking appropriate measures to prevent loss, damage or unauthorised access (POPIA, 2013).

Zeng, Liu and Chang (2023) propose an optional privacy-preserving data aggregation scheme for fog-enhanced IoT networks, allowing users to choose between privacy encryption and no encryption, balancing convenience and privacy. Borra, Khond and Srivalli (2023) discuss security and privacy in IoT applications within cloud environments, highlighting the importance of comprehensive data collection, transmission and storage privacy-preserving technologies. Al-Fuqaha, Guizani, Mohammadi, Aledhari and Ayyash (2015) state that big data from IoT technology needs smart and efficient storage. The authors further allude to the fact that connected devices need mechanisms to store, process and retrieve data. After smart devices have collected data, the data can be stored anywhere worldwide. Data storage looks at the collected data in terms of where it is stored. Is it within a specific jurisdiction? Is it essential that the collected data reside locally or otherwise? What are the challenges if we do not know the data storage, and do consumers have a right to know such information?

Mary and Amalarethinam (2017) assert that cloud storage needs physical, logical and access control policies. Mahesh, Kumar, Ramasubbareddy and Swetha (2020) state that the use of smart devices will continue to grow for a long time, thus generating more data to be stored in

cloud storage. The authors suggest that storing more and more data in cloud storage facilities negatively affects the storage system's performance. CIoT service providers need to keep in mind the criticality of storage systems in performing their functions optimally, such as improving the utilisation of the storage, protecting the stored data and eliminating redundant data. Zhao, Rong, Jaatun and Sandnes (2010) raise some concerns about cloud storage fault tolerance and service availability. Their concerns relate to system failures or when a cloud service provider ceases business. This is a problem when CIoT providers depend on one cloud service provider. To avoid this, CIoT providers need the capability of migrating from one provider to another.

Mary and Amalarethinam (2017) further state that the cloud offers a vast space to store data. However, they quickly warn that data storage security is the most significant concern in cloud storage. Sultan, Varadharajan, Zhou and Barbhuiya (2020) state that there is much reluctance to store data in the cloud when the information is sensitive. This is especially true in the health industry. They further argue that consumers lose control over their data once they store it in the cloud. Mary and Amalarethinam (2017) discuss that consumers outsource storage services because of their flexible, efficient and seamless services. Sultan et al. (2020) state that public cloud storage is popular with individuals and organisations. They mention examples such as Microsoft Azure Storage Service, Amazon S3 and Google Cloud Storage. Developers of CIoT systems make use of these cloud services. There are many advantages to using these public cloud providers. One example relates to saving on the investment costs of building their storage. Another benefit is accessing ubiquitous data through the internet without worrying about managing and maintaining the outsourced data. There are increased concerns for data security and privacy when CIoT providers outsource data storage services to cloud providers. Data is normally stored around the world in distributed geographical areas. This makes it impossible for data owners or consumers to be certain where their information resides. While the researchers acknowledge the benefits of cloud storage, the security and privacy of the data stored in the cloud remain a concern.

When IoT devices collect sensitive information, such information may be stored anywhere worldwide. The health industry keeps a lot of sensitive patient information. The cloud service providers may misuse such data. For example, service providers may sell patient information to medical insurance companies. These providers can extract, modify, copy, destroy or even sell personal information. These concerns threaten personal information privacy. Xu et al. (2017) opine that cloud providers store consumers' data, such as photos and contacts, and make this data available to other mobile apps. The authors warn about the complexity of the data and that some underlying information may fall into the hands of cybercriminals. For example, a collection of photos may have tags with the consumer's notes.

Xu et al. (2017) worry about the adequacy of information protection in cloud storage. They state that existing platforms do not have adequate support for mobile apps' data management. They give an example of Dropbox on Android storing files in public storage, thus giving up all the necessary data protection. Sultan et al. (2020) state that the confidentiality of outsourced data needs preservation to prevent any entity, like service providers, from accessing data without proper authorisation. Access to information in public clouds requires suitable access control mechanisms and policies. The policies must restrict any person or entity from accessing data other than what the data owners allow.

Research methodology

This qualitative study explored the data privacy issues in consumer IoT through the triangulation of the narrative inquiry method and the Delphi technique. The use of the two designs assisted with the triangulation of the research. Many scholars agree on the definition of triangulation as combining methodological approaches, theoretical perspectives, data sources, investigators, and analysis methods in studying the same phenomenon (Hussein, 2009). The study sought to find meaning in the philosophy of experiences in a personal and social context from consumers of IoT using narrative inquiry. The narrative inquiry comprised interviews with six purposively selected participants who were users of mobile apps, labelled Participant A1 to Participant A6.

Using the Delphi method, the researchers purposively selected five individuals according to predefined guidelines and asked them to participate in three rounds of structured surveys. For this study, the sample consisted of experts from telecommunication industry selected through snowball sampling. The idea was that the participants needed to be users of mobile apps for IoT purposes in the case of narrative enquiry or be experts in the IoT industry for Delphi method. Once the researchers identified one or two participants, they sought referrals to people familiar with using mobile apps for IoT purposes. When saturation was reached, data collection was discontinued for narrative enquiry while Delphi method had three rounds of questions. The researchers generated themes from the collected data through thematic analysis. Thematic analysis is the process of identifying themes within qualitative data. The essential characteristic is the systematic process of coding, examining meaning and describing social reality through the creation of the theme.

Findings

Dinev and Hart (2006) discuss the trade-off between disclosing one's personal information for associated benefits. They describe two perspectives: privacy benefits and privacy risks. The authors challenge the notion that absolute privacy is unattainable. Individuals make decisions in which they give up a certain amount of privacy in exchange for outcomes that they believe are worth the risk of information disclosure. Some participants believed it was up to the consumers to protect their information. They were concerned that excessive data protection would stifle innovation. Participant A3 observed that:

> "Most IoT devices I have come across display a privacy policy that the consumer must agree to whenever he switches them on."

He gave an example of a 'Mercedes me connect' app.

During the narration, the majority of the participants stated that the terms and conditions or privacy policies that come with software and devices are too long, making it impractical to read them before using the CIoT system. The general consensus was that these privacy policies were time-consuming and unnecessary. The participants generally agreed that they wanted to keep their data private, and the key point was that they saw their personal information as a valuable asset. Participant A5 noted that:

> "I am not aware whether my personal information resides on the smart device or somewhere else".

All consumers believed that when they used IoT devices, service providers tracked them. They monitor their behaviour patterns, locations, spending habits and health, to name a few. In most cases, they do this without the consumer's knowledge.

Participant A2 stated that his Fitbit wearable monitors his heart rate, sleep patterns and physical activity. He stated that:

> "I am well aware that they follow my actions and my health status. I am okay with it because they noted these in the terms and conditions that apply before using the device."

Participants A1 and A6 expressed concern about criminals stealing their information. They discovered that they began using fake email addresses and other accounts as a result of the concerns. To register to use websites or mobile apps to access the CIoT system, they would create accounts that had nothing to do with their personal information. Some participants resorted to creating fake email accounts and turning off usage tracking. For example, Participant A4 expressed his main concern about location-related data by saying:

> "Location-related data, such as when using the navigation system in a car or using wearables that track me when doing road running, worries me a bit. This worry is mainly because these reveal things like my place of work, the places I frequently visit, my home, and any other daily routines. I do not know what would happen if criminals hacked me and traced me. Additionally, hackers could easily impersonate me after hacking the IoT system and gaining access to all my data. They could commit crimes using my information by pretending to be me."

Sharing personal information was less of an issue for Participant A3. He believed that:

> "The global brands take all the necessary steps to ensure the information shared with their partners is not used for nefarious purposes. I feel I am positively contributing to innovation when sharing my information with a service provider such as the IoT. In future, they can improve the services using the provided data. I am also aware that these companies can resell my information. However, I believe it's for the greater good".

Participant A2 justified the use of CIoT by considering the benefits and weighing them against the risks. He gave the following justification:

> "I am worried about how these companies use my personal information, but the convenience of using the services outweighs the risks. For example, we still buy and drive cars, even though car accidents happen constantly. We still board aeroplanes, despite some reported air crashes."

Participant A1 believed that using home automation systems and connecting them to the internet posed security risks and a threat to homeowners. However, he quickly stated that the advantages of protecting his home from burglars outweighed the risks of data privacy breaches. Participant A5 felt that companies are not transparent about how they use personal data. She stated that:

> "They should always declare what they will do with our data. The data belongs to me, and thus I feel I have a right to know what is happening to any data related to me. I think most, if not all, companies are suspect when it comes to declaring their intentions

> concerning our data. My other problem is that if they happen to declare, they use jargon, which makes it hard to decipher what they are trying to convey."

None of the participants could explain what IoT providers do with the data they collect. Participant A3 raised his concerns and stated that:

> "I worry about the things that can be done using my personal information. The damage can be very dire, and I have heard of stories whereby people's identities landed in the wrong hands, resulting in stolen identities. My brother was once a victim, but luckily for him, he took action before the damage was too much."

Participant A5, who had previously been a victim of identity theft and house robbery, was deeply concerned about security and privacy. His past experiences influence the intensity of his concerns. He acknowledged that there is concern about the physical safety of his home. The challenge or dilemma is to strike a balance between online security and data privacy concerns and the physical break in at his home. He used camera systems that he can access via his mobile phone. The phone connected to his house via the internet. He was concerned about the possibility of someone stealing his online profile. However, he perceived an even greater threat when people can break into his home and rob his family at gunpoint. He mentioned the following:

> "I was once a victim of stolen identity and a victim of house robbery. The question for me is to balance the level of trust in the systems I use to protect my home. I tried to use fake profiles as much as I could to avoid criminals interfering with my real profile or identity."

The experts' opinions addressed the majority of the consumer concerns, as well as the technological and legal approaches to data privacy in the CIoT. They all agreed on the need for new legislation that specifically addresses IoT. Experts expressed concern that current legislation is insufficient to address IoT issues. For example, South Africa's POPIA and Consumer Protection Act do not fully address consumer IoT concerns. In addition to the legal instruments, the experts agreed that:

- there is a need for hardware and software design methodology that can help designers and developers to deliver more secure devices
- there are standardised security protocols
- blockchain technology or other distributed ledger technologies are used to establish shared trust in information created and exchanged by smart things and people
- there is a focus on secure physical infrastructure, operations systems and storage.

Many participants believed that CIoT service providers had too much access to and control over personal information. This study discovered that people who have previously been victims of personal information breaches are more concerned about their data privacy on IoT devices. CIoT service providers must be more transparent with their users and give them more control over their privacy. The consumers' themes were summarised as follows:

- Identity theft
- Financial risks
- Selling of personal information
- Location-based tracking

- Medical privacy
- Unfair discrimination due to profiling

Interpretation and discussion

Consumers' experiences influence future behavioural intentions. This means that how consumers perceive privacy concerns influences how they approach information privacy issues. Some of the IoT consumers interviewed expressed no technical knowledge or concerns. The terms and conditions or policies of CIoT devices must be clearly displayed to the general consumer who lacks technical knowledge. The service providers must make their information practices clear. The legal instrument must enforce this in such a way that it becomes standard practice for all CIoT service providers. The information should be clear and include explicit warnings about the potential dangers to consumers from using the device or system. CIoT service providers should be open about the data they collect, process, store, and use. Consumers should be educated about the dangers of using IoT devices. Consumers must understand that the risks of CIoT are the same, if not greater, than any other online dangers to personal information.

Data privacy refers to personal information. While businesses see consumers accepting their terms and conditions, laws like the POPIA, aim to give consumers back control over their personal data. Some experts believed that once a consumer accepts the terms and conditions of a CIoT provider, they relinquish their rights to their personal information. This is incompatible with human rights in general. In South Africa, it violates the POPIA, the CPA and the ECT Act.

The findings suggested that interactions with CIoT assemblages provide positive experiences. These positive experiences encourage adoption and use. PII went beyond the consumer's known information like age, gender, race and other characteristics. Smart devices can help consumers extend their identities. They can identify consumers because smart things generate data about their location, preferences, and shopping habits, among other things. Routine and frequent use can help people integrate their identities with things. According to the data collected, consumers' experiences show that smart devices are an important part of their lives.

Consumers' revelation that the terms and conditions or policies that accompany CIoT systems imply that they have not read those policies at all. Consumers must take responsibility for their actions. If they do not read and understand the "small print," they should not be surprised to learn that third parties use their personal information for unknown purposes. The idea is that if a person cannot read the terms and conditions before using a service, he or she cannot blame anyone else for the alleged misuse. The experts disagreed, believing that consumers could not fully bear the responsibility for data privacy. According to the researchers, data privacy requires a collaborative effort from all stakeholders. None of the stakeholders should delegate their responsibilities to others. To avoid ambiguity, legal instruments should specify the lines of responsibility.

Consumers of IoT expressed concern about companies and criminals using their data for evil purposes. However, the findings indicated that consumers value the convenience of IoT technology. The findings also indicate that perceived privacy risks and personal interests influence consumers' future behavioural intentions to adopt CIoT. The consumer is aware that location-based information is being tracked but still continues to use the devices intentionally. For example, services may run in the background, or a user may forget to log out of a smart

device or system. The difficulties are exacerbated when CIoT service providers track personal information, and the consumer is unaware that the service provider is monitoring them. Sometimes, these location-based services connect to social media, exposing consumers' data to the rest of the world. When this occurs, criminals may use the information to carry out their criminal activities. Kidnapping, breaking into empty homes and car theft are all examples of crimes.

When location-based information connects to social media, criminals can use it to commit crimes like breaking into an empty house. In some cases, the intentional recording of personal data occurs in the background. A good example is a health monitoring service that consistently monitors an individual's critical health parameters without constantly notifying them. Therefore, it is critical to understand usage patterns and perceptions from the consumer's perspective. This understanding will help develop IoT services while keeping appropriate privacy and security standards in mind.

Conclusion and recommendations

This study used the narrative inquiry method and the Delphi technique to explore the data privacy issues associated with consumer IoT. The collected data was analysed using thematic analysis. The researchers and participants generated data privacy themes, indicating significant concerns about privacy in consumer IoT. Despite the concerns raised, all participants believed that the benefits outweighed the negatives. They emphasised the importance of dealing with concerns decisively in order to capitalise on technology, stimulate economic growth, and reduce societal ills.

The study examined data privacy from a variety of angles. A CIoT system can compromise data from collection to storage and transfer points. The researchers recommend that consumers use trusted devices approved by the Independent Communications Authority (ICASA) and the South African Buro of Standards (SABS) in South Africa. If ICASA has not tested the sensors or devices that collect consumer data, they may infect other internet-connected systems. Furthermore, this would be a violation of statutory bodies and legal instruments.

Consumers must accept responsibility for their actions when dealing with CIoT personal data, and all other stakeholders must also act responsibly when dealing with consumer data. Consumers of IoT lack complete confidence and control over how service providers use the data they share and thus do not trust the CIoT ecosystem. The researchers recommend specific legal instruments that set clear boundaries for the responsible parties in terms of data privacy. Privacy policies should not contradict national laws, and national laws should contact the international regulator. Companies must ensure that their policies do not violate fundamental human rights such as privacy, safety and the freedom to choose, among others. The researchers advise against using a centralised system and instead recommend distributed ledger technology. Among other risks, stealing personal information (identity theft) becomes more difficult in distributed systems.

ICASA must work on a legal instrument that explicitly addresses IoT in South Africa. The legal tools should address how we approach data privacy, from collection to transfer and storage. The risk of hackers stealing personal information from storage is high, and the incident highlighted these risks. The legal instrument must be transparent about where CIoT service providers can store their data. For example, how can consumers or stakeholders file legal claims if the service is provided in South Africa but the data is stored in the United States? Some

countries do not even have consumer protection laws, and countries such as South Africans which uses some of these overseas storage services, may be at risk because they have no legal recourse. As a result, the researchers recommend that ICASA should require service providers to store consumer information in South Africa.

Service providers must ensure that personal information is transferred from devices to storage areas using secure channels. The experts recommended using strong passwords and security exchange protocols. ICASA must be clear about the responsibility of the service provider in preventing hackers from stealing personal information. Service providers frequently use personal information without the consumer's permission. The legal instrument must be strict in terms of how service providers can use personal information and must respect the privacy of consumers. The legal instrument should prevent marketers from doing whatever they want with consumers' information.

There is genuine concern about private information stored on IoT devices. Many participants believed that IoT companies have complete control over their personal information. Some participants resorted to creating fake email accounts and turning off usage tracking. According to the findings of this study, individuals who have been exposed to or were victims of personal information breaches are more concerned about the privacy of their information on IoT devices. Technology companies should be more transparent with their users and give them more control over their privacy. The majority of participants believed that well-known global brands posed security risks. Any perceived security threat is constraining and limiting rather than positive and enabling.

Consumers' experiences with privacy issues and perceptions of their ability to protect privacy influence their behaviour. Some IoT consumers are general users with no technical knowledge or concerns. In the interest of overall consumer protection, IoT devices display specific information about their data practices. This should include explicit warnings about the risks they may present to consumers. IoT companies and manufacturers must be much more transparent about the data they collect and how it is processed, stored and used. It is necessary to educate all IoT users about the dangers of using IoT devices, which are the same as connecting to the internet.

The study discovered that PII goes beyond the consumer's known information, such as age, gender, race and other characteristics. Smart devices can help consumers extend their identities. This is because smart things collect data on consumers' location, preferences and shopping habits, among other things. Routine and habitual use can help people integrate their identities with things. According to the data collected, consumers' experiences highlight the importance of smart devices in their lives.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials,* 17(4): 2347-2376.

Alghamdi, S. and Beloff, N. 2014. *Towards a comprehensive model for e-Government adoption and utilisation analysis: The case of Saudi Arabia.* Paper presented at the 2014 Federated Conference on Computer Science and Information Systems, Warsaw, Poland.

Bojanowska, A.B. 2019. Customer data collection with Internet of Things. *MATEC Web of*

Conferences. https://doi.org/10.1051/matecconf/201925203002

Borra, S.R., Khond, S. and Srivalli, D. 2023. Security and privacy aware programming model for IoT applications in cloud environment. *International Journal on Cloud Computing: Services and Architecture*, 13(1): 1-12.

Boualouache, A., Nouali, O., Moussaoui, S. and Derder, A. 2015. A BLE-based data collection system for IoT. *2015 First International Conference on New Technologies of Information and Communication (NTIC)*, 1-5.

Caron, X., Bosua, R., Maynard, S.B. and Ahmad, A. 2016. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Compututer Law and Security Review*, 32: 4-15.

Dinev, T. and Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research,* 17(1): 61-80.

Fong, L.H.N., Lam, L.W. and Law, R. 2017. How locus of control shapes intention to reuse mobile apps for making hotel reservations: Evidence from chinese consumers. *Tourism Management,* 61: 331-342.

Guo, C., Chen, C.-H., Chang, C.-C., Hwang, F.-J. and Chang, C.C. 2023. De-correlation neural network for synchronous implementation of estimation and secrecy. *IEEE Communications Letters,* 27: 165-169.

Helberger, N. 2016. *Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law*. [Online]. Available WWW: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717 (Accessed 16 February 2020).

Hu, B., Chen, Y., Yu, H., Meng, L. and Duan, Z. 2022. Blockchain-enabled data-sharing scheme for consumer IoT applications. *IEEE Consumer Electronics Magazine,* 11: 77-87.

Hussein, A. 2009. The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work,* 4(1): 1-12.

Kawamoto, Y., Nishiyama, H., Kato, N., Shimizu, Y., Takahara, A. and Jiang, T. 2017. Effectively collecting data for the location-based authentication in Internet of Things. *IEEE Systems Journal,* 11: 1403-1411.

Keophilavong, T., Widyawan, W. and Rizal, M.N. 2019. Data transmission in machine to machine communication protocols for Internet of Things application: A review. *2019 International Conference on Information and Communications Technology (ICOIACT)*, 899-904.

Lysogor, I.I., Voskov, L., Rolich, A. and Efremov, S. 2019. Study of data transfer in a heterogeneous LoRa-Satellite network for the Internet of Remote Things. *Sensors (Basel, Switzerland),* 19.

Mahesh, B., Kumar, K.P., Ramasubbareddy, S. and Swetha, E. 2020. A review on data deduplication techniques in cloud. In *Embedded systems and artificial intelligence* (pp. 825-833): Springer.

Mämmelä, O., Karhula, P. and Mäkelä, J. 2019. Scalability analysis of data transfer in massive Internet of Things applications. *2019 IEEE Symposium on Computers and Communications (ISCC)*, 1-7.

Mary, B.F. and Amalarethinam, D.G. 2017. *Data security enhancement in public cloud storage using data obfuscation and steganography.* Paper presented at the 2017 World Congress on Computing and Communication Technologies (WCCCT).

Moqurrab, S.A., Anjum, A., Tariq, N. and Srivastava, G. 2023. Instant_Anonymity: A lightweight semantic privacy guarantee for 5G-enabled IIoT. *IEEE Transactions on industrial informatics,* 19: 951-959.

Neves, F., Souza, R., Sousa, J., Bonfim, M.S. and Garcia, V. 2023. Data privacy in the Internet

of Things based on anonymization: A review. *Journal of Computer Security*, 31: 261-291.

Ngwenya, M. 2020. Data privacy, security and trust in "consumer internet of things "assemblages and associated mobile applications in South Africa. PhD Thesis, Pretoria: University of South Africa.

Ngwenya, M. and Ngoepe, M. 2020. A framework for data security, privacy, and trust in "consumer internet of things" assemblages in South Africa. *Security and Privacy*, 3.

Ngwenya, M. and Ngoepe, M. 2022. Data trust in Consumer Internet of Things assemblages in the mobile and fixed telecommunication operators in South Africa. *South African Journal of Information Management*, 24(1) a1426. https://doi.org/10.4102/sajim.v24i1.1426

Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. and Ladid, L.J.2016. Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications,* 34(3): 510-527.

Peppet, S.R. 2014. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Texas Law Review,* 93: 85.

Perera, C., Ranjan, R., Wang, L., Khan, S.U. and Zomaya, A.Y. 2015. Big data privacy in the internet of things era. *IT Professional*, 17(3): 32-39.

Perez, A.J., Zeadally, S. and Cochran, J. 2018. A review and an empirical analysis of privacy policy and notices for consumer Internet of things. *Security and Privacy,* 1.

Rewagad, P. and Pawar, Y. 2013. *Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing.* Paper presented at the 2013 International Conference on Communication Systems and Network Technologies.

Rose, K., Eldridge, S. and Chapin, L. 2015. The internet of things: An overview. *The Internet Society*, 1-50.

Samania, A., Ghenniwa, H.H. and Wahaishi, A. 2015. *Ambient systems, networks and t echnologies (ANT 2015) privacy in Internet of Things: A model and protection f ramework.*

South African Government. 2013. *Protection of Personal Information Act 4 of 2013*. Government Printers: South Africa,

South African Government. 2020. *Cybercrimes Act 19 of 2020*. Government Printers: Pretoria.

Sultan, N.H., Varadharajan, V., Zhou, L. and Barbhuiya, F.A. 2020. A role-based encryption scheme for securing outsourced cloud data in a multi-organization context. *arXiv preprint arXiv:*2004.05419.

Weber, R.H. 2010. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1): 23-30.

Wei, Z., Zhu, M., Zhang, N., Wang, L., Zou, Y., Meng, Z., … Feng, Z. 2022. UAV-assisted data collection for Internet of Things: A survey. *IEEE Internet of Things Journal*, 9, 15460-15483.

Wu, W., Peng, H., Tong, F. and Li, L. 2023. Novel secure data transmission methods for IoT based on STP-CS with multilevel critical information concealment function. *IEEE Internet of Things Journal,* 10: 4557-4578.

Xu, Y., Hunt, T., Kwon, Y., Georgiev, M., Shmatikov, V. and Witchel, E. 2017. EARP: Principled storage, sharing, and protection for mobile apps. *GetMobile: Mobile Computing and Communications*, 20(3): 29-33.

Yang, G. 2022. An overview of current solutions for privacy in the Internet of Things. *Frontiers in Artificial Intelligence,* 5.

Zeng, Z., Liu, Y. and Chang, L. 2023. A robust and optional privacy data aggregation scheme for fog-enhanced IoT network. *IEEE Systems Journal*, 17: 1110-1120.

Zhang, W. and Qu, B. 2013. Security architecture of the Internet of Things oriented to perceptual layer. *International Journal on Computer, Consumer and Control (IJ3C),* 2(2): 37-45.

Zhao, G., Rong, C., Jaatun, M.G. and Sandnes, F.E. 2010. *Deployment models: Towards eliminating security concerns from cloud computing.* Paper presented at the 2010 International Conference on High Performance Computing & Simulation.

Ziegeldorf, J.H., Morchon, O.G. and Wehrle, K. 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks,* 7(12): 2728-2742.