Journal of Information Systems and Informatics
Vol. 4, No. 2, June 2022 e-ISSN: 2656-4882 p-ISSN: 2656-5935
http://journal-isi.org/index.php/isi Published By DRPM-UBD

Towards Privacy by Design on the Internet of Things (IoT) Use: A Qualitative Descriptive Study

Ahmad Luthfi[1], Emigawaty[2]

[1]Department of Informatics, Faculty of Industrial Technology, Universitas Islam Indonesia, Yogyakarta, Indonesia
[2]Department of Informatics, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
Email: [1]ahmad.luthfi@uii.ac.id, [2]emigawaty@amikom.ac.id

Abstract

From remote control and surveillance to energy and health monitoring, IoT devices provide cutting-edge services to improve our lives. Nevertheless, IoT technologies raise complicated, innovative privacy-related issues that might limit their widespread adoption. Due to the passive nature of many IoT devices, it may be challenging for users to understand that their personal information is being gathered. Therefore, this paper aims to examine the Privacy by Design IoT application idea. We adapted the seven principles of Ann Cavoukian's Privacy by Design, which were first developed. In this study's qualitative descriptive methodology with interview sections are used. The results indicate that the majority of IoT users agree with and have high expectations for the Privacy by Design concept to be one of the remedies to the imbalance between concerns about the risks and benefits of using IoT.

Keywords: Privacy by Design, Internet of Things, Qualitative Descriptive

1. INTRODUCTION

Through the use of network-based topologies of Internet-connected sensors and actuators, the Internet of Things (IoT) makes technology more advanced by enabling automation, personalisation, and remote control [1]. Even though IoT was initially intended for manufacturing and industrial spheres, the idea has found application in a wide range of settings, from public ones like smart cities to the most private ones like our homes and wearable technologies [2]. In addition, IoT devices provide innovative services to better our lives, from energy and health monitoring to remote control and surveillance.

At the same time, IoT technologies bring up complex and new concerns concerning privacy challenges that might prevent their comprehensive implementation [3]. IoT users may find it challenging to learn that their personal information is being collected because many IoT devices are passive in nature [2, 4]. Devices in public places can automatically gather information, while

occasionally, they rely on users to choose not to have their information recorded. IoT devices will intrude into traditionally private locations like the home and expand data collection strategies used online into offline configurations [5]. Data collecting will get closer and closer to our bodies and private locations as more and different kinds of sensors are launched [6].

IoT device penetration has resulted in a rapid accumulation of data, which offers a wealth of insights but also poses a wealth of privacy and security issues [7]. Organisations need to think about how the data is processed, given the rise in data volume. Moreover, individual consumers' privacy, for instance, may be violated by IoT systems, and they are rarely given a chance to learn about or object to the data collecting tactics being used against them [5, 6]. Even for primary users, IoT privacy protections are frequently inadequate, which results in poor privacy management procedures [5].

The connecting of IoT devices results in several potential privacy concerns. First, in the case of companies or IoT providers that offer hardware or services that have access to IoT datasets, there is an opportunity that they might use or share personal information for actions that are not in the public interest, including profiling, targeted advertising, or providing data to data aggregators [8]. Therefore, the ownership and control of the information, as well as the uses to which it will be put, must be taken into account when personal data is gathered via public IoT ecosystems like smart cities. Second, the organisation that receives IoT datasets might be able to reidentify them using auxiliary information. Inferences made from the dataset using artificial intelligence and machine learning techniques, for example, may reveal sensitive or even extremely private information [9]. This means that if the IoT dataset is used to train and merge, the related personal attributes are linked. Accordingly, information about individuals in the IoT dataset may indeed be easily identified.

Based on these potential privacy risks and violations, Privacy by Design for IoT use is crucial to preserving the individual's best interests above all else by providing measures such as substantial privacy defaults, adequate warning, and empowering user-friendly options [6, 8]. When storing or accessing personal data, Privacy by Design is a proactive method that encourages confidentiality compliance throughout IoT project lifecycles [10]. Also, the IoT requires Privacy by Design because privacy issues and accountability are becoming more important in a connected society. Therefore, this paper investigates the Privacy by Design concept of IoT use.

In this research, we adapted the seven foundational principles of Privacy by Design, formulated for the first time by Ann Cavoukian [11]. To obtain a comprehensive overview of the privacy by design concept in the IoT context, we

interviewed 15 potential IoT users. Then, we did qualitative descriptive to capture the current viewpoints on the implementation of the Privacy by Design concept. Based on the findings of this descriptive interview, it can be concluded that the majority of IoT users agree with and hold high hopes for the Privacy by Design idea to be one of the solutions to the disparity between worries about the risks and advantages of using IoT.

2. METHODS

This study employs interview sections in a qualitative descriptive method. In qualitative descriptive studies, incidents are described, analysed, and interpreted to reveal the causes of particular phenomena [12]. Qualitative descriptive research aims to provide a thorough summary of certain events that people or groups have observed. Finding out the characteristics of the key events under examination is the primary goal of qualitative descriptive data collection [13]. Hence, structured, open-ended, individual or focus group interviews ranging from light to moderate intensity are used to collect data [12, 13].

Furthermore, unlike most other qualitative methodologies, data analysis for qualitative descriptive investigation uses no pre-existing set of guidelines produced by the philosophical or epistemological position of the field that developed the particular qualitative research method. Instead, qualitative descriptive research is fully data-derived because codes are created from the data during the investigation. Qualitative descriptive studies are typically characterised by contemporary data collection and processing, similar to other qualitative research methodologies [13].

2.1. Research Methods

Several categories of IoT service consumers, including industrials, individuals, and researchers, participated in the study's interview. During April 1–30, 2022, the interview section was conducted online using the Google Meet platform. Procedure-wise, interview sections had to spend about 45 to 60 minutes on average answering four main questions from the interviewer. The results of the interview mechanisms that were given to the person who was the existing and the candidate of the IoT users will subsequently be used as primary research data.

2.2. Organising the Interview Section Instrument

In order to make it simpler to categorise and validate the findings of quantitative research using a structured question structure, the interview instrument in this study was separated into two main groups. First, we looked into the participant's demographics by asking them five key questions about their age, gender, education, employment status, administrative province of origin, and level of IT

usage. We next looked at user experiences with and viewpoints on IoT devices. Eight open-minded questions covering the user perception and personal thoughts about IoT use, general comprehensions related to the potential risks in using IoT, and the participant's general opinion about the personal and privacy issues in the IoT practice comprise this section's material for the participants. Third, we used the seven Privacy by Design questions to get the user's perspective on privacy issues with IoT use.

2.3. Theoretical Background

2.3.1 Benefits and Risks of the Internet of Things (IoT) Use

The phrase "Internet of Things" (IoT) was first introduced in 1999 by British technology pioneer Kevin Ashton to propose a system in which real things may be connected to the Internet by sensors [1]. In its simplest form, IoT is a network in which all physical items are connected to the Internet via network equipment or routers and exchange data [2, 3]. Through existing network infrastructure, IoT enables remote control of physical items. Additionally, this method offers autonomous control, which allows any gadget to operate independently of human input [1, 2].

IoT has the ability to have an impact on society, the environment, and the economy. Accurate knowledge of the condition, location, and identifying things that affect the environment and are a part of it enables individuals to make more informed decisions [1, 2]. Logistics, transportation, asset tracking, smart environments (houses, buildings, manufacturers, transportation, smart cities, industrial infrastructures), energy, defense, and agriculture are a few areas where IoT concepts have been used. IoT fundamentally affects all areas of society and undoubtedly has the ability to do so [1, 2, 4]

In addition to its advantages and merits, several important IoT-related problem areas are also investigated to explore some of the technology's most urgent problems and issues. Among them are interoperability, security, privacy, and legal [3]. In the security issues, for instance, the large amount of information that IoT devices collect makes them potentially very risky for confidentiality in terms of how the data is used and accessed [3-5]. An increasing concern is the ability to recognise an individual and their behavioural tendencies.

Furthermore, IoT device connectivity raises several possible other privacy issues [6, 7]. First, there is a chance that businesses or IoT providers who sell hardware or provide services and have access to IoT datasets will share or utilise personal information for purposes like profiling, targeted advertising, or giving information to data aggregators [8]. Therefore, while collecting personal data through open IoT ecosystems like smart cities, consideration must be given to the ownership and

control of the information as well as the purposes for which it will be used. Second, the company receiving the IoT datasets might be able to reidentify them using auxiliary data. Machine learning and artificial intelligence algorithms may be used to draw conclusions from the dataset that expose delicate or even incredibly confidential information [8, 9].

2.3.2 Privacy by Design

The idea of Privacy by Design was established in the 1990s to address the systemic consequences of substantial interconnected data systems and the ever-expanding ICTs. According to Privacy by Design, privacy cannot be guaranteed in the future just by adhering to legal requirements; instead, it must become an organisation's standard operating procedure [11]. The Trilogy of comprehensive applications that make up Privacy by Design includes (1) IT systems, (2) responsible business practices, and (3) physical design and networked architecture [11]. Bu these trilogies, all forms of personal information can be covered by the principles of Privacy by Design, but sensitive data like financial and medical records should be covered with extra vigour. The vulnerability of the data usually corresponds to how strong the privacy protections are. Therefore, the primary goals of Privacy by Design are to protect privacy and give individuals control over their information.

According to Ann Cavoukian [11], there are seven fundamental principles of Privacy by Design, as follows:

1. *Proactive not Reactive; Preventative not Remedia*
   Proactive rather than reactive actions are what define the Privacy by Design methodology. It foresees and terminates privacy-invading occurrences before they take place. Privacy by Design and its cures do not wait for privacy problems to manifest before taking action to address them. It seeks to stop them before they start.
2. *Privacy as the Default Setting*
   In order to provide the highest level of privacy, Privacy by Design ensures that all IT systems and business procedures automatically secure personal data. The right to privacy is not violated if a person does nothing. To maintain their privacy, the person need not take any action.
3. *Privacy Embedded into Design*
   IT systems and business procedures are built with privacy by design principles in mind. It is not tacked on after the event as an addition. As a result, privacy is now a crucial part of the fundamental functionality being provided. Without sacrificing functionality, privacy is an essential component of the system.
4. *Full Functionality (Positive-Sum, not Zero-Sum)*
   With Privacy by Design, no unnecessary trade-offs are made and all sovereign rights and goals are accommodated in a positive-sum "victory" way rather than the old-fashioned zero-sum method. By proving that it is conceivable to have both privacy and security, Privacy by Design does away with the façade of false equivalencies like privacy versus security.

5. *End-to-End Security*
   Adequate security measures are vital to privacy from start to finish. Privacy by Design extends safely across the entire lifecycle of the data involved since it is built into the system before the first information element is acquired. This guarantees that all data are safely stored and promptly erased after the operation is complete. Thus, Privacy by Design guarantees completion, safe information lifecycle governance from birth onward.
6. *Visibility and Transparency*
   Privacy by Design aims to reassure all stakeholders that whatever the business strategy or underlying technology operates by the stated pledges and purposes, subject to independent verification. Both consumers and providers may still see and understand how it works and its constituent elements.
7. *Respect for User Privacy*
   In order to comply with Privacy by Design, architects and operators must prioritise the needs of the individual by providing safeguards such as privacy protection defaults, adequate notice, and enabling user-friendly possibilities. Therefore, keep the user in mind.

3. RESULTS AND DISCUSSION

In this section, the research results will be presented in three groups. Firstly, the participants' demographic findings. Secondly, the findings from participant interviews are relevant to the general viewpoint and comprehension of the problem of potential hazards and privacy breaches in the IoT infrastructure. Third, the findings of the inquiry into how the Privacy by Design principles might be applied to IoT technologies. The demographic information of the interviewees who voluntarily participated in this study is shown in Table 1.

Tabel 1. Participant's Demographic

Question: ***Please provide your age, gender, education, employment status, administrative province of origin, level of IT***

Interviewee's ID	Interviewee's response
INTV#001	24, Male, Bachelor's degree, full-time, Central Java, novice user
INTV#002	29, Male, Bachelor's degree, full-time, Bali, novice user
INTV#003	35, Male, Master's degree, full-time, Central Java, knowledgeable user
INTV#004	27, Male, Master's degree, full-time, Yogyakarta, knowledgeable user
INTV#005	36, Male, Bachelor's degree, full-time, Yogyakarta, expert user
INTV#006	22, Male, Bachelor's degree, part-time, Bali, knowledgeable user
INTV#007	24, Female, Bachelor's degree, part-time, Yogyakarta, novice user
INTV#008	28, Male, Master's degree, full-time, Yogyakarta, expert user

INTV#009	33, Male, Master's degree, full-time, East Java, expert user
INTV#010	36, Male, Doctoral degree, full-time, Yogyakarta, expert user
INTV#011	25, Female, Bachelor's degree, temporary, Yogyakarta, novice user
INTV#012	23, Female, Bachelor's degree, temporary, Bali, novice user
INTV#013	25, Female, Bachelor's degree, part-time, East Java, knowledgeable user
INTV#014	32, Male, Master's degree, full-time, Central Java, knowledgeable user
INTV#015	40, Male, Doctoral degree, full-time, Central Java, expert user

From the results of participant's demographics in Table 1, it can be explained that:

1) Out of a total of 15, 9 IoT users (or 60%) are between the ages of 20 and 30, whereby 6 are between the ages of 31 and 40 (40%). This indicates that the majority of the study's interviewees are of productive age. Regarding gender issues, 11 participants (73%) were male, while 4 participants (27%) were female.
2) Regarding the participants' formal educational backgrounds, the majority of them are undergraduate (bachelor's degree), with 8 of them (54%), followed by 5 master's graduates (33%) and 2 graduates of PhD programs (13%). In terms of their employment position, 3 respondents are part-time (20%), 10 participants are full-time (66%), and the final 2 are temporary employers (14%).
3) Considering the administrative regions of the informants in this study, it can be noted that they are from four provinces in Java and Bali: Central Java, with 4 users (27%), Yogyakarta with 6 users (40%), East Java contribute 2 respondents (13%), and Bali participate 3 users in total (20%).

Tabel 2. Participant's General Perspective in Using IoT

Question #1: ***When you hear the term "Internet of Things," what is the first thing that comes up to your viewpoint?***

Interviewee's ID	**Interviewee's response**
INTV#001	Smart home appliances
INTV#002	Complicated computer networks and sophisticated devices
INTV#003	Smart thing but not so useful for personal needs
INTV#004	Huge IoT networks with big data platforms included
INTV#005	Programs that make people's life much easier dan more fun
INTV#006	Something that needs to be used immediately
INTV#007	The use of smart home equipment
INTV#008	Connecting home devices with Internet technology
INTV#009	Helping people to do sophisticated artificial things

INTV#010	Many sensors can be connected to various devices
INTV#011	Using a smartphone to control home electricity devices
INTV#012	Useful programs but tend to be more expensive things
INTV#013	Manage different types of devices, such as refrigerators, fire alarms, doors and windows, and security systems
INTV#014	Easy to access home appliances at any time and anywhere
INTV#015	Smart platforms that make society's lives easier and more pleasurable

The outcomes of participant's general perspective in Using IoT (Question#1: When you hear the term "Internet of Things," what is the first thing that comes up to your viewpoint?) in Table 2 can be justified as follows:

1) Many interviewees described IoT technology as synonymous with the idea of a smart house and connected devices, high-tech equipment to assist the convenience of daily activities. At the same time, other participants described the IoT as a system that uses numerous sensors and huge data and can be managed by smartphone at any time and anywhere.
2) On the other hand, some interviewees believe that the IoT is a complicated and enormous computer network system connecting various objects with the help of existing sensors. The aforementioned items include household media, such as security systems (CCTV), smart doors and windows, and smart fire alarms.
3) Despite all of these individual viewpoints, they all agree that the IoT is a smart platform that can help many people carry out their social and personal activities more conveniently and comfortably.

Based on these above three main categories of viewpoints, it can be indicated that every interviewee comprehended the fundamental ideas and definitions of the IoT and certain real-world applications. Before exploring information on potential risks and violations of personal data in IoT use, it is essential for researchers to establish their equality of thoughtful.

Tabel 3. Participant's General Perspective in Privacy Issues

Question #2: ***Do you currently detect or perceive any broader risk of IoT usage compromising personal information? Please provide further details in your response.***

Interviewee's ID	**Interviewee's response**
INTV#001	Personal information will be collected and shared with others
INTV#002	Personal data breaches
INTV#003	Individual data theft
INTV#004	Safe network platforms but insecure personal data transmission
INTV#005	Data breaches and invasion of personal privacy

INTV#006	Too much reliance on smart home appliances raises the possibility of intrusion
INTV#007	Data breaches of privacy and disturbances caused by deliberately
INTV#008	Smart devices gather data in ways that the ordinary user is unaware of
INTV#009	It gathers a variety of information that, the misused, might be hazardous
INTV#010	The risk of privacy infringement is increased because of our over-reliance on smart home appliances
INTV#011	Privacy and data protection issues may arise dangerously
INTV#012	Capturing individual user data and identifying user behaviours
INTV#013	To protect personal information, the three key issues are authentication, authorisation, and access control
INTV#014	The data that is transmitted via the IoT network is private and secure
INTV#015	The owner, risk of identity, or habit exposure are all data sources that IoT companies can get.

Meanwhile, regarding the results of the interview sections with the focus of the subsequent question (Question #2: Do you currently detect or perceive any broader risk of IoT usage compromising personal information?), in Table 3, this can be described in more detail as follows:

1. Some characteristics of dominance are severe and of concern to IoT users. These considerations include scenarios where customers might readily acquire their data when connected to IoT networks and services. Data can so readily be stolen or shared with irresponsible parties.
2. IoT is thought to present prospects for potential data leakage, which brings us to the next issue. The IoT service provider may have purposefully violated users' privacy and accessed their data. The potential for personal data to be misused for a variety of reasons, including criminal activity, is a concern when data is transferred from one server to another.
3. Additionally, IoT users have severe concerns about the possibility of identifying user behaviour due to the simplicity with which personal data may be collected. As a result, it's important to secure the transmission of personal data via the IoT network. One respondent provided three main points of view about the security of personal information. Access control, authorisation, and authentication make up the three points.

In general, it can be observed from the results of the interviews about the potential for personal data breaches presented in Table 3 that interview participants could recognise the potential hazards. Figure 1 shows the keywords that may be generated to illustrate some of the potential dangers of data breaches in the IoT system.

Journal of Information Systems and Informatics
Vol. 4, No. 2, June 2022
p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Figure 1. Several Keywords of Potential Risks in IoT Use

Subsequently, Table 4 presents the results of the extent to which the IoT user agrees or disagrees about using the Privacy by Design concept.

Tabel 4. Participant's Perspective Towards the Privacy by Design in IoT Use (N participant=15. Scales= Strongly agree, Agree, Disagree, Strongly Disagree)

No	Privacy of Design Principles	Frequency	Percentage of user's response
1	**Proactive not Reactive; Preventative not Remedia (**Question: "*To what extent do you agree or disagree that Privacy by Design should consider privacy issues before they arise?)*	10	66% (strongly agree)
2	**Privacy as the Default Setting (**Question: "*To what extent do you agree or disagree that Privacy by Design should include in the IoT systems by default?)*	13	87% (strongly agree)
3	**Privacy Embedded into Design (**Question: "*To what extent do you agree or disagree that privacy is a crucial component of the system and business procedures?)*	13	87% (strongly agree)
4	**Full Functionality-Positive-Sum, not Zero-Sum (**Question: "*To what extent do you agree or disagree that Privacy by Design does away with the façade of false equivalencies like privacy versus security?)*	12	80% (agree)
5	**End-to-End Security (**Question: "*To what extent do you agree or disagree that Privacy by Design guarantees completion, safe information lifecycle governance from birth onward?)*	14	93% (Strongly agree)
6	**Visibility and Transparency (**Question: "*To what extent do you agree or disagree that Privacy by Design that both consumers and providers may still see and understand how it works and its constituent elements?)*	9	60% (Agree)

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

7	**Respect for User Privacy (**Question: "*To what extent do you agree or disagree that Privacy by Design must prioritise the needs of the individual by providing safeguards such as privacy protection defaults, adequate notice, and enabling user-friendly possibilities?)*	15	100% (Strongly agree)

From the outcomes of participant's general perspective in Using IoT and Privacy Concerns in Table 4, it can be justified that:

1) About 66% of participants strongly believe that Security by Design should consider privacy concerns before they develop in relation to the first principle, which is Proactive not Reactive; Preventative not Remedial. This demonstrates that the majority of IoT users do not think Privacy by Design can stop the theft of personal data.
2) According to the second and third principles, which are privacy as the default setting and privacy incorporated into the design, 13 out of the total 15 participants (or 87%) strongly believe that Privacy by Design should be a standard feature of IoT systems.
3) A total of 12 interviewees (80%) strongly agreed that Privacy by Design could get rid of false equality facades like privacy vs security when it comes to the fourth principle's issue of Full Functionality-Positive-Sum, not Zero-Sum.
4) A remarkable 93% of interview participants believed that Privacy by Design could ensure complete, secure information lifecycle governance from the moment of birth with regard to the End-to-End Security component, which is mentioned in the fifth principle.
5) On the elements of Visibility and Transparency, which differ slightly from the preceding tenets, only roughly 60% of the interviewees completely concurred that Privacy by Design may still be seen and understood by customers and service providers, as well as its component parts. This is feasible because IoT users have little knowledge and experience with the idea of transparency in the context of consumer transactions.
6) Finally, all interviewees (100%) believed and strongly agreed that Privacy by Design should prioritise individual requirements by offering safeguards, including privacy protection settings, proper notification, and user-friendly options. This goes against the principle of Respect for User Privacy.

4. CONCLUSION

According to the findings of this descriptive interview, most IoT users concur and have high expectations that the Privacy by Design idea can help bridge the gap between worries about the risks and advantages of using IoT. As a brief summary, the outcomes and conclusions of this interview session are exclusive to one nation.

They cannot be generalised to other places with varying degrees of development and comprehension. As a result, it is also required to conduct more thorough observations by including more interview subjects with a variety of backgrounds and IoT technology usage experiences.

REFERENCES

[1] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications,* vol. 3, no. 5, 2015.
[2] N. Ali Jasim and H. T. S. ALRikabi "Design and Implementation of Smart City Applications Based on the Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 13, 2021.
[3] X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," *Digital Communications and Networks* vol. 7, no. 3, 2021.
[4] P. Bellini, P. Nesi, and G. Pantaleo, "IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies," *Jurnal of Applied Science,* vol. 12, no. 3, 2022.
[5] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies," *Jurnal of Applied Science,* vol. 12, no. 3, 2022.
[6] M. I. Ahmed and G. Kannan, "Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring," *Journal of King Saud University - Computer and Information Sciences,* 2021.
[7] D. G. Glance and R. Cardell-Oliver *Privacy of Edge Computing and IoT. Book Secure Edge Computing*. CRC Press, 2021.
[8] Y. Ashibani and Q. H. Mahmoud "A Behavior Profiling Model for User Authentication in IoT Networks based on App Usage Patterns," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society,* 2018.
[9] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Journal of Internet of Things,* vol. 11, 2020.
[10] J. van Rest, "Designing Privacy-by-Design," *Designing Privacy by Design,* vol. 8319, 2014.
[11] A. Cavoukian, "Privacy by Design: the definitive workshop," *Identity in the Information Society,* vol. 3, no. 2, 2010.
[12] L. Bloomberg and M. Volpe, *Completing Your Qualitative Dissertation: A Road Map From Beginning to End*. 2018.
[13] V. S. Brayan, N. Smith, and C. Mitton, "The Qualitative Descriptive Approach in International Comparative Studies: Using Online Qualitative Surveys," *International Journal of Health Policy Management,* vol. 7, no. 9, 2018.