Perception of Information Sensitivity for Internet Users in Saudi Arabia

Khaled Almotairi [1] ⓘ**, Bilal Bataineh** [2] ⓘ

Abstract

The rapid evolution of Internet use has led to the collection of big data about users, which has raised users' privacy concerns about their personal information. This study adopts the hypothesis to evaluate the perception of the information sensitivity of Internet users in Saudi Arabia as research subjects. This study analyzes the sensitivity of 35 types of information through a questionnaire with answers from 508 participants from Saudi Arabia and estimates the cultural influence by comparing Saudi results with users from the USA, Brazil and Germany. Demographic information, such as age, gender, marital status and education, and attitude characteristics, such as disposition to privacy, propensity to take risks, privacy violation experience and trust in institutions, influence Saudi individuals' perception of sensitivity towards various types of information. The survey results show slight differences in the sensitivity levels between Internet users in Saudi Arabia and their counterparts in other nations. Ultimately, this study contributes to improving the international model of information sensitivity perception between different nations.

Keywords: Cultural privacy, Information privacy, Perception of sensitivity, Sensitive information.

1 Introduction

The Internet has completely changed our lives. It changes people's experience with shopping, learning, communication, social media, lifestyle, healthcare, and so on. In this regard, there has been a rapid increase in Internet users and connected devices, and more people are moving toward dealing with electronic services (Kapoor et al., 2018; Markos et al., 2017). The Internet dependency explosion has led to the creation and collection of large amounts of data called "big data." Big data is important for researchers and businesses in finding new knowledge and information and developing new products and services (Alashoor et al., 2017; van Zoonen, 2016). This big data includes valuable personal information about users. For various reasons, Internet users are forced to disclose their sensitive information, which creates serious security and privacy concerns (Alashoor et al., 2017; Fianu, Ofori, Boateng & Ampong, 2019; Kapoor et al., 2018; Markos et al., 2017; van Zoonen, 2016).

Given the fast-growing popularity of online services and social media, there has been a massive increase in the information given by users (Fianu et al., 2019; Markos et al., 2017; Stutzman et al., 2013). E-service providers from government and private institutions collect

---

[1] Department of Computer Engineering, Umm Al-Qura University, Makkah, Saudi Arabia

[2] Department of Computer Science, Umm Al-Qura University, Makkah, Saudi Arabia

✉ bmbataineh@uqu.edu.sa

information about users to improve and manage services (Mutimukwe et al., 2019). Meanwhile, social media platforms and device operators collect different types of users' personal, biometric identification, browsing data, location, and daily processes data (Fianu et al., 2019; Hung & Cheng, 2009; Pires, Garcia, Pombo, & Flórez-Revuelta, 2016). That, in turn, has given rise to the concerns of Internet users about the information collected from the user in a way that threatens their privacy and security, or can be revealed to a third party (Mutimukwe et al., 2019; Xu et al., 2011). Therefore, the self-disclosure of information highlights inquiries about the importance and sensitivity degrees of information types being disclosed. However, the sensitivity varies based on many factors; it varies from person to person and from country to country (Bergström, 2015; Chang & Heo, 2014; Fianu et al., 2019; Krasnova & Veltri, 2010; Mutimukwe et al., 2019; Schomakers, Lidynia, Müllmann, & Ziefle, 2019; Stutzman et al., 2013).

The differences between nations' cultures is one of the most important factors that determine the degree of sensitivity of information types (Chang & Heo, 2014; Krasnova & Veltri, 2010; Markos et al., 2017; Schomakers et al., 2019). However, most previous studies targeted countries with a secular lifestyle, such as the USA, European countries, East Asia, and Latin America. Therefore, it was expected to find similar perceptions of information sensitivity (Bauer & Schiffinger, 2016; Hong & Thong, 2013; Markos et al., 2017; Pentina, Zhang, Bata, & Chen, 2016; Schomakers et al., 2019).

Article (Schomakers et al., 2019) claimed that studies on information sensitivity have focused on Western countries. For that reason, more studies about Asia, Africa, and Oceania are needed to shape the global model of information sensitivity among nations. In this regard, there exists an omission to analyze the information sensitivity of Internet users in the Middle East. Middle Eastern countries are significantly culturally different from the countries that were previously targeted. Middle Eastern countries are greatly affected by a conservative lifestyle that emerges from the interaction between Islamic rules and traditional extended family rules, which leads to a lifestyle that is somewhat different from Western countries.

This study aims to analyze and evaluate the perception of information sensitivity for people in the Middle East area, which is achieved by targeting Internet users in Saudi Arabia. The present study is developed according to the hypothesis of (Markos et al., 2017). We compare the outcomes of this study with the perception of information sensitivity of users from the USA, Brazil (Markos et al., 2017), and Germany (Schomakers et al., 2019). The results will contribute to clarifying the Saudi perception of information sensitivity in the international perception model.

The rest of the paper is organized as follows. Section 2 presents the background and related works. Section 3 describes the adopted methodology and data. Section 4 shows the results and discussion, and Section 5 provides the conclusion.

2 Related Works

This section presents a review of literature about privacy concerns, information sensitivity, and the perception of information sensitivity between countries.

2.1 Background

In 1948, the United Nations Universal Declaration of Human Rights recognized privacy as a fundamental human right (Assembly, 1949). According to Westin (1967), privacy is people's desire to obtain the freedom of choice under any circumstances and choose to what extent

they display their attitudes and behavior to others. With the rise of the Internet, information privacy has become an essential issue that interacts with several considerations (Bauer & Schiffinger, 2016; Bergström, 2015; Hong & Thong, 2013; Kapoor et al., 2018; Pentina et al., 2016; Xu et al., 2011). Pentina et al. (2016) pointed out that the rapid evolution of mobile technology and its apps, social networks, gaming, multimedia exchanges, and commercial transactions compel Internet service providers to collect many types of user information, such as gender, age, location, interests, personal preferences, browser history, calendar events, pictures, contacts, and so on. The main goal of collecting this data is to improve services for users. However, this data collection leads to security and privacy issues.

Mutimukwe et al. (2019) claimed that with the increase of Internet use, creating a consistent basic definition of information privacy is important. They summarized the definitions of information privacy of many researchers by stating that it is the control of transactions between people to enhance autonomy and/or minimize risks. According to Hung & Cheng (2009), in the field of information systems, privacy is an individual's right to determine how, when, and to what extent information about the self will be released to another person or an organization. Based on (Öğütçü et al., 2016), users' self-disclosure highlights essential concepts, such as privacy concerns, self-disclosure behaviors, and information sensitivity for Internet users.

2.2 Privacy concerns

The number of social media users worldwide is expected to reach 3.02 billion by 2021 (Gilbert, 2019; Huo et al., 2019). Moreover, the number of devices connected to the Internet was expected to reach 50 billion different devices by 2020 (Mollah et al., 2019). This increase leads to disclosing more personal information by increasing the ability of organizations to collect, store, process, and exploit personal information from users, which reduces individuals' ability to control their information and increases their privacy risk (Mutimukwe et al., 2019). Milne et al. (2016) claimed that the most common worries of users are physical, monetary, social, and psychological risks.

Considering some privacy concerns of social networks as an example, (Fianu et al., 2019) mentioned that social media platforms primarily use users' data to make profits by selling user data to external parties, such as government and private organizations. Moreover, the default privacy setting allows unwanted people, such as friends of friends and group members, to obtain access to other users' profiles. This shares information with people who should not be able to access that information. In addition, Wirth et al. (2019) mentioned that friends share personal information, such as photos, only with their friends who trust them. However, one of these friends can then disclose the information to other people, even if the first user requested confidentiality for it.

2.3 Information sensitivity

Despite the privacy concerns of Internet users, the literature review shows various contradictions between privacy concerns and the behavior of information disclosure (Barth & de Jong, 2017; Roberts, 2012). For example, the most common password used is 12345, and most people use one password for multiple accounts. Moreover, people disclose their private information online, although they have security concerns about their privacy and data (van Zoonen, 2016). Kokolakis (2017) asked a question about this issue, why do users take so many risks? Pentina et al. (2016) claimed that Internet users make mindful trade-offs between benefits and privacy risks. Thus, most people are willing to share their data with the

organization that requests it when these benefits are of direct personal relevance (Markos et al., 2017; Acquisti et al., 2013).

In this regard, van Zoonen (2016) claimed that users are interested in two specific points about their privacy. The first point is that people's privacy concerns vary according to the purpose for which the data is collected. The second represents the fact that people assume some data are more sensitive than others. Information type plays an important role in identifying the degree of privacy concerns. For example, personal data, such as nationality, gender, or age, are considered less sensitive information compared with medical and financial information that are considered highly sensitive for users. Users also differ in the perceived sensitivity of their information. For some people, this information is private, and for others, it is available to everyone without any concern (Robbins & Stylianou, 2002; van Zoonen, 2016).

Several works have studied the factors that influence the degree of information importance and sensitivity. Milne et al. (2016) performed a survey to analyze 52 types of information on the basis of expected risks. The results show a wide variation in the sensitivity of information types according to the perceived risk. Moreover, the current study demonstrates that cultural differences influence the assessment of perceived sensitivity to information types. Robbins and Stylianou (2002) examined the reflection of differences in national cultures on websites and on data sensitivity. The result shows that cultural considerations are an important factor in information systems and the degree of data sensitivity.

Veltri et al. (2011) compared the risk assessment of information disclosure on Facebook between American and Moroccan Facebook users. The results show that Moroccan users show greater privacy concerns than US users. Krasnova et al. (2012) analyzed the same point between German and American Facebook users. The results show that German users are more likely to self-disclose their private information than users from the USA. Li et al. (2018) studied the impact of culture to determine the intentions to share health information on social media. The case study on China and Italy shows a clear difference between the nations in that perception. Liu and Wang (2018) analyzed the influence of cultures in different countries on individual self-disclosure decisions. The comparisons between the USA and China show strong differences.

Jiacheng et al. (2010) studied the mechanisms of knowledge exchange between individuals in China and the USA. The results show that the country's culture is an important factor in knowledge exchange. Chen et al. (2013) analyzed the respective levels of information privacy of mobile users in the USA and Korea. The results show that Koreans are more used to commercial activities via mobile phones, whereas Americans were more concerned about their information privacy. Trepte et al. (2017) studied the cultural factors that influence the perception of privacy risks in Germany, the Netherlands, the United Kingdom, the USA, and China. The results show important differences in user perception of privacy risks between nations.

Markos et al. (2017) examined several factors, such as the country of origin, age, and type of information on data sensitivity and on users' willingness to disclose information on the Internet. The sample works comprised American and Brazilian users, and the results show significant differences according to the country of origin. Following the hypothesis of the previous study, Mutimukwe et al. (2019) added greater understanding of the cultural impact on the perception of data sensitivity. The German values concerning the disclosure of different types of information were compared with the results of American and Brazilian users in (Markos et al., 2017). The results show minor differences in sensitivity perception between the USA, Brazil, and Germany.

The literature review above showed that the perceived levels of information sensitivity greatly vary between nations. Although previous works targeted certain countries (USA, China, and some European countries) that are considered secular and developed countries, unlike other nations that are considered conservative and traditional that have been ignored. Schomakers et al. (2019) claimed that the sensitivity of information has been studied in Western countries, and more information is needed about Asia, Africa, and Oceania. According to (Markos et al., 2017; Schomakers et al., 2019), further studies about different nations and countries are important to build a global model of perception of information sensitivity.

2.4 Differences of Saudi characteristics

The omission in the literature review to study the perception of information sensitivity in the Middle East is clear. This region includes many countries with similar cultural values from the interaction between Islamic rules and rules of traditional extended families. This leads to a significant difference in the lifestyle between the Middle East and Western countries, which entails differences in privacy concerns and perceptions of information sensitivity. Saudi Arabia is one of the key countries in the Middle East. Based on Alshahrani (2016), the first Internet connection in Saudi Arabia was by the King Fahd University of Petroleum and Minerals in 1993. Approximately 31.1 million (92.3% of the population) in Saudi Arabia used the Internet in 2020.

Based on Hoftede et al. (2010), Figure 1 represents a set of cultural differences between Saudi Arabia, USA, Brazil, and Germany which cause differences in privacy concerns between Internet users. Saudi Arabia shows high degrees of large power distance and strong uncertainty avoidance results in strong religiosity, which indicates that the Saudi society follows the laws and administrative systems with high acceptance and accepts the belief that there is a single truth more than the USA, Brazil and Germany. Hoftede et al. (2010) claimed that people from cultures of high degrees of large power distance and strong uncertainty avoidance are careful when making information disclosure decisions.
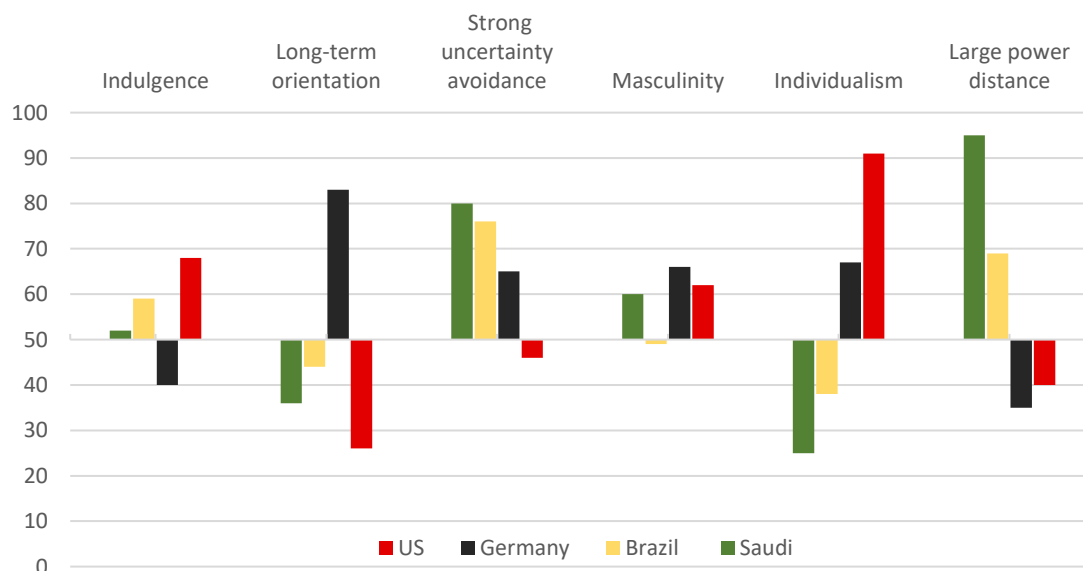

Fig. 1. *Comparison of Cultural Characteristics between Saudi Arabia, USA, Brazil, and Germany according to the Hofstede model (Hoftede et al., 2010).*

Saudi Arabia shows a low degree of Individualism. Strong religiosity and social norms display high collectivity. The Saudi society is a great example of tightly integrated relationships that bind extended families, such as the unquestioning loyalty and support for each other when a conflict arises with another group. Hoftede et al. (2010) unveiled that people from individual cultures are less likely to disclose information than those from collective cultures. Consequently, Posey et al. (2010) found that people from collective cultures are more concerned about the harm they may do to the privacy of their group.

According to the degree of masculinity versus femininity, Saudi Arabia has a value close to that of the USA and Germany, and it is more open than Brazil to accept differences. In terms of long-term orientation, the low degree indicates that US, Saudi Arabia, and Brazil honor and maintain traditions. Finally, the indulgence score shows that Saudi societal norms give average degrees of freedom to citizens in fulfilling their human desires, unlike Western countries that allow free gratification of human desires. With these terms, people tend to disclose more information with high scores (Hofstede, 2011).

3 Method and Data

This study adopted an experimental questionnaire approach to collect the data by using an online survey method. A total of 508 Internet users in the Kingdom of Saudi Arabia (KSA) were involved to estimate their perceived sensitivity of 35 different types of information on the Internet. This study analyzed the results statistically and compared them with the results of American, Brazilian, and German users according to experiments that have been conducted (Markos et al., 2017; Schomakers et al., 2019).

3.1 Selection of information types

This study adopts the hypothesis of (Markos et al., 2017) and the additions of (Schomakers et al., 2019). This study also uses the same information types as those studies to perform a descriptive comparison between Saudi users and users from the USA, Brazil, and Germany. Lastly, the researchers analyze the types of information suggested by (Markos et al., 2017), and modified by (Schomakers et al., 2019) to select suitable items for Saudi participants.

This study estimates which global types of information match the laws and culture in the Middle East, particularly in the KSA. We excluded certain information types from this study because of their seriousness in the Middle East. For example, certain information types are considered criminal behavior, such as homosexuality (sexual preference) and alcohol consumption. Others are rejected in conservative and religious societies, which are the majority of the population of the study area, such as online dating activities and women's hair color. In addition, this study drops DNA profile items because it is considered an unknown type of information for most people. Figure 2 displays the final list of 35 types of information.

3.2 Questionnaire and survey

This study presents the selected types of information as an online questionnaire. At the beginning, the topic was clearly presented to the participants. Then, the participants reported their demographic characteristics. Next, we asked the participants to evaluate the degree of perceived sensitivity of each type of information disclosed on the Internet or when they use smart devices. We also asked them to report any sensitive information that is not included in the questionnaire. Moreover, we instructed the participants to evaluate their privacy disposition, previous experiences of violation, a tendency to risk the disclosure of information, and their trust in institutions.

Given that we surveyed Internet users in the KSA, we asked a native speaker to formulate the questions in the Arabic language in a way suitable for the participants. We implemented and distributed the survey on an online platform called SmartSurvey. We divided our questionnaire into three parts. The participants provided their demographic information: age, gender, educational level, and marital status in the first part. Then, they evaluated the sensitivity of 35 types of information in the second part. We arranged these 35 types of information randomly to prevent sequence effects and asked the participants questions regarding their sensitivity toward the sample information types we provided for them (i.e., "How sensitive are the following information types for you?"). They rated their sensitivity to the given information types on a six-point Likert scale ranging from 1 "not sensitive at all" to 6 "very sensitive" (Markos et al., 2017; Schomakers et al., 2019). We used this type of scale to help participants distinguish the scores (Lozano et al., 2008; Markos et al., 2017). Afterward, we converted the results to a 10-point scale to compare it with the relevant business results of Markos et al. (2017) and Schomakers et al. (2019).

We also asked the participants to show their degree of agreement for eight points about their willingness, past violations, risk appetite, and trust in institutions in the third part of the questionnaire (Schomakers et al., 2019). They evaluated their agreement on a six-point Likert scale ranging from 1 "extremely disagree" to 6 "extremely agree." To compare our results with those of Markos et al. (2017) and Schomakers et al. (2019), we converted the scale to a 10-point scale.

3.3   The Sample

The researchers relied on various methods to distribute the questionnaire to reach a representative sample of Saudi Internet users. First, the questionnaire was distributed online to social groups from universities, employees, and communities. Also, face-to-face meetings were held with various members of the community to encourage them to participate as students and employees. To ensure adequate female participation, especially in the KSA, female students and employees were in buildings separate from males. Researchers contacted officials in the women's branches of educational and government institutions to encourage females and their families to participate. The previous process was applied in various areas of KSA.

In this survey, participants completed the questionnaire in January 2020. In total, 508 Saudi participants completed the questionnaire. Table 1 presents the demographic characteristics of the collected sample. Roughly 80% of the participants (406 individuals) were in the age range of 18–50, approximately 7% of the participants (36 individuals) were under 19 years old, and 13% of the participants (66 individuals) were older than 50 years of age. The sample shows a varied distribution related to age by average (M = 34.2) and standard deviation (SD = 22.84). It also shows varied distributions regarding the fact that 66.93% of the participants were males, 84.26% of the participants had a university degree, and 61.4% were married.

Age	Mean (**SD**)		34.19 (**22.84**)
		19 and less	7.1%
		20–29	24.7%
		30–39	28.8%
		40–49	26.4%
		50 and older	13%
Gender	Male		66.9%
	Female		33.1%
Education	University degree		84.3%
	Other		15.7%
Marital status	Single		38.6%
	Married		61.4%

Tab. 1. Demographic characteristics of the collected sample (N = 508). Source: Authors.

3.4 Measurements and analysis

To explore Saudi information sensitivity perception, we compared the outcomes with the available outcomes of Internet users in the USA, Brazil (Markos et al., 2017), and Germany (Schomakers et al., 2019). By imitating the methodology that was used by (Markos et al., 2017; Schomakers et al., 2019), we shaped the rank–order model of information sensitivity degrees on the basis of the average values according to the Saudi perspective. The resulting model includes the results of the average values of the USA, Brazil, and Germany to be compared with Saudi results. All 35 average values for perceptions are available for Germany, while only 29 are available for the USA and Brazil. Next, we categorized the variables into high, medium, and less sensitive data groups and analyzed them by using the threshold values between these three categories following the German experiments.

4 Results and Discussion

This section shows the descriptive results of the information sensitivity perception of Saudi Internet users. In addition, it shows a comparison between Saudi results and American, Brazilian, and German results on the basis of the outcomes of (Markos et al., 2017; Schomakers et al., 2019). Moreover, this section analyzes the sensitivity outcomes, highlights their characteristics, and finds factors that influence the sensitivity of Saudi Internet users.

4.1 Information sensitivity of Internet users in Saudi Arabia

On the basis of our survey, Figure 2 presents the rank–order of the average sensitivity ratings for each information type. The rank–order is sorted according to the average values (*M*) of Saudi Internet users from the highest sensitivity degrees to the lowest. As a result, the *Password* got the highest sensitivity by $M = 9.64$. Then, each of *Fingerprint* and *Financial account information* with some variance by $M = 9.17$ and $M = 8.82$, respectively. By contrast, *Name of pet*, *Religion*, and *Occupation* were less sensitive information for Saudi users in average about $M = 2.4$, $M = 3.08$, and $M = 3.11$, respectively.
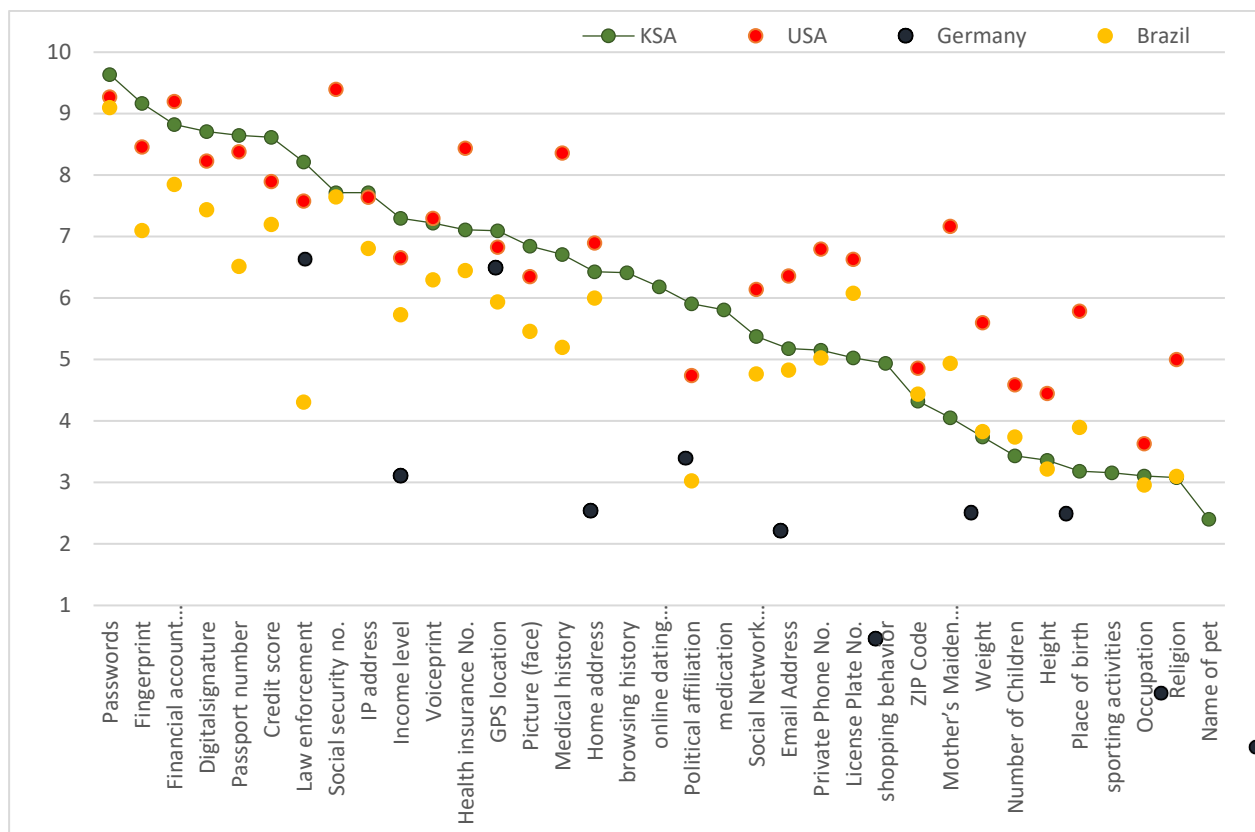
Fig. 2. Rank–order of Saudi users' perception of information sensitivity and its comparison with American, Brazilian (Markos et al., 2017), and German users (Schomakers et al., 2019).

Regarding our collected data, Internet users in the KSA showed some radical perception toward information sensitivity compared with their counterparts in other countries. From the 29 values common to all countries, Internet users in the KSA showed high degrees of sensitivity for each of passwords, fingerprint, digital signature, passport number, credit score, income level, and political affiliation. By contrast, they showed lesser degrees of sensitivity in seven items than their counterparts in the USA, Brazil, and Germany; these are license plate no., ZIP Code, mother's maiden name, weight, number of children, place of birth, and religion.

Saudi Arabia, Brazil, and Germany agree with the highest sensitivity for passwords by 9.6, 9.1, and 9.3, respectively. American users give the social security number as the most sensitive type (9.4). Saudi users clearly show a high sensitivity toward verification information types (passwords, fingerprint, digital signature, and passport number) than other countries. Moreover, political affiliation and law enforcement items show the most variance for Saudi users compared with other countries.

Among the participants, Internet users in KSA also showed lesser degrees of sensitivity in all the six values in common with Germany only, which are browsing history, online dating activities, medication, shopping behavior, sporting activities, and names of pets.

Based on the values of each country in common with the KSA, the correlation for information sensitivity shows high similarity between the KSA and Germany by r = 0.93, then r = 0.79 between KSA and USA, and r = 0.78 between KSA and Brazil. In detail, some differences are clear between our sample of Saudi users and other countries. The clearest difference between Saudi and Brazilian users was in law enforcement by 8.2 and 4.3, respectively. The clearest

difference between Saudi and American users was in mother's maiden name by 4.1 and 7.2, respectively. The highest difference between Saudi and German users was in private phone numbers by 5.2 and 7.7, respectively.

4.2   Category of information and analysis

Similar to (Markos et al., 2017; Schomakers et al., 2019), we categorized information types into three groups of sensitivity value. We classified each type into low-sensitivity information, medium-sensitivity information, or high-sensitivity information classes as presented in Table 2.

To perform that, we scaled the average values of the sensitivity of each country between 0 and 10 by using the following formula:

$$Scaled_{Value} = \frac{Sensitivity_{Value} - Min_{Value}}{Max_{Value} - Min_{Value}} \times 10$$

Where $Scaled_{Value}$ is the new scaled average value of sensitivity, and $Sensitivity_{Value}$ is the original average value of sensitivity. Min_{Value} and Max_{Value} are the minimum and maximum average values of the sensitivity of each country respectively. Then, we classified the variables by using the threshold levels from a previous study (Schomakers et al., 2019). The high-sensitivity items had values higher than 7.67, whereas low-sensitivity values had less than 4.7; in between was the medium sensitivity. We adopted these thresholds to obtain results comparable with the (Schomakers et al., 2019). The different numbers and scaling processes of used variables in this study could cause overlapping clustering when we use k-mean clustering.

Comparing the high, medium, and low sensitivity information groups of Saudi users to the USA, Brazil (Markos et al., 2017), and Germany (Schomakers et al., 2019) shows some differences regarding the classification of the sensitivity of information types.

While the *Credit score* and *Law enforcement* were considered highly sensitive information for Saudi users, they were considered medium sensitive for German and American users, and some were low sensitivity for Brazilian users (*Law enforcement*). Moreover, ***Political affiliation*** was considered a medium-sensitivity information type for Saudi users, but it was considered low sensitivity for German, American, and Brazilian users.

Regarding the 29 items that are common to all the countries involved, we noticed various similarities between Internet users in the KSA and their counterparts in other countries. Internet users in the KSA were similar to those in Germany seven times, six times to those in the USA, and only twice to those in Brazil in the category with a high level of sensitivity. Internet users in the KSA matched seven times with those in Germany and five times with those in the USA and Brazil in the category with a medium level of sensitivity. Internet users in the KSA matched 11 times with those in Germany, eight times with those in the USA, and ten times with those in Brazil in the final category with the least level of sensitivity. Overall, Internet users in the KSA matched 25, 19, and 17 times with Internet users in Germany, the USA, and Brazil, respectively.

Information type	Low Sensitive	Medium Sensitive	Highly Sensitive
Passwords			KSA, USA, Brazil, Germany
Fingerprint		Brazil	KSA, USA, Germany
Financial account information			KSA, USA, Brazil, Germany
Digital signature		Brazil	KSA, USA, Germany
Passport number		Brazil	KSA, USA, Germany
Credit score		USA, Brazil, Germany	KSA
Law enforcement	Brazil	USA, Germany	KSA
Social security no.		Brazil	KSA, USA, Germany
IP address		USA, Brazil	KSA, Germany
Income level		KSA, USA, Brazil, Germany	
Voiceprint		KSA, USA, Brazil, Germany	
Health insurance No.		KSA, Brazil	USA, Germany
GPS location		KSA, USA, Brazil, Germany	
Picture (face)	Brazil	KSA, USA, Germany.	
Medical history	Brazil	KSA, Germany	USA
Home address		KSA, USA, Brazil, Germany	
Browsing history		KSA, Germany	
Online dating activates		KSA, Germany	
Political affiliation	USA, Brazil, Germany	KSA	
Medication		KSA, Germany	
Social network profile	KSA, USA, Brazil, Germany		
Email address	KSA, Brazil, Germany	USA	
Private phone no.	KSA, Brazil	USA, Germany	
License plate no.	KSA, Germany	USA, Brazil	
Shopping behavior	KSA, Germany		
Zip code	KSA, USA, Brazil, Germany		
Mother's maiden name	KSA, Brazil, Germany	USA	
Weight	KSA, USA, Brazil, Germany		
Number of children	KSA, USA, Brazil, Germany		
Height	KSA, USA, Brazil, Germany		
Place of birth	KSA, USA, Brazil, Germany		
Sporting activities	KSA, Germany		
Occupation	KSA, USA, Brazil, Germany		
Religion	KSA, USA, Brazil, Germany		
Name of pet	KSA, Germany		

Tab. 2. *Groups of the high-, medium-, and low-sensitivity information of Saudi Arabia, the USA, Brazil, and 17 times with Germany. Source: Authors.*

The rank distributions of Saudi Arabia, the USA, Brazil, and Germany were compared by using the average rank-order scores and their standard deviation analysis. First, we grouped and ranked all information from 1 to N, where N = 130. *N* is the total number of observations across all countries. Then, we extracted the mean (M) and standard division (SD). The USA had the highest average of ranks (M = 77.81, SD = 33.88), whereas Brazil had the lowest average of ranks (M = 49.75, SD = 35.91). The KSA and Germany showed average ranks (M = 61.79 and 68.4, SD = 40.94 and 32.5, respectively).

The outcomes of the last part of the questionnaire assess the attitude of Saudi users to a set of privacy concerns such as disposition to privacy, propensity to take risks, privacy violation experience, and trust in institutions. Participants demonstrate a high value of attention to their privacy (M = 4.97, SD = 1.38). In terms of propensity to take risks, they tend to risk disclosing their personal information online (M = 5.37, SD = 1.15). Regarding their experiences with online privacy violations, several participants lower than average had a bad experience, or misuse of information experiences (M = 2.57, SD = 1.86). Finally, participants demonstrate a discrepancy in the trust in institutions, depending on their type. They are highly trusting of government institutions (M = 4.76, SD = 1.66), whereas they show low trust levels in private companies (M = 2.15, SD = 1.48).

Users' disposition to their privacy value	**M = 4.97, SD = 1.38**
• Compared to others, I am more eager to share my personal information with companies online	M = 4.65, SD = 1.57
• I am interested in preserving my privacy online	M = 5.12, SD = 1.31
• Compared to others, I tend to pay attention to the risks and threats that may threaten my privacy	M = 5.13, SD = 1.25
The propensity to take risks	
• I am not inclined to take a risk with matters of my personal data or privacy online	M = 5.37, SD = 1.15
Privacy violation experience	**M = 2.57, SD = 1.86**
• I have had bad experiences with my online privacy	M = 2.63, SD =1.88
• I have experienced misuse of data from friends or family	M = 2.5, SD =1.81
Trust in institutions	
• I trust government institutions to use my private data	M = 4.76, SD =1.66
• I trust private non-governmental institutions to use my private data	M = 2.15, SD =1.48
1 "extremely disagree" to 6 "extremely agree".	

Tab. 3. *Saudi users' characteristics of privacy concerns. Source: Authors.*

4.3 Discussion

This study focused on Internet users in Saudi Arabia as a case study aiming to evaluate the perceptions of information sensitivity in Middle Eastern and Islamic countries. We compared the outcomes of our collected sample of Internet users in the KSA with the outcomes of samples from different nations, namely, the US, Brazil, and Germany, as presented by Markos et al. (2017) and Schomakers et al. (2019). Based on the results, we deduced/found several similarities and differences between Saudi users compared with American, Brazilian, and German users.

The survey results showed that passwords, fingerprints, financial accounts, digital signatures, and passport numbers are the most sensitive information for Internet users in the KSA. In addition to the identifying information, we evaluated credit score, law enforcement, social security no., and IP address as highly sensitive information types for Internet users in the KSA. We considered them high risks because this information is used for security purposes in this country.

In contrast, the names of pets were the least sensitive type of information for Saudi users. It is reported as the lowest value of all information types for all nations. That is because Saudis, like most Muslims, are not interested in adopting many types of pets such as dogs and reptile due to Islamic rules that limit this behavior. In this regard, religion, occupation, information about sporting activities, and place of birth are the less sensitive types for Saudi users from low to high, respectively. Generally, Saudi users reported less averages in sensitivity about these types compared with other nations. It shows the cultural influence on the values of the sensitivity of information as claimed by Hofstede (2011). Moreover, these types that do not have any risk cases were taken into consideration; these information types are not used for any security purposes in Saudi Arabia.

The comparison between Saudi and American, Brazilian, and German users shows that the averages of Saudi users were higher than those of American, Brazilian, and German Internet users with information types that were classified as highly sensitive information. The averages were the lowest with information types that were classified as less sensitive information and were similar were classified as medium sensitivity information.

The rank–order of the perceptions of information sensitivity was almost similar across different countries. Internet users in the US, Germany, and the KSA showed the highest perception average of information sensitivity. By contrast, those in Brazil showed below average. Internet users in Germany and the KSA showed the closest average scores. However, the similar rank–order supports the guess–work of (Markos et al., 2017; Schomakers et al., 2019). They claimed that an international consensus exists about similar degrees of information sensitivity, regardless of the difference of cultures, nations, and religions.

The attitude of Saudi users towards their privacy concerns showed an interest in preserving their privacy online. Saudi users are not inclined to risk disclosing personal data online. In this regard, our survey shows that a low percentage of Saudis have a bad experience with their online privacy or have experienced the misuse of their friends' or family' data. In addition, Saudi users tend to trust government agencies to use their data. In contrast, they exhibit low levels of trust in private NGOs.

This study showed slight differences between Internet users in the KSA, the US, Brazil, and Germany concerning their perception of information sensitivity. Nevertheless, our results showed similarities concerning the global model of perception of information sensitivity. Internet users in the KSA were close in their perceptions with those in Germany, and they

showed the most variance with those in Brazil. Except for personally identifiable information, Internet users in the KSA generally showed lower sensitivity levels than those in the US and Germany and higher sensitivity levels than those in Brazil.

5   Conclusion

This study aimed to evaluate the perception of information sensitivity of Internet users in Saudi Arabia as a case study to evaluate the perceptions of information sensitivity in Middle Eastern and Islamic countries. In addition, this study tested the factors influencing Saudi privacy perception. For that, we conducted an online questionnaire, analyzed and compared the results of 508 participants from Saudi Arabia with the information sensitivity perception of American, Brazilian, and German users. Based on our survey, results show slight differences between Internet users in Saudi Arabia, USA, Brazil, and Germany in the perception of information sensitivity.

Meanwhile, the rank–order of the sensitivity of information types shows similarity among nations. This study scoped an important area in the world. Generally, the Middle East and particularly Saudi Arabia have been ignored in these types of studies. Therefore, this study contributes to improving the understanding of the international perception of information sensitivity. This study adds views about the perception of a wide region different from the usual case studies of Western and Asian counterparts.

ORCID

Khaled Almotairi   http://orcid.org/0000-0002-5961-183X

Bilal Bataineh   http://orcid.org/0000-0002-4525-1642

References

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, 42(2), 249–274. https://doi.org/10.1086/671754

Alashoor, T., Sehee, H., & Rhoda, J. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, 41. https://doi.org/10.17705/1CAIS.04104

Alshahrani, H. A. (2016). A brief history of the Internet in Saudi Arabia. *TechTrends*, 60(1), 19–20. https://doi.org/10.1007/s11528-015-0012-5

Assembly, U. N. G. (1949). *Universal declaration of human rights* (Vol. 3381). Department of State, United States of America.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bauer, C., & Schiffinger, M. (2016). Perceived risks and benefits of online self-disclosure: Affected by culture? A meta-analysis of cultural differences as moderators of privacy calculus in person-to-crowd settings. In *Proceedings of the 24th European Conference on Information Systems* (Article 68). AIS.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419–426. https://doi.org/10.1016/j.chb.2015.07.025

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior*, *30*, 79–86. https://doi.org/10.1016/j.chb.2013.07.059

Chen, J. Q., Zhang, R., & Lee, J. (2013). A Cross-Culture Empirical Study of M-commerce Privacy Concerns. *Journal of Internet Commerce*, *12*(4), 348–364. https://doi.org/10.1080/15332861.2013.865388

Fianu, E., Ofori, K. S., Boateng, R., & Ampong, G. O. A. (2019). The Interplay Between Privacy, Trust and Self-disclosure on Social Networking Sites. In *Proceedings of the International Working Conference on Transfer and Diffusion of IT* (pp. 382–401). Springer. https://doi.org/10.1007/978-3-030-20671-0_26

Gilbert, M. A. (2019). Strengthening Your Social Media Marketing with Live Streaming Video. In Al-Masri A., Curran K. (eds.) *Smart Technologies and Innovation for a Sustainable Future* (pp. 357–365). Springer. https://doi.org/10.1007/978-3-030-01659-3_42

Hofstede, G. (2011). Dimensionalizing Cultures: the Hofstede Model in Context. *Online Readings in Psychology and Culture*, *2*(1). https://doi.org/10.9707/2307-0919.1014

Hoftede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: software of the mind: intercultural cooperation and its importance for survival.* McGraw-Hill.

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275–298. https://doi.org/10.25300/misq/2013/37.1.12

Hung, P. C. K., & Cheng, V. S. Y. (2009). Privacy. In *Encyclopedia of Database Systems* (pp. 2136–2137). Springer. https://doi.org/10.1007/978-0-387-39940-9_274

Huo, J., Desai, R., Hong, Y.-R., Turner, K., Mainous, A. G., & Bian, J. (2019). Use of Social Media in Health Communication: Findings from the Health Information National Trends Survey 2013, 2014, and 2017. *Cancer Control*, *26*(1), 107327481984144. https://doi.org/10.1177/1073274819841442

Jiacheng, W., Lu, L., & Francesco, C. A. (2010). A cognitive model of intra-organizational knowledge-sharing motivations in the view of cross-culture. *International Journal of Information Management*, *30*(3), 220–230. https://doi.org/10.1016/j.ijinfomgt.2009.08.007

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2017). Advances in Social Media Research: Past, Present and Future. *Information Systems Frontiers*, *20*(3), 531–558. https://doi.org/10.1007/s10796-017-9810-y

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*. ACM. https://doi.org/10.1109/HICSS.2010.307

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering*, *4*(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Li, Y., Wang, X., Lin, X., & Hajli, M. (2018). Seeking and sharing health information on social media: A net valence model and cross-cultural comparison. *Technological Forecasting and Social Change*, *126*, 28–40. https://doi.org/10.1016/j.techfore.2016.07.021

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management*, *55*(8), 1005–1023. https://doi.org/10.1016/j.im.2018.05.006

Lozano, L. M., García-Cueto, E., & Muñiz, J. (2008). Effect of the Number of Response Categories on the Reliability and Validity of Rating Scales. *Methodology*, *4*(2), 73–79. https://doi.org/10.1027/1614-2241.4.2.73

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *Journal of Public Policy & Marketing*, *36*(1), 79–96. https://doi.org/10.1509/jppm.15.159

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2016). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs*, *51*(1), 133–161. https://doi.org/10.1111/joca.12111

Mollah, M. B., Zeadally, S., & Azad, M. A. K. (2019). Emerging Wireless Technologies for Internet of Things Applications: Opportunities and Challenges. In *Encyclopedia of Wireless Networks* (pp. 1–16). Springer. https://doi.org/10.1007/978-3-319-32903-1_328-1

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2019). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, 37(1), 101413. https://doi.org/10.1016/j.giq.2019.101413

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Pires, I., Garcia, N., Pombo, N., & Flórez-Revuelta, F. (2016). From Data Acquisition to Data Fusion: A Comprehensive Review and a Roadmap for the Identification of Activities of Daily Living Using Mobile Devices. *Sensors*, *16*(2), 184. https://doi.org/10.3390/s16020184

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems*, 19(2), 181–195. https://doi.org/10.1057/ejis.2010.15

Robbins, S. S., & Stylianou, A. C. (2002). A study of cultural differences in global corporate web sites. *Journal of Computer Information Systems,* 42(2), 3–9. https://doi.org/10.1080/08874417.2002.11647480

Roberts, T. H. (2012). A Cross-Disciplined Approach to Exploring the Privacy Paradox: Explaining Disclosure Behaviour Using the Theory of Planned Behaviour. In *UK Academy for Information Systems Conference Proceedings 2012*. AIS.

Schomakers, E.-M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management*, *46*, 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2). https://doi.org/10.29012/jpc.v4i2.620

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*, *3*(1), 205630511668803. https://doi.org/10.1177/2056305116688035

Veltri, N. F., Krasnova, H., & Elgarah, W. (2011). Online Disclosure and Privacy Concerns: a Study of Moroccan and American Facebook Users. In *Proceedings of 17th Americas Conference on Information Systems*. AIS.

Westin, A. F. (1967). *Privacy and freedom*. Athenum.

Wirth, J., Maier, C., Laumer, S., & Weitzel, T. (2019). Perceived information sensitivity and interdependent privacy protection: a quantitative study. *Electronic Markets*, *29*(3), 359–378. https://doi.org/10.1007/s12525-019-00335-0

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

The article has been peer-reviewed.