computers

MDPI

Article

Privacy Preservation Instruments Influencing the Trustworthiness of e-Government Services

Hilal AlAbdali [1,*], Mohammed AlBadawi [1], Mohamed Sarrab [2] and Abdullah AlHamadani [1]

[1] Department of Computer Science, Sultan Qaboos University, Muscat 123, Oman; mbadawi@squ.edu.om (M.A.); abd@squ.edu.om (A.A.)
[2] Communication & Information Research Center, Sultan Qaboos University, Muscat 123, Oman; sarrab@squ.edu.om
* Correspondence: s24096@student.squ.edu.om

Abstract: Trust is one of the most critical factors that determine willingness to use e-government services. Despite its significance, most previous studies investigated the factors that lead to trusting such services in theoretical aspects without examining the technical solutions. Therefore, more effort is needed to preserve privacy in the current debate on trust within integrated e-government services. Specifically, this study aims to develop a model that examines instruments extracted from privacy by design principles that could protect personal information from misuse by the e-government employee, influencing the trust to use e-government services. This study was conducted with 420 respondents from Oman who were familiar with using e-government services. The results show that different factors influencing service trust, including the need for privacy lifecycle protection, privacy controls, impact assessments, and personal information monitors. The findings reveal that the impeding factors of trust are organizational barriers and lack of support. Finally, this study assists e-government initiatives and decision-makers to increase the use of services by facilitating privacy preservation instruments in the design of e-government services.

Keywords: e-services; integration; e-government; privacy; privacy by design; software engineering

Citation: AlAbdali, H.; AlBadawi, M.; Sarrab, M.; AlHamadani, A. Privacy Preservation Instruments Influencing the Trustworthiness of e-Government Services. *Computers* **2021**, *10*, 114. https://doi.org/10.3390/computers10090114

Academic Editor: George Angelos Papadopoulos

Received: 23 August 2021
Accepted: 7 September 2021
Published: 13 September 2021

1. Introduction

Recently, the demand for e-government services has increased [1], and business needs require more personal information [2]. Due to technological advancements, the protection of personal information has become more complicated, and balancing technological advancements with privacy has become more difficult [3]. Governments, businesses, and researchers today look at information as a highly valuable resource. In e-governments, the demand for e-services has grown rapidly, and the government must protect personal information without compromising the quality of services. Over the past two decades, governments have taken steps to automate their services by integrating data from multiple government entities to improve access, usability, and efficiency [4]. Technology has allowed government entities to interact flexibly and efficiently, allowing different entities to exchange needed information quickly and efficiently. The rapid growth of technology has transformed these interactions into transactions, in which it requests a large amount of information in a single transaction [5].

Trust is a crucial enabler for building an effective relationship between the government and the public [6]. One of the main concerns individuals may have about sharing their personal information with the e-government is that the government employees may misuse their personal information [7]. Therefore, e-government services are adversely affected, impacting the trust by a lack of privacy protection. The e-government services can lose their trustworthiness if the personal information is not protected. It will lead to providing incorrect information when requested from the data owner. Thus, many government entities enact privacy regulations for e-government services to protect personal information and consider

privacy as a core role when designing their e-services [8]. However, this rapid growth of the interactions between various government entities affects the trust of e-government services if the government employee misuses personal information. Thus, there is a need to use privacy preservation tools so that personal information cannot be misused.

Continuing in the same logic, building trustworthy e-government services is very important to have a successful initiative. In this regard, and to the best of the author's knowledge, no study has used the privacy preserve instruments based on privacy by design (PbD) principles to investigate how these instruments may affect the trust between the users and the e-government integrated services. This study examines instruments that can ensure that personal information is protected from misuse by e-government employees. It influences the trust positively while using e-government services. To accomplish this aim, a set of objectives are identified as follows: (1) to design a conceptual framework based on the relevant literature; (2) to derive privacy-preserving instruments as accurately as possible; (3) to identify and validate the data collection method; (4) to verify the reliability of the collected data; and (5) to examine and analyze the positive and negative correlation results between used instruments.

The scope of this study is to elaborate on the impact of different used privacy-preserving instruments, which can protect the integrated e-government information to build a reliable service in Oman. The availability of the government's infrastructure and its affective engagement of transformation to a digital country reveals promising future opportunities in Oman regarding e-services [9]. Oman's e-readiness rank has improved from 55 in 2019 [10] to 44 in 2020 [11], showing a rapid growth in implementing e-services. Thus, this study uses Oman's e-government services as a case study to measure privacy preservation instruments that may affect the trust between the government and the end-users. Accordingly, the results of this study may apply to any e-government initiative.

There are four sections in this study. The first section reviews the previous studies to formalize this study's objective and design the conceptual model, which will be the basis of the other phases. The second section aims to discuss the methodology used to design a survey in the optimal method. Next, using the data gathered from the previous phases, the finding will be obtained in the third section by analyzing the reliability of the used approach and checking the correlation of used instruments. Finally, the last section will revisit the purpose of this study, analyzing the findings and linking them with the literature reviews to elaborate on the contribution of this research.

2. Literature Review

The review of the previous studies aims to define the gaps in previous studies and the elements of measurements instruments to design a conceptual model based on the subsequent phases. Firstly, it starts with looking at the literature describing privacy and its concept in different streams. Then, it will use these key concepts to determine the privacy challenges within integrated e-government services. Next, it will identify the measurement instruments for these challenges, where they can play a significant role in enhancing privacy-preserving. Lastly, it will revise all challenges, elements, and reviews to design the final conceptual model.

2.1. Concepts and Challenges

As defined in 1890 [12] "privacy is the right to be let alone". In this sense, the authors have perceived that everybody has a right to allow individual independence, which was considered the most valuable of all rights. However, considering privacy as the right to be alone in a generic and non-obvious sense has been criticized by other authors [13]. In [14], Tom Gerety defined privacy as "an autonomy or control over the intimacies of personal identity". On the other hand, [15] says that privacy has nothing to do with being yourself; but it has to do with being yourself when and where you choose, without unreasonable restrictions. Therefore, it is clear from all these concepts that privacy is essential as a basis for building an individual's identity.

For the time being, privacy is becoming an increasingly important aspect of modern society. In this sense, Information and Communication Technology (ICT) redefined privacy and initiate a new term known as: "Information Privacy" as "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [16]. According to Records and Information Management (RIM), privacy is: "the right for a living and identifiable individual to have some control over the collection, storage, and disclosure of his or her personal information held by government agencies, financial institutions, medical facilities, educational institutions, and other public and private entities" [17]. In [18–21], it was defined as: "The absence of unreasonable, and potentially intrusive, collection and use of personal information," whereas others defined it as: "Privacy is an ability to keep personal affairs out of the public view" [22].

The technology revolution has impacted different aspects of dealing with personal information, such as e-services, e-commerce, and e-government. In short, personal information protection becomes more complex as technology improves; as technology progresses, privacy [23]. Since little sensitive information was exchanged early at the inception of e-government initiatives, minor privacy issues emerged till e-government interactions improved into transactions, which leads to high demand for data integration [5]. The online transaction poses challenges from a privacy perspective since requests are processed faster, and information is significantly transformed [24]. Due to the high demand for e-services, the information requested and transferred between various government entities without oversight is significant, increasing the likelihood of misuse [25]. Therefore, this will adversely affect the trustworthiness of the e-government services, where a lack of clear privacy discourages individuals from sharing their information [26], which negatively impacts the quality of service [27]. Therefore, this highlights that the primary barrier of trustworthiness in e-government is implementing e-services without considering data privacy. Thus, there is a need to find a way to integrate personal information between the various e-government entities reliably and transparently.

2.2. Related Studies

Despite the importance of protecting personal information in an e-government initiative, little empirical research has directly studied the influence of privacy protection tools on the trustworthiness of the e-service. Therefore, with consideration of the previous most related research in the domain of this study, there are only seven studies that examined privacy preservation instruments—indirectly—and used them as either independent, dependent, or mediating variables. Furthermore, Table 1 illustrates that these studies have gaps from the standpoint of this study since they used other privacy instruments not directly related to the integrated e-government services as this study is attempting to do. For example, the authors in [28] developed a model to investigate the relationship between different information system success models, technology acceptance models, and preserved privacy through the mediation of trust in e-government. Most of the variables used focused on the quality of service and not on protecting personal information within integrated e-government services. In [28], the authors limited the study to the factors of information transparency only, including data collection, data processing, and data usage. The study needs more non-information aspects, such as privacy-preserving techniques, used in e-government systems.

Table 1. Previous studies that are most relevant to this study.

Ref.	Context	Independent Variables	Dependent Variables	Mediating Variables
[28]	e-government	* Data collection information, * data processing information, * data use information	Cynicism, emotional exhaustion	* Privacy information * Transparency
[29]	e-banking	Access	* Perceived privacy	Perceived effectiveness of privacy policy, * privacy control, * privacy risk, privacy concern, * trust
[30]	Consumer behavior, m-communication	* Usage intention	Privacy concern	* Trust, * perceived risk
[31]	e-government	Optimism bias, * perceived privacy, * perceived trust, perceived security	E-government use behavior	* Perceived risk
[32]	m-government, Perceived trust, Social influence	Social influence, cost of service, * perceived trust, perceived usefulness, perceived ease of use	* Usage behavior	Behavioral intention
[33]	e-government, e-services, e-commerce	Perceptions of privacy policy taken, perceptions of organizational privacy self-regulations	Privacy concerns, * trust beliefs, non-self-disclosure behavior	* Privacy risk, * control perceptions
[34]	e-government	Intention to use	Preserved information quality, preserved system quality, preserved service quality, preserved usefulness, preserved ease of use, * preserved privacy	* Trust in e-government

The variables that are indicated with * are those that are correlated partially to this study and reflect privacy preservation.

Other studies [29] propose a model examining privacy policy, control, risk, and trust as mediator variables between principles and perceives. However, the study did not consider specific individual-related instruments affected by government employee behaviors. The authors of [30] investigated the relationship between privacy concerns, perceived risk, trust, and service usage, by utilizing trust and perceived risk as mediation variables. Still, the authors in the previous study have limited privacy concerns by measuring the impact on trust and perceived risk, while there are many other impacts, such as instruments used to preserve personal information. The aim of [31] is to investigate the constructs of optimism bias, privacy, security, and trust, as independent variables and perceived risk as the mediator variable that can influence citizen's behavior of using e-government services. However, the study did not account for government employee's behaviors and the constructs used in the study to assess service delivery rather than the trustworthiness of the e-services. In [32], the study investigates user acceptance using the factors of trust, usefulness, ease of use, cost, and social influence as independent variables. The study used few factors to investigate, and it is limited to mobile services only. Finally, the study [33] is limited to privacy protection in a general mechanism. It does not investigate using privacy preservation instruments extracted from principles of PbD to protect personal information from misuse by government employees when the e-government entities are integrated.

2.3. Hypotheses and Conceptual Model

Based on the above, the literature identified a lack in the extant works on privacy protection in integrated e-government services did not examine deeper specific effects of the privacy preservation instruments extracted from PbD antecedents from the service trustworthiness. As e-service delivery has become more ubiquitous, users have become more concerned about their privacy as e-government allows various entities to collect, save, and process personal data in extraordinary ways. Consequently, an individual's privacy control is likely to decrease, and privacy risks may increase [33]. Individuals must have the ability to control and give permissions to use their information within e-services [35]. Using personal information without permission from individuals is a privacy violation [36]. Individuals must be involved in controlling and permitting access to their information when it is requested.

Additionally, individuals are the owners of personal information, so empowering individuals with control will help e-government services be more trusted [37]. In this regard, the increment of control leads to an increase in the trust of the e-services. Therefore, this study suggests the following hypothesis:

Hypothesis 1 (H1). *Privacy control positively influences the trust to use e-government services.*

Therefore, to implement trustworthy e-services, it is imperative to understand individual's privacy concerns systematically. Failing to do so may adversely affect service delivery as privacy influences the trust and willingness of individuals to participate in personal information [33]. The impact assessment is required to have the ability to measure privacy concerns based on reliable measurements and taking appropriate actions upon those measurements to minimize the risk [38]. Setting clear privacy control procedures will help have proactive and preventative actions rather than reactive ones after privacy is misused. In other words, this will prevent any privacy breach before it happens rather than responding to it afterward [8]. Therefore, measuring the impacts when personal information is requested helps make an efficient decision regarding the allowing of data sharing. By considering the previous discussion, this study proposed the following hypotheses:

Hypothesis 2 (H2a). *A higher impact assessment correlates with a higher level of control in e-government services.*

Hypothesis 2 (H2b). *Impact assessment positively influences the trust to use e-government services.*

Hypothesis 2 (H2c). *Impact assessment and service lifecycle protection are positively correlated.*

The preventive principle emphasizes the necessity of identifying problems before they happen and defining solutions to prevent privacy issues from arising [39]. Citizens must monitor how the government entities use their information and know when they will disclose their information [35]. There are always relations between the monitor and control, where monitoring the provided services in the e-government help to get efficient control. Further, the more government actions on preventive monitoring policies exist, the more individuals feel confident [40]. Due to prior empirical evidence, this study proposed the following hypotheses:

Hypothesis 3 (H3a). *More preventive monitoring leads to increasing relations between the government and users in a trustworthy manner.*

Hypothesis 3 (H3b). *Preventive monitoring and privacy control in e-government services are positively correlated.*

Lifecycle protection means that intense action is taken throughout the entire e-services process cycle to protect privacy. Essentially, it is the process of ensuring the destruction of

personal information after use [41]. Privacy must be protected from start to finish in the e-services lifecycle and ensure that all data has been destroyed adequately upon finishing the process [42]. Therefore, information security and protection are crucial to ensure the trustworthiness of e-services [35]. According to [43], protecting the information enhances trust, increasing the ability to trust e-services providers. In this regard, this study suggested the following hypothesis:

Hypothesis 4 (H4). *Increasing privacy protection will lead to an increase in the trust of the e-services.*

Figure 1 shows the proposed conceptual model. The model underlying in this study includes five instruments, where there are two dependent variables; (1) preventive monitor, and (2) impact assessment, two mediating variables; (3) privacy control, and (4) lifecycle protection, and one independent variable; (5) service trust. As described previously and using the suggested seven hypotheses, instruments influence the trust when a positive or a negative correlation is recorded depending on the path indicated by the conceptual model.

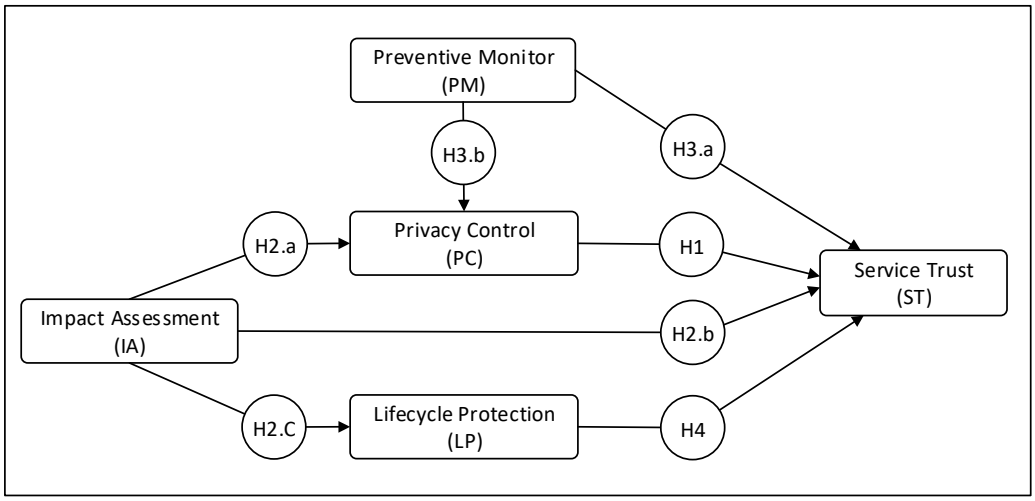

Figure 1. Conceptual Model.

2.4. Measurement Instruments

This study uses a qualitative method to measure the privacy instruments that can influence the trustworthiness of e-government services. As shown in Table 2, several books, academic journals, and other literature review resources were used to set the required tools to preserve privacy based on PbD. Furthermore, the survey was used and distributed to encourage the e-government service users. The survey aims to ensure that the selected instruments are useful and that there are positive correlations between these instruments and the trustworthiness of e-government services.

Table 2. Measurement Instruments.

Instruments	Items	Measures	References
Preventive Monitor	PM1	Send notification if anyone attempts to access their personal information.	[39,44]
	PM2	Aware of which personal information has been used in e-government services.	[39]
	PM3	The information should be tracked when it has been shared.	
	PM4	Determine who should be involved in the monitoring.	[35]
	PM5	Appropriateness of sharing the information.	[44]

Table 2. *Cont.*

Instruments	Items	Measures	References
Privacy Control	PC1	Segregation of permissions.	[36,39]
	PC2	The purpose of request.	[37,39]
	PC3	The ability to share basic information.	[39]
	PC3	Use government regulations to permit sharing information.	[38]
	PC4	Control the request when personal information is requested.	[35,39]
Lifecycle Protection	LP1	Authentication methods are used in e-government services.	[39]
	LP2	Use the information implicitly rather than explicitly.	[45]
	LP3	Destroy the requested information at the end of the integration.	[41,42]
	LP4	Govern policies and rules to protect privacy.	[37,41]
	LP5	Protect personal information at all stages from start to end.	[38,39,41]
Impact Assessment	IA1	Whenever there is a need to share data between government entities, the impact must be evaluated.	[33,36,38]
	IA2	Assist individuals in making decisions when personal information is requested.	[33,37]
	IA3	Impact assessment helps determine who should be permitted to use the required information.	[33,38]
	IA4	It is essential to assess the impact at all stages of the services, from the beginning to the end.	[38]
	IA5	For an accurate impact assessment, it is necessary to use the sensitivity scale.	[8]
Service Trust	ST1	Trustworthy e-governance increases the use of e-government services.	[33,43,46]
	ST2	Trustworthy e-governance increases the participation of individuals to provide their correct information.	[33,46]
	ST3	The clarity in all stages when sharing personal information will increase the trustworthiness of the e-services.	[47]
	ST4	Citizen participation in privacy protection will increase the trustworthiness of the e-government service.	[35,37,47,48]
	ST5	Determining the impact will increase the trustworthiness of the e-government service.	[43]
	ST6	Protecting personal information will increase the trust between the data owner and e-government services.	[43,46]

3. Methodology

This study uses a quantitative approach to measure the relations between hypothesized constructs. A wide range of responses was collected online using a survey, including public sector workers, students and academic members, and people with experience in providing e-government services. As shown in Figure 2, the study aim and the design of the conceptual model were formulated using the literature review. In the next step, the survey questions will be designed and validated with the help of a sampling algorithm, sorting, and pilot test. Using SPSS software, the reliability and correlation can be determined. Finally, after the data analysis and findings, the study aim can be revisited.

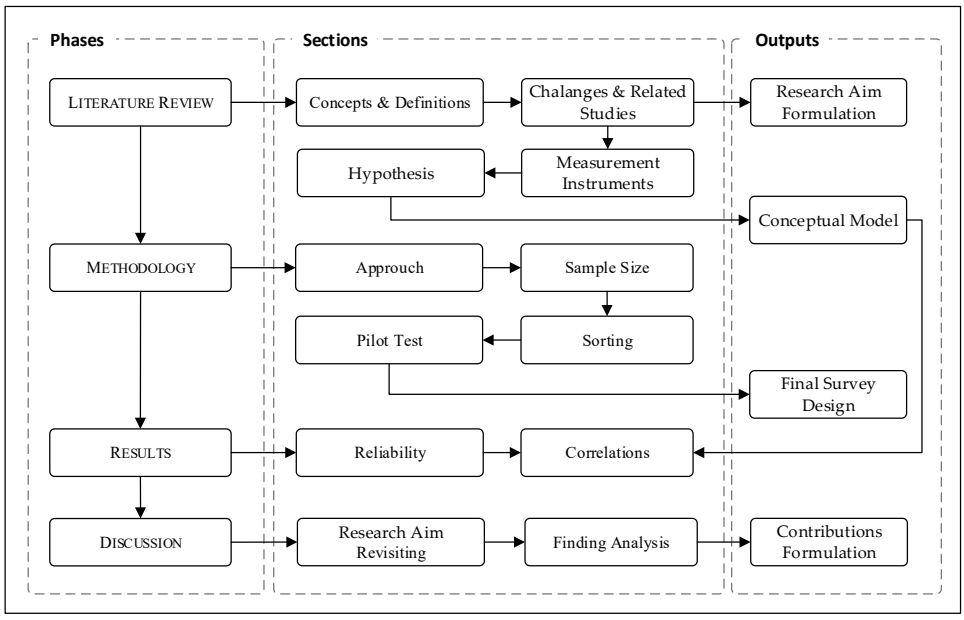

Figure 2. Research Methodology.

3.1. Validation Approach

Survey instruments aim to test the proposed hypotheses experimentally, determine the needed tool's accuracy and correctness, and reduce the measurement error. The survey helps verify and test the factors proposed in the hypothesis and supports it with evidence. As a result, this will also lead to the understanding of the relations between the hypotheses. The literature [49–51] are used as development guidelines to validate and reduce the measurement error accurately were discussed in Tables 2 and 3 and summarized this process.

Table 3. Survey Validation Phases.

Phase	Description
Definition's formalization	Construct definitions were derived from various sources, including preexisting definitions and reviews of relevant literature conducted in this study.
Measurement instruments	The scales were derived as accurately as possible from the relevant literature.
Sample Size	Determine who will be targeted in this study and how many people will be involved.
Feedback	To perform the survey validation, academics and experts in this field were provided with the draft survey. A total of two academics, as well as three experts, were involved. Therefore, five changes were made to the survey questions to make the survey more consistent.
Sorting	The method used for sorting is Q-sorting. The participants were instructed to pick and drop random items within boxes, and it was performed in two stages to improve the reliability of the sorting.
Testing	Two academics completed the sorted survey to enhance validity and reliability. As a result, there has been a slight change in the survey's terms, structure, and length.
Pilot test	Prior to sending the survey publicly, ten people completed the survey, including academics, experts, and others. Based on the feedback they provided, a minor change has been made to the design.

3.2. Sample Size

The key enabler of any e-government initiative is the users of the services and business needs. Hence, this study utilized a mixed-method approach to analyze the user acceptance and the need for the suggested instruments to preserve privacy within the integrated information. This study used the tailored design method for designing the survey [52], targeting the individuals and residents in Oman. Most of the survey samples are non-technical people, so the questions are designed to be understandable by a general audience. The survey will fill the technical gaps, analyze information flows, and align the current instruments with the results.

$$\text{Sample Size } (n) = \frac{\left(\frac{z^2 \mathrm{p}(1-p)}{e^2}\right)}{1 + \left(\frac{z^2 \mathrm{p}(1-p)}{e^2 N}\right)} \quad (1)$$

To determine the sample size of this study we used Equation (1), variable proportion degree, and standard confidence level, as well as the precision level. Where the margin error value is (e), the size of the population is (N), the variability degree is (p), and (z) is the value of how the mean is a way from standard deviation. Based on the National Center for Statistics & Information (NCSI), the total population of Oman is 4492,471 people [53]. A total of 43% of the total population is under 18 years old, and this study focuses on populations above 18 years old [54]. Therefore, the total population is around 2,560,708. As a result, the population is quite large; therefore, the variability proportion value must be 0.5. Accordingly, to reduce the risk, the confidence and precision of data will be set at 95%

and 5%, respectively. Equation (2) shows the sample size of 384 obtained after the above values were applied.

$$\text{Sample Size } (n) = \frac{\left(\frac{(1.96)^2 \times 0.5(1-0.5)}{(0.05)^2}\right)}{1 + \left(\frac{(1.96)^2 \times 0.5(1-0.5)}{(0.05)^2 \times 2560708}\right)} \approx 384 \text{ samples} \quad (2)$$

3.3. Sorting

The sorting technique used in this study is a Q-sorting technique with the help of the Qualtrics software. The purpose of Q-sorting is to evaluate the survey's reliability and validity. The purpose of this type of sorting is to determine whether each survey item corresponds to a particular factor [51]. Thus, this study uses two different rounds to improve the reliability of the sorting. Four different participants are involved in each round to judge and sort the items, two academics and two experts. In each round, the sorting paired the participants into two groups; one is academic, the other is expert, and there is no cooperation between them.

Nevertheless, they may ask about anything related to sorting if they wish [55]. The use of Cohen's Kappa index [56] and hit ratio values [50] to measure the degree of agreement between two judges was undertaken, so evaluations and assertions of the measurement will become more valid and reliable. Based on [57], excellent argument scores are between 76% and 100%, moderate argument scores are between 40% and 75%, and poor arguments are 39% or less. Accordingly, a higher hit ratio will indicate a greater degree of agreement between the judges.

A total of 37 questions were used randomly in the first sorting round. Each participant picked a question and placed it into one of five categories boxes. In addition, the "Not Applicable" category allows the participants to complete without putting them in a particular category; the participants are not restricted to the given categories. As shown in Table 4, the participants agreed about 28 questions out of 37 with a 74% hit ratio. A total of 55 out of 74 questions were classified correctly in this round, and seven were categorized as not applicable. As a result, the ambiguous questions have been revisited, and five non-applicable questions have been removed.

Table 4. First Sorting Round.

		Sorted							
	Instruments	**PM**	**PC**	**LP**	**IA**	**ST**	**N/A**	**Total**	**Hits**
Predicted Sort	PM	11		1	1		1	14	76%
	PC	2	10			1	1	14	71%
	LP	1	1	10	2			14	71%
	IA		1		14		3	16	88%
	ST	1		1	2	10	2	16	63%
	Questions:	74		Hits:	55			Total Ratio:	74%

Upon removing the five questions from the non-applicable category, 32 questions were conducted and used in the second round. There were two participants in the second round, one from the academic field and an expert in services integration. Those who participated in the first round were not involved in the second round. The question orders were randomized, and the participants categorized them and placed them into the appropriate boxes. As shown in Table 5, the participants agreed to about 59 questions out of 64 with a 93% hit ratio. Compared to the previous round, the hit ratio has improved by 19%. According to [57] and Cohen's Kappa Index, a satisfactory agreement level score is 76% to 100%.

Table 5. Second Sorting Round.

		Sorted							
	Instruments	**PM**	**PC**	**LP**	**IA**	**ST**	**N/A**	**Total**	**Hits**
Predicted Sort	PM	12						12	100%
	PC		11				1	12	92%
	LP			12				12	100%
	IA		1		12		1	14	86%
	ST					12	2	14	86%
	Questions:	64		Hits:	59			Total Ratio:	93%

Consequently, the total ratio values in the second round were 93%, which is considered an excellent index value. Thus, the sorting ends with two Q-sorting rounds, and it ends up with high reasonable level questions and high reliability categorized items. As a result, after two Q-sorting rounds, the survey ends up with 30 questions divided into five categories, and each of these categories consists of six questions.

3.4. Pilot Test

This study is targeting the public in Oman who can use the e-government services. Thus, this phase aims to make sure that the survey questions are understandable by most survey respondents. The participants filled out the survey and provided their feedback upon completion. A five-point Likert scale was used for the survey, starting with (1) strongly disagree to (5) strongly agree [58]. Moreover, the selected participants provided some suggestions to improve the quality of the survey. After conducting the pilot test and obtaining feedback from the participants, minor changes were made to the design and to the context in a manner that is easy to understand.

4. Results

4.1. Reliability and Usefulness

This study distributed 420 surveys randomly. Based on the measurement installments described previously, the reliability was measured using Cronbach's alpha. Most of the research studies determine that Cronbach's Alpha values above or equal to 0.7 were good, while 0.8 and above were better, and 0.9 and above were the best [59]. Accordingly, any value more than 0.7 will be reliable.

According to [58], Table 6 shows that all instruments' Cronbach's Alpha values indicate their reliability. With a Cronbach's Alpha of 0.973, the service trust (ST) instrument has the highest value, whereas the impact assessment (IA) had the lowest value at 0.905. Both the preventive monitor (PM) and privacy control (PC) had Cronbach's Alpha values 0.962 and 0.961, respectively. Lastly, the lifecycle protection (LP) had a 0.905 value for the six given questions. The average Cronbach's Alpha for all 30 questions was 0.946.

Table 6. Survey Reliability.

Instruments	**Cronbach's Alpha**	**Questions**
Preventive monitor (PM)	0.962	6
Privacy control (PC)	0.961	6
Lifecycle protection (LP)	0.905	6
Impact assessment (IA)	0.932	6
Service trust (ST)	0.973	6
Total	**0.946**	**30**

4.2. Normality Testing

A normality test is a fundamental assumption in many statistical procedures and estimation techniques, and nonnormality leads to inaccurate statistical outcomes [60]. Pearson's Skewness and Kurtosis values determine whether the results fall within the acceptable normality range. The acceptable values of Skewness and Kurtosis lie within the range of −2.58 to +2.58 [61]. Table 7 indicates that the Skewness and Kurtosis values for all instrument items were within the acceptable range. In this case, all results were normal, and they can be used to provide accurate statistics.

Table 7. Skewness and Kurtosis Values.

Instruments	Item	Skewness	Kurtosis
Preventive monitor (PM)	PM1	−1.136	0.564
	PM2	−1.178	0.673
	PM3	−1.063	0.498
	PM4	−1.249	1.004
	PM5	−1.148	0.706
	PM6	−1.068	0.495
Privacy control (PC)	PC1	−0.999	0.052
	PC2	−0.978	−0.174
	PC3	−0.878	−0.425
	PC4	−0.988	0.015
	PC5	−1.023	0.088
	PC6	−0.937	−0.393
Lifecycle protection (LP)	IA1	−1.037	−0.238
	IA2	−1.416	1.172
	IA3	−1.234	0.104
	IA4	−1.676	2.117
	IA5	−1.357	0.553
	IA6	−1.609	1.794
Impact assessment (IA)	LP1	−1.655	1.445
	LP2	−1.719	2.333
	LP3	−1.526	1.126
	LP4	−1.673	2.108
	LP5	−1.717	1.751
	LP6	−1.433	1.186
Service trust (ST)	ST1	−0.631	−0.806
	ST2	−0.711	−0.761
	ST3	−0.799	−0.618
	ST4	−0.676	−0.787
	ST5	−0.814	−0.602
	ST6	−0.739	−0.737

4.3. Construct Validity

Construct validity is "the degree to which a test measures what it claims, or purports, to be measuring" [62]. This validation examines how closely the value correlates to other tests that measure similar qualities. The validity methods used in this study to test the construction validity are convergent and discriminant. A structural equation model (SEM) is used to ensure the result's dimensionality, validity, and reliability [63]. Figure 3 shows the SME consisting of measurement and structural models, and Table 8 shows the measurement model results.

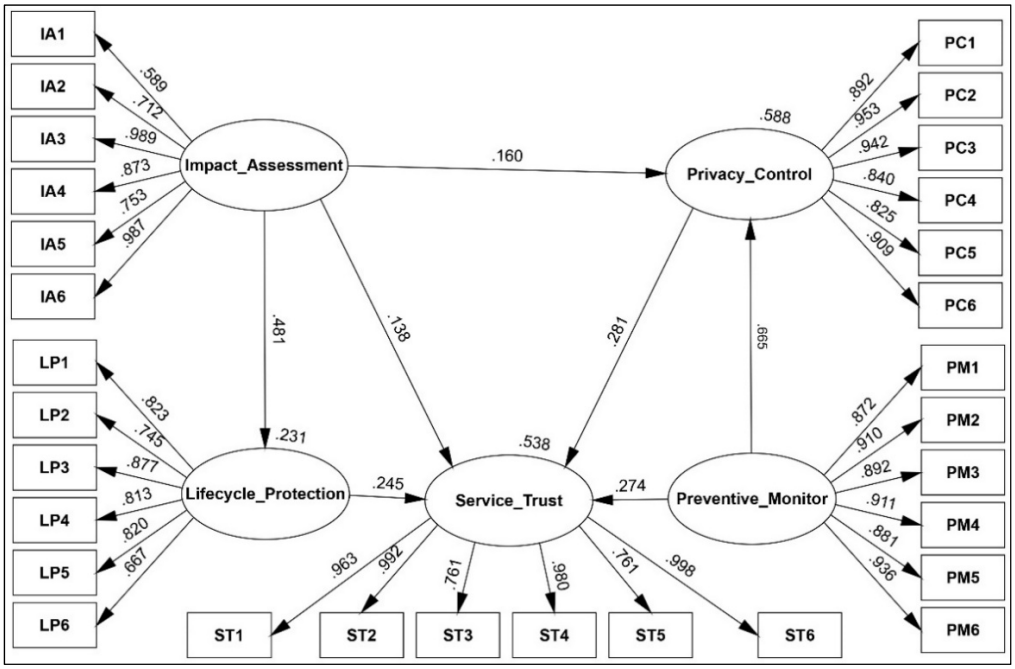

Figure 3. Structural equation modeling (SEM).

Table 8. Model Statistics, Convergent Validity, and Reliability.

Instruments	Item	Mean	Std. Dev.	Loading	AVE	AVE Square Root	CR
Preventive monitor (PM)	PM1	4.39	0.788	0.709	0.615	0.784	0.905
	PM2	4.41	0.775	0.838			
	PM3	4.41	0.740	0.781			
	PM4	4.40	0.789	0.840			
	PM5	4.37	0.791	0.695			
	PM6	4.37	0.773	0.830			
Privacy control (PC)	PC1	4.46	0.695	0.713	0.544	0.738	0.877
	PC2	4.44	0.727	0.749			
	PC3	4.46	0.681	0.778			
	PC4	4.46	0.698	0.754			
	PC5	4.47	0.695	0.648			
	PC6	4.47	0.695	0.775			
Lifecycle protection (LP)	IA1	4.50	0.696	0.807	0.567	0.753	0.886
	IA2	4.50	0.765	0.705			
	IA3	4.55	0.701	0.836			
	IA4	4.55	0.753	0.697			
	IA5	4.59	0.658	0.821			
	IA6	4.51	0.798	0.629			
Impact assessment (IA)	LP1	4.66	0.630	0.528	0.597	0.773	0.897
	LP2	4.55	0.753	0.717			
	LP3	4.64	0.623	0.873			
	LP4	4.54	0.770	0.853			
	LP5	4.68	0.605	0.737			
	LP6	4.50	0.777	0.870			
Service trust (ST)	ST1	4.35	0.708	0.825	0.584	0.764	0.892
	ST2	4.38	0.716	0.824			
	ST3	4.42	0.705	0.631			
	ST4	4.37	0.714	0.818			
	ST5	4.42	0.706	0.627			
	ST6	4.39	0.718	0.827			

As shown, the composite reliability (CR) values were above 0.87, where a CR value of 0.7 was considered sufficient for satisfying construct validity requirements [64]. Further, the minimum average variance extracted (AVE) value was 0.544, where an AVE greater than 0.5 was considered sufficient and a good value [61]. The loading should be removed

from the construct when the AVE value is under 0.4 [65]. Consequently, all constructs passed the reliability and convergence validity requirements. As shown in Tables 8 and 9, the square root of AVE for each construct was more significant than its correlation with other constructs. The minimum square root of the AVE value was 0.738, and the maximum correlation value was 0.729. Therefore, based on [65], all constructs passed the discriminant validity and were established.

Table 9. Correlations Results.

Constructs	Cross Correlations				
	ST	**PM**	**PC**	**LP**	**IA**
ST	1.000				
PM	0.703 **	1.000			
PC	0.729 **	0.725 **	1.000		
LP	0.618 **	0.505 **	0.572 **	1.000	
IA	0.658 **	0.583 **	0.585 **	0.523 **	1.000

** Correlation is significant at the 0.01 level (two-tailed).

4.4. Correlation Analysis

Correlation analysis is considered one of the most common statistical methods used for many purposes, including descriptive data analysis, mathematical modeling, and data engineering [66]. The correlations between continuous variables are measured using Pearson's correlation coefficient based on its covariance values. This coefficient provides information about the relation direction and the association magnitude. Many researchers generally agree that a negligible relationship is a value less than 0.10, and those with coefficients of more than 0.90 reflect very strong relationships. While the correlation coefficient value is higher than or equal to 0.70 and lower than 0.90, it is strongly associated. Finally, a correlation coefficient between 0.40 and 0.69 indicates a good or moderate association, and a weak correlation is between or equal to 0.10 and 0.39.

As shown in Table 9, the trust correlates with the other four privacy instruments: monitor, control, protection, and assessment. All shown correlations were significant at the 0.01 level with two-tailed. The relationship between these instruments and the trust was generally strong to good. The correlation values between service trust (ST) and privacy control (PC) were most significant, with a value of 0.729. The correlation between trust and preventive monitoring (PM) was 0.703. Thus, preventive monitoring and privacy control are strongly associated with service trust. Lifecycle protection (LP) and impact assessments (IA) were well associated with the trust with correlation values of 0.618 and 0.658, respectively. Meanwhile, there was a good association between the impact assessment and the preventive monitor, with a value of 0.583. Additionally, privacy control (PC) and lifecycle protection (LP) correlate well with impact assessments (IAs), with values of 0.585 and 0.523, respectively.

4.5. Hypothesis Testing

As shown in Table 10, all the hypotheses for given paths were supported. Privacy control ($\beta = 0.281$, $t = 5.024$, $p < 0.01$), impact assessments ($\beta = 0.159$, $t = 0.159$, $p < 0.01$), preventive monitor ($\beta = 0.160$, $t = 4.755$, $p < 0.01$), and lifecycle protection ($\beta = 0.245$, $t = 5.721$, $p < 0.01$) showed positive relationships with service trust. Therefore, H1, H2b, H3a, and H4 were supported positively. Preventive monitor ($\beta = 0.665$, $t = 13.951$, $p < 0.01$), and impact assessments ($\beta = 0.160$, $t = 3.882$, $p < 0.01$) showed positive relationships with privacy control. Thus, H2a and H3b were supported positively. Finally, the H2c was supported because the values of impact assessments ($\beta = 0.481$, $t = 9.106$, $p < 0.01$) showed positive relationships with lifecycle protection. The β values for all the paths were above 0.01, this indicates that any increment on dependent variable leads to an increment in the independent variable.

Table 10. Hypothesis Testing Results.

Hypothesis	Relations	Std. Error	Std. Beta (β)	*t*	*p*	F	Finding
H1	PC → ST	0.063	0.281	5.024	0.000	474.251	Supported
H2a	IA → PC	0.032	0.160	3.882	0.000	217.313	Supported
H2b	IA → ST	0.041	0.138	2.953	0.003	318.831	Supported
H2c	IA → LP	0.035	0.481	9.106	0.000	157.564	Supported
H3a	PM → ST	0.058	0.160	4.755	0.000	408.678	Supported
H3b	PM → PC	0.043	0.665	13.951	0.000	463.757	Supported
H4	LP → ST	0.057	0.245	5.721	0.000	258.656	Supported

The coefficient of determination (R^2) value of the service trust was 0.54; this means all the dependent variables explained 54% of the variance in service trust. The privacy control and lifecycle protection R^2 values were 0.59 and 0.57, respectively. It indicates that service trust and impact assessments can explain 59% of the variance in lifecycle protection. The service trust and impact assessments and preventive monitoring can explain 57% of the variance in privacy control.

5. Discussion

5.1. Findings of the Study

This study aims to develop a model for evaluating preventive monitor, privacy control, lifecycle protection, and impact assessment, which influences citizen's trust in e-government services to protect citizen's personal information from being misused by government employees. Citizens consider protecting their personal information from misuse by government employees a significant factor in trusting the e-government services, where the degree of trust between citizens and e-services increases when privacy protection is at a high level [26]. In general, the results indicate that all discussed instruments in this study perceive privacy as a factor that positively influences citizen's trust. It is in line with the study's findings by [33], who found perceived privacy significantly affects trusting e-government services. Therefore, to implement a trustworthy e-government service, citizens need to believe that their information is protected from unauthorized interception by unauthorized employees. Hence, governments should enhance their efforts to protect personal information when integrated with various government entities by setting policies and security measures to provide reliable e-services.

In addition, the result of this study shows that preventive monitoring has a positive impact on service trust. It indicates that the personal information collected by the government and shared with other governments entities must be transparent with the citizens, and it is required to achieve trust. This finding aligns with earlier findings of [28], who found a positive correlation between information transparency and the trust of the e-services provided. Therefore, showing collected personal information to the users transparently increases the user's trust in the system [67]. Accordingly, citizens must be informed when an e-government needs to share personal information between government entities.

This study showed that impact assessment led to an increase in service trust. It indicates that the trust in associated services increases when they have a high level of risk assessment in the provided e-service. To the author's knowledge, no study has investigated the interaction effect between privacy impact assessment and its impact on the trustworthiness of e-government services. As discussed previously in the literature, the impact assessment is the process of minimizing the privacy risk when implementing the services. Therefore, comparing this with earlier studies of [30–32], it was found that a higher perceived risk of service resulted in a lessening of trust in that service. Therefore, those who viewed e-government services as risky were less inclined to use them when dealing with e-government entities. It implies that risk implications and issues should be thoroughly addressed and assessed to increase citizen's trust and become a viable method for accessing e-services within various government entities [31]. As a result, the e-government needs to provide tools to perform impact assessments to determine the risk

when personal information needs to be shared. In addition, impact assessment was found to be a significant factor not only on service trust but also in the privacy lifecycle protection. It indicates that when the risk impact assessment increases, it leads to an increment of privacy protection. In other words, if the personal information is not risky to share in perspective of privacy, then the privacy is protected. This finding is in line with the finding of [31] that reveals negative relations between the risk and security, where an increase of the security leads to risky service. It implies that there is a need for privacy risk assessments to increases data protection. On the other hand, there are positive relations between the impact assessment and the privacy control, where the increasing of assessments lead to an increment in control.

Furthermore, this study found a significant correlation between lifecycle protection and service trust, where increasing protection of personal information is associated with increased trust in related services. It indicates that it is crucial to protect personal data within the service integration lifecycle from start to end. Interestingly, this finding is congruent with earlier studies [30,34], which found a positive correlation between privacy protection and e-government trustworthiness. Accordingly, high privacy protection means high trust, which leads to more citizens using the e-services. Consequently, this finding has strategic implications, as it provides valuable information for future e-government implementation.

5.2. Theoretical Contributions

This study has filled a gap in the literature of the lack of previous studies on the impact of different privacy-preserving instruments that can affect the trust of the e-government services within integrated information. Most previous studies have mentioned the importance of privacy-preserving instruments in line with citizen's trust to encourage them to use integrated e-government services conceptually, while this study supported empirical results. Furthermore, the study contributes to the knowledge regionally since few empirical studies have validated citizen's trust factors in Arab countries, such as Oman. Another contribution of this study is that the empirical results have achieved an excellent explanatory power of 54%, which is significant. This study also contributes to extending the existing knowledge on highlighting the relations of different privacy-preserving instruments with the trust for integrated e-government services that shared information between various government entities. On the other hand, most prior studies focus on internal systems within the same government entity.

5.3. Practical Contributions

The practical contribution of this study will enhance citizen's trust, create a culture of candor by enabling them to provide the correct information, and encouraging them to use e-government services. Using the results of this study can assist the decision-makers in implementing e-government initiatives in effective and efficient strategies to increase citizen's trust towards achieving trustworthy e-government services. Consequently, this study highlights the need for government entities to use and implement privacy-preserving instruments to increase the citizen's trust as a critical aspect of their behavior to participate in e-government services. It can enable decision-makers in the e-government initiative to review and improve the e-services process by practically facilitating these instruments.

6. Conclusions

Although e-governments have found their way to provide beneficial services in everyday life because of their decentralized method and strength upon data integration, privacy-preserving remains a challenge. Therefore, to protect personal information within integrated systems, appropriate instruments must be implemented to leverage e-government service's power without compromising privacy fully. This study developed a technology acceptance model using privacy-preserving instruments from the literature to understand the factors influencing citizen's trust for e-government integrated services. The finding revealed that the privacy lifecycle protection, privacy controls, impact assessment,

and personal information monitors significantly influence the service trust. The finding indicated that the privacy lifecycle protection, privacy controls, impact assessment, and personal information monitors significantly impact the service trust. Generally, this study emphasized that the government entities must realize the influence of citizen's trust and make it an essential key to using e-government services.

This study has some difficulties in that it planned to use a selective quantitative approach, where the respondents will be selected to explain the study's purpose and respond to any further inquiries, but due to COVID-19 restrictions, the online random method was used. Furthermore, this study has observed three limitations, and it needs further investigation in the future. Firstly, the empirical data collected for this study is from Oman, and thus it is limited to the context of a particular culture. Thus, in the future comparative analyses can be done between studies conducted in different countries. Secondly, the focus of the study was on the factors influencing trust from the citizen's perspective. Therefore, there is a need to examine the e-government regulations and policies that can influence privacy-preserving instruments. Finally, a quantitative method is used in this study to validate the correlations between various constructs. This study can be strengthened by including qualitative methods for examining more aspects and identifying other correlations to understand citizen's trust better.

Author Contributions: Conceptualization, H.A; methodology, H.A and M.A.; software, H.A..; validation, H.A; formal analysis, H.A.; investigation, H.A.; resources, H.A.; data curation, H.A.; writing—original draft preparation, H.A.; writing—review and editing, H.A. and M.A.; visualization, H.A.; supervision, M.A., M.S. and A.A.; project administration, M.A.; funding acquisition, H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by Sultan Qaboos University (SQU). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of SQU.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

This study used the following abbreviations:

PM	Preventive monitor
PC	Privacy control
LP	Lifecycle protection
IA	Impact assessment
ST	Service trust
RIM	Records and information management
PbD	Privacy by design
e-government	Electronic government
e-services	Electronic services
ICT	Information and communication technology

Mathematical Symbols

This study used the following mathematical symbols:

n	Sample size
z	Mean away from standard deviation
P	Variability degree
E	Margin error value
N	Population size
CR	Composite reliability
AVE	Average variance extracted
β	Standard beta
t	The size of the difference relative to the variation in your sample data
p	the probability that an observed difference could have occurred just by random chance
R^2	Coefficient of determination

References

1. Qin, F.; Li, L.; Zeng, W.; Wang, T.; Wang, C.; Yu, L. Construction of E-government Data Sharing Framework Based on Big Data Technology. *E3S Web Conf.* **2021**, *257*, 02038. [CrossRef]
2. Kim, H.Y.; Cho, J.-S. Data governance framework for big data implementation with NPS Case Analysis in Korea. *J. Bus. Retail. Manag. Res.* **2018**, *12*. [CrossRef]
3. Mazurek, G.; Małagocka, K. Perception of privacy and data protection in the context of the development of artificial intelligence. *J. Manag. Anal.* **2019**, *6*, 344–364. [CrossRef]
4. Al-Khanjari, Z.; Al-Hosni, N.; Kraiem, N.; Jamoussi, Y. Developing e-Government interoperability driven methodology. *J. Emerg. Technol. Web Intell.* **2014**, *6*. [CrossRef]
5. Holden, S.H.; Millett, L.I. Authentication, Privacy, and the Federal E-Government. *Inf. Soc.* **2005**, *21*, 367–377. [CrossRef]
6. Aladalah, M.; Cheung, Y.; Lee, V.C. Towards a Model for Engaging Citizens via Gov2.0 to Meet Evolving Public Value. *Int. J. Public Adm. Digit. Age* **2018**, *5*, 1–17. [CrossRef]
7. Beldad, A.; Van Der Geest, T.; De Jong, M.; Steehouder, M. A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Gov. Inf. Q.* **2012**, *29*, 41–49. [CrossRef]
8. Cavoukian, A.; Taylor, S.; Abrams, M.E. Privacy by Design: Essential for organizational accountability and strong business practices. *Identit-Inf. Soc.* **2010**, *3*, 405–413. [CrossRef]
9. Jamil, A.R.S.A.; Aref, M.; Rehman, A. Oman e-readiness: A paradigm shift for businesses. *Int. J. Econ. Res.* **2016**, *13*, 2223–2233.
10. Portulans, I. *Oman–Network Readiness Index 2019*; Portulans Institute: Washington, DC, USA, 2019.
11. Portulans, I. *Oman–Network Readiness Index*; Portulans Institute: Washington, DC, USA, 2020.
12. Samuel, D.W.; Louis, D.B. The Right to Privacy. *Harvard Law Rev.* **1890**, *4*, 193–220.
13. Al-Fedaghi, S.S. The "right to be let alone" and private information. In Proceedings of the Seventh International Conference on Enterprise Information Systems, Miami, FL, USA, 25–28 May 2005; SCITEPRESS-Science and Technology Publications: Setúbal, Portugal, 2005; pp. 98–107.
14. Gerety, T. Redefining privacy. *Harv. Civ. Rights Civ. Liberties Law Rev.* **1977**, *12*, 233–296.
15. Koops, B.-J.; Galič, M. Unity in Privacy Diversity: A Kaleidoscopic View of Privacy Definitions. *SSRN Electron. J.* **2021**, *73*. [CrossRef]
16. Westin, A.F. Privacy and Freedom, Atheneum. New York, 1967; p. 7. Available online: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 (accessed on 20 August 2021).
17. Beckles, C. An international perspective on protecting personal information. *Inf. Manag. J.* **2014**, *44*, 33–37.
18. Langenderfer, J.; Miyazaki, A.D. Privacy in the Information Economy. *J. Consum. Aff.* **2009**, *43*, 380–388. [CrossRef]
19. Laudon, K.; Laudon, J. *Management Information Systems: International Edition, 11/E*; Pearson Higher Education: London, UK, 2009.
20. LaRose, R.; Rifon, N.J. Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *J. Consum. Aff.* **2007**, *41*, 127–149. [CrossRef]
21. Culnan, M.J. Protecting Privacy Online: Is Self-Regulation Working? *J. Public Policy Mark.* **2000**, *19*, 20–26. [CrossRef]
22. Bekara, K.; Laurent, M. Enabling User Privacy in Identity Management Systems. In Proceedings of the 2010 IEEE International Conference on Information Theory and Information Security, Institute of Electrical and Electronics Engineers (IEEE), Beijing, China, 17–19 December 2010; pp. 514–520.
23. Collier, B. The power to structure: Exploring social worlds of privacy, technology and power in the Tor Project. *Inf. Commun. Soc.* **2021**, *24*, 1728–1744. [CrossRef]
24. Butt, T.A.; Iqbal, R.; Salah, K.; Aloqaily, M.; Jararweh, Y. Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions. *IEEE Access* **2019**, *7*, 79694–79713. [CrossRef]
25. Sabani, A.; Deng, H.; Thai, V. A Conceptual Framework for the Adoption of E-Government in Indonesia. In Proceedings of the Australasian Conference on Information Systems 2018, University of Technology, Sydney (UTS), Sydney, Australia, 3–5 December 2018.

26. Al-Nidawi, W.J.A.; Al-Wassiti, S.K.J.; Maan, M.A.; Othman, M. A Review in E-Government Service Quality Measurement. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *10*, 1257–1265. [CrossRef]
27. Weerakkody, V.; Irani, Z.; Lee, H.; Hindi, N.; Osman, I.H. Are U.K. Citizens Satisfied With E-Government Services? Identifying and Testing Antecedents of Satisfaction. *Inf. Syst. Manag.* **2016**, *33*, 331–343. [CrossRef]
28. Agozie, D.Q.; Kaya, T. Discerning the effect privacy information transparency on privacy fatigue in e-government. *Gov. Inf. Q.* **2021**, 101601. [CrossRef]
29. Chang, Y.; Wong, S.F.; Libaque-Saenz, C.F.; Lee, H. The role of privacy policy on consumers' perceived privacy. *Gov. Inf. Q.* **2018**, *35*, 445–459. [CrossRef]
30. Zhou, T. The impact of privacy concern on user adoption of location-based services. *Ind. Manag. Data Syst.* **2011**, *111*, 212–226. [CrossRef]
31. Munyoka, W.; Maharaj, M.S. Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *SA J. Inf. Manag.* **2019**, *21*, 9. [CrossRef]
32. Almarashdeh, I.; Alsmadi, M. How to make them use it? Citizens acceptance of M-government. *Appl. Comput. Inform.* **2017**, *13*, 194–199. [CrossRef]
33. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Gov. Inf. Q.* **2020**, *37*, 101413. [CrossRef]
34. Ahmad, K.; Singh, D.; Ayyash, M. Investigating the Effect of Information Systems Factors on Trust in E-Government Initiative Adoption in Palestinian Public Sector. *Res. J. Appl. Sci. Eng. Technol.* **2013**, *5*, 3865–3875. [CrossRef]
35. Khan, S.; Umer, R.; Umer, S.; Naqvi, S. Antecedents of trust in using social media for E-government services: An empirical study in Pakistan. *Technol. Soc.* **2021**, *64*, 101400. [CrossRef]
36. Khan, G.F.; Swar, B.; Lee, S.K. Social Media Risks and Benefits. *Soc. Sci. Comput. Rev.* **2014**, *32*, 606–627. [CrossRef]
37. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information privacy practices in e-government in an African least developing country, Rwanda. *Electron. J. Inf. Syst. Dev. Ctries.* **2019**, *85*, e12074. [CrossRef]
38. Anand, A. Exploring Net Benefits in the Context of an E-Government Project. In *Proceedings of the Collaboration in a Hyperconnected World*; Springer Science and Business Media LLC: Cham, Switzerland, 2020; pp. 415–421.
39. Gerunov, A.A. Attitudes towards privacy by design in e-government: Views from the trenches. *J. Soc. Ad-Min. Sci.* **2020**, *7*, 1–17. [CrossRef]
40. Singh, P.; Dwivedi, Y.K.; Kahlon, K.S.; Sawhney, R.S.; Alalwan, A.; Rana, N.P. Smart Monitoring and Controlling of Government Policies Using Social Media and Cloud Computing. *Inf. Syst. Front.* **2019**, *22*, 1–23. [CrossRef]
41. Kurtz, C.; Semmann, M. *Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors*; Americas Conference on Information Systems: New Orleans, LA, USA, 2018.
42. Hertzman, C.P.; Meagher, N.; McGrail, K.M. Privacy by Design at Population Data BC: A case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. *J. Am. Med. Inform. Assoc.* **2013**, *20*, 25–28. [CrossRef] [PubMed]
43. Salo, J.; Karjaluoto, H. A conceptual model of trust in the online environment. *Online Inf. Rev.* **2007**, *31*, 604–621. [CrossRef]
44. Al-Naimat, A.M.; Fraihat, A. E-Government's Service Quality; User perception Significance and Measurement. *IJCSNS* **2020**, *20*, 101. [CrossRef]
45. Larson, M.; Oostdijk, N.; Borgesius, F.Z. Not Directly Stated, Not Explicitly Stored. In Proceedings of the Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization; Association for Computing Machinery (ACM), Utrecht, The Netherlands, 21–25 June 2021; pp. 388–391.
46. Smith, H.J.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Q.* **2011**, *35*, 989. [CrossRef]
47. Warkentin, M.; Sharma, S.; Gefen, D.; Rose, G.M.; Pavlou, P. Social identity and trust in internet-based voting adoption. *Gov. Inf. Q.* **2018**, *35*, 195–209. [CrossRef]
48. Liu, D.; Carter, L. Impact of citizens' privacy concerns on e-government adoption. In *Annual International Conference on Mobile Computing & Networking-MobiCom '13*; ACM: New York, NY, USA, 2018; p. 27.
49. MacKenzie, S.B.; Podsakoff, P.M.; Podsakoff, N.P. Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. *MIS Q.* **2011**, *35*, 293. [CrossRef]
50. Moore, G.C.; Benbasat, I. Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Inf. Syst. Res.* **1991**, *2*, 192–222. [CrossRef]
51. Lewis, B.R.; Templeton, G.F.; Byrd, T.A. A methodology for construct development in MIS research. *Eur. J. Inf. Syst.* **2005**, *14*, 388–400. [CrossRef]
52. Dillman, D.A.; Smyth, J.D.; Christian, L.M. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
53. Information N.C.f.S. Available online: https://www.ncsi.gov.om/Pages/NCSI.aspx (accessed on 21 June 2021).
54. NCSI. *Community Statistics*; NCSI: Muscat, Oman, 2021; pp. 3–4.
55. Brown, S.R. Q Methodology and Qualitative Research. *Qual. Heal. Res.* **1996**, *6*, 561–567. [CrossRef]
56. Cohen, J. A Coefficient of Agreement for Nominal Scales. *Educ. Psychol. Meas.* **1960**, *20*, 37–46. [CrossRef]
57. Landis, J.R.; Koch, G.G. The Measurement of Observer Agreement for Categorical Data. *Biometrics* **1977**, *33*, 159–174. [CrossRef]
58. Likert, R. A technique for the measurement of attitudes. *Arch. Psychol.* **1932**, *140*, 1–55.

59. Le, H.T.H.; Tuyet, V.T.B.; Hanh, C.T.B.; Do, Q.H. Factors Affecting Tax Compliance among Small- and Medium-sized Enterprises: Evidence from Vietnam. *J. Asian Financ. Econ. Bus.* **2020**, *7*, 209–217. [CrossRef]
60. Islam, T.U. Ranking of Normality Tests: An Appraisal through Skewed Alternative Space. *Symmetry* **2019**, *11*, 872. [CrossRef]
61. Murtagh, F.; Heck, A. *Multivariate Data Analysis*; Springer Science & Business Media: Berlin, Germany, 2012; Volume 131.
62. Brown, J.D. What is Construct Validity. In *Encyclopedia of Evaluation*; Sage Publications, Inc.: Thousand Oaks, CA, USA, 2005; Volume 4, pp. 8–12.
63. Alnaser, F.M.; Ghani, M.A.; Rahi, S. Service quality in Islamic banks: The role of PAKSERV model, customer satisfaction and customer loyalty. *Accounting* **2018**, 63–72. [CrossRef]
64. Thorndike, R.M. Book Review: Psychometric Theory (3rd ed.) by Jum Nunnally and Ira Bernstein New York: McGraw-Hill, 1994, xxiv + 752 pp. *Appl. Psychol. Meas.* **1995**, *19*, 303–305. [CrossRef]
65. Hair, J.F., Jr.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM). *Eur. Bus. Rev.* **2014**, *26*, 106–121. [CrossRef]
66. Core Team, R. *R: A Language and Environment for Statistical Computing*; R Foundation for Statistical Computing: Vienna, Austria, 2013.
67. Oulasvirta, A.; Suomalainen, T.; Hamari, J.; Lampinen, A.; Karvonen, K. Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance. *Cyberpsychology Behav. Soc. Netw.* **2014**, *17*, 633–638. [CrossRef] [PubMed]