*future internet*

MDPI

*Article*

# Privacy Policy Analysis of Banks and Mobile Money Services in the Middle East

**Yousra Javed [1,*], Elham Al Qahtani [2] and Mohamed Shehab [2]**

[1] School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad 44000, Pakistan
[2] Department of Software and Information Systems, University of North Carolina, Charlotte, NC 28201, USA; ealqahta@uncc.edu (E.A.Q.); mshehab@uncc.edu (M.S.)
* Correspondence: yousra.javed@seecs.edu.pk

**Abstract:** Privacy compliance of the Middle East's financial sector has been relatively unexplored. This paper evaluates the privacy compliance and readability of privacy statements for top banks and mobile money services in the Middle East. Our analysis shows that, overall, Middle Eastern banks have better privacy policy availability and language distribution, and are more privacy compliant compared to mobile money services. However, both the banks and mobile money services need to improve (1) compliance with the principles of *children/adolescent's data protection*, *accountability and enforcement*, and *data minimization/retention*, and (2) privacy statement texts to be comprehensible for a reader with ∼8 years of education or less.

**Keywords:** banks; FDIC; GSMA; middle east; mobile money; privacy compliance; privacy policy

check for updates

**Citation:** Javed, Y.; Al Qahtani, E.; Shehab, M. Privacy Policy Analysis of Banks and Mobile Money Services in the Middle East. *Future Internet* **2021**, *13*, 10. https://doi.org/10.3390/fi13010010

Received: 27 November 2020
Accepted: 28 December 2020
Published: 3 January 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

Online banking enables bank customers to perform transactions via web or mobile app from the convenience of their homes. Similarly, mobile money services enable users, especially those without a bank account to request/transfer money, and make bill payments etc. over the phone.

The Middle East has recently seen an exponential growth in the adoption of smartphones and mobile payment solutions. According to Deloitte's Global Mobile Consumer Survey [1], two Middle Eastern regions, namely, the Kingdom of Saudi Arabia and the United Arab Emirates have the highest smartphone penetrations at 97% compared to other countries. In addition, 40%, 22%, and 24% of users in the Middle East use mobile payments offered by banks, Telecom providers, and other organizations respectively. Moreover, the recent COVID-19 pandemic has further accelerated the push towards such solutions in the Middle East [2]. For instance, the Saudi Arabian Monetary Authority [3] recently established its payment infrastructure to encourage cashless payments (e.g., STC Pay) in order to reduce physical contact among customers and merchants. Other examples of mobile money services deployed in the Middle East include BenefitPay in Bahrain [4] and Orange Money in Jordan and Egypt [5].

This increase in usage of mobile money services and online banking in the Middle East along with the recent data breaches in some of these banks [6–8] highlight the importance of investigating their user data protection and privacy practices. To the best of our knowledge, no study on the privacy compliance of Middle Eastern banks and mobile money services exists in the literature. Although Bowers et al. [9] have evaluated the privacy policies of International mobile money services and US banks, only two of these were from the Middle East. Other work on privacy policy analysis in the Middle East has focused on e-government websites and e-commerce sectors [10,11]. We perform an analysis of privacy policies from Middle Eastern banks and mobile money services in relation to the principles of widely examined standards for the mobile money industry and government, namely,

Global System for Mobile Communications (GSMA) [12] and Federal Deposit Insurance Corporation (FDIC) [13], respectively, using a methodology similar to Bowers et al. [9]. This is because there is no such standard for the Middle East and only a few of the Middle Eastern countries currently have their own data protection laws [14]. We investigate the following research questions (RQs):

**RQ1.** How compliant are the privacy policies of Middle Eastern banks and mobile money services with the GSMA and FDIC privacy principles?

**RQ2.** How readable are the privacy policies of Middle Eastern banks and mobile money services?

To answer these research questions, we performed a manual analysis on a privacy policy dataset of top 25 banks and 30 mobile money services from the Middle East. Our results show that, overall, Middle Eastern banks have better privacy policy availability and language distribution, and are more privacy compliant compared to mobile money services. However, both the banks and mobile money services need to improve (1) compliance to the principles of *children/adolescent's data protection*, *accountability and enforcement*, and *data minimization/retention*, and (2) privacy statement texts to be comprehensible for a reader with about eight years of education or less.

The rest of the paper is organized as follows: Section 2 discusses the background for this work. Section 3 discusses the existing literature relevant to this topic. Section 4 describes our methodology in detail, and Section 5 shows the results of our analysis. In Section 6, we discuss our findings along with their practical implications, and opportunities for future work. Section 7 concludes the paper with main takeaways.

## 2. Background

### *2.1. Privacy Policy*

A privacy policy is a document that describes whether and how a user's personal data are being collected, stored, used, and shared with third parties according to the applicable privacy laws and regulations in the region. Any organization that collects personally identifiable information from its users is required to provide an accessible privacy policy for the end-users, usually through a link in the footer section of the website/app's landing page. Figures 1 and 2 show screenshots of privacy policy of a bank and mobile money service from the Middle East.

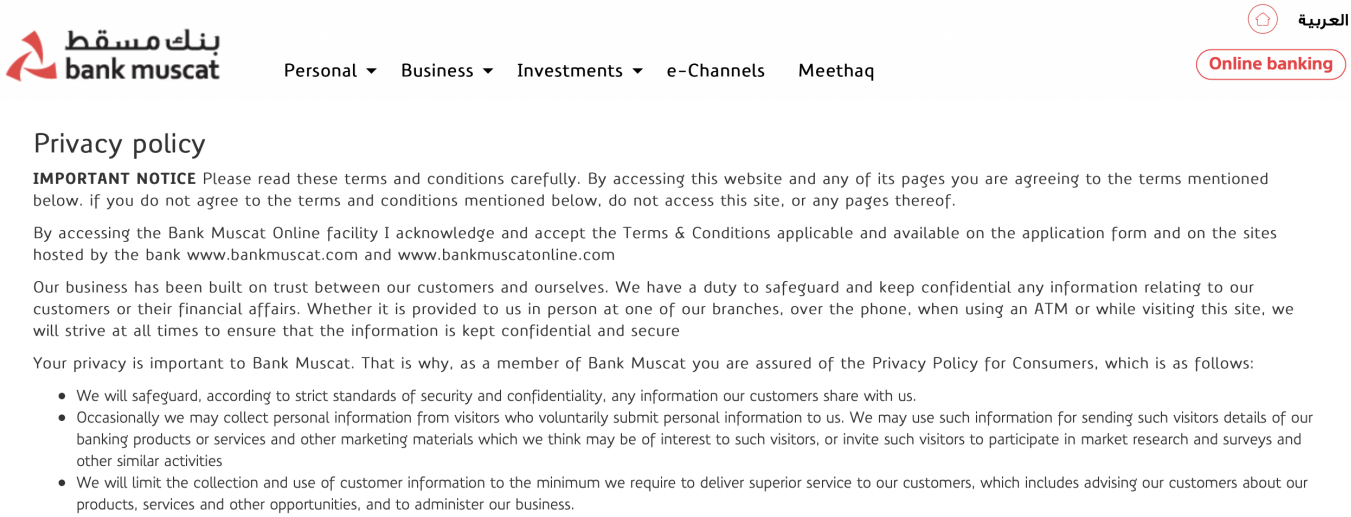


**Figure 1.** A screenshot of Qatar Islamic Bank privacy policy.

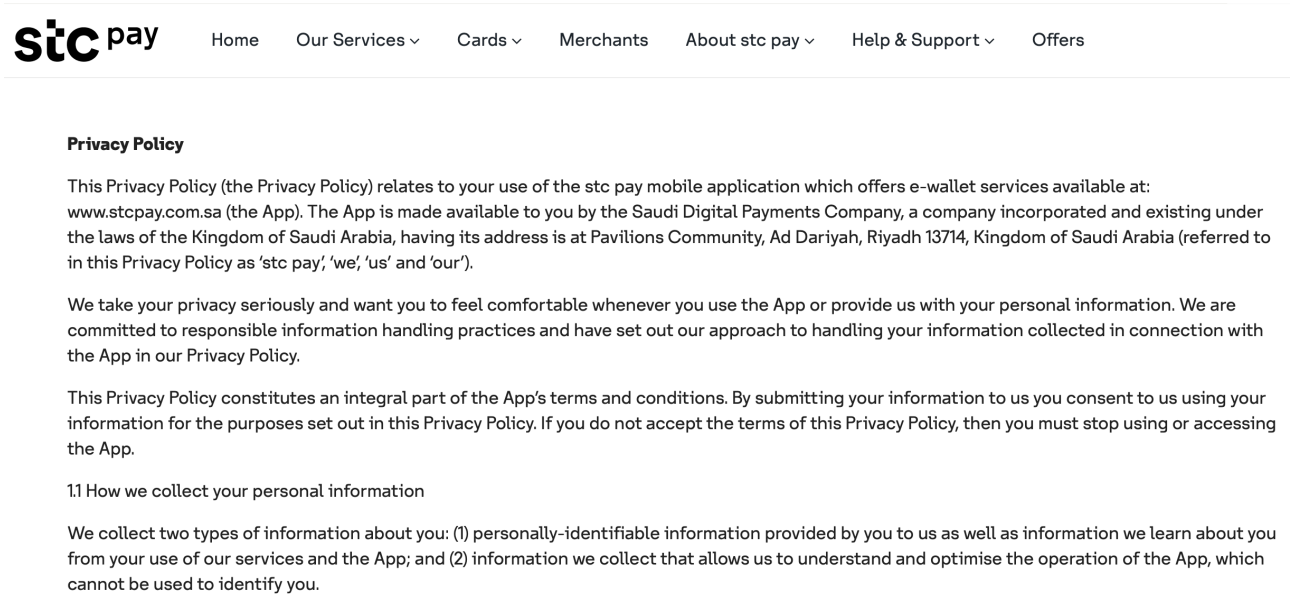


**Figure 2.** A screenshot of STC Pay privacy policy.

***Note:*** *In the remainder of the paper, we use the terms privacy policy, privacy statement, and privacy notice interchangeably.*

### *2.2. Mobile Money Services*

Mobile money or mobile-phone-based financial service is a service that allows users to spend, store, or receive money using an account stored on their cell phones. Mobile money services differ from phone-based access to mobile banking (e.g., Bank of America mobile app) and mobile payment services (e.g., Google Pay, PayPal) in terms of targeted customers, services providers, and technology for supporting these services [9].

Mobile money offers services to unbanked users as well as customers who have a bank account for some apps (e.g., STC Pay as shown in Figure 3), whereas both mobile payment and mobile banking target only their existing customers. In addition, mobile money is often provided by telecommunication providers or local financial regulations, whereas both mobile payment and mobile banking are run by financial regulators. Mobile money services are supported by mobile Internet, SMS, or Universal Supplementary Services Data as part of phone's configuration, whereas both mobile payment and mobile banking are activated only through mobile Internet.

According to the GSMA [15], two billion unbanked people in Middle East and North Africa do not have access to financial services. However, the gradual increase in usage of mobile money is providing payment services to low-income populations in the developing countries such as Middle East and North Africa since banks do not provide services to customers with low balances. The Kenyan mobile money app, M-Pesa, was deployed by SafariCom and was introduced for this purpose in March 2007 [16]. The recent statistics [17] show that more than 20% customers in the Middle East and North Africa perform transactions through smartphone apps that run the country's mobile phone services. For instance, the Arab States of the Gulf (e.g., Qatar and Saudi Arabia) [18,19] have many immigrant workers who make international remittances through mobile money apps in an easy and secure way.

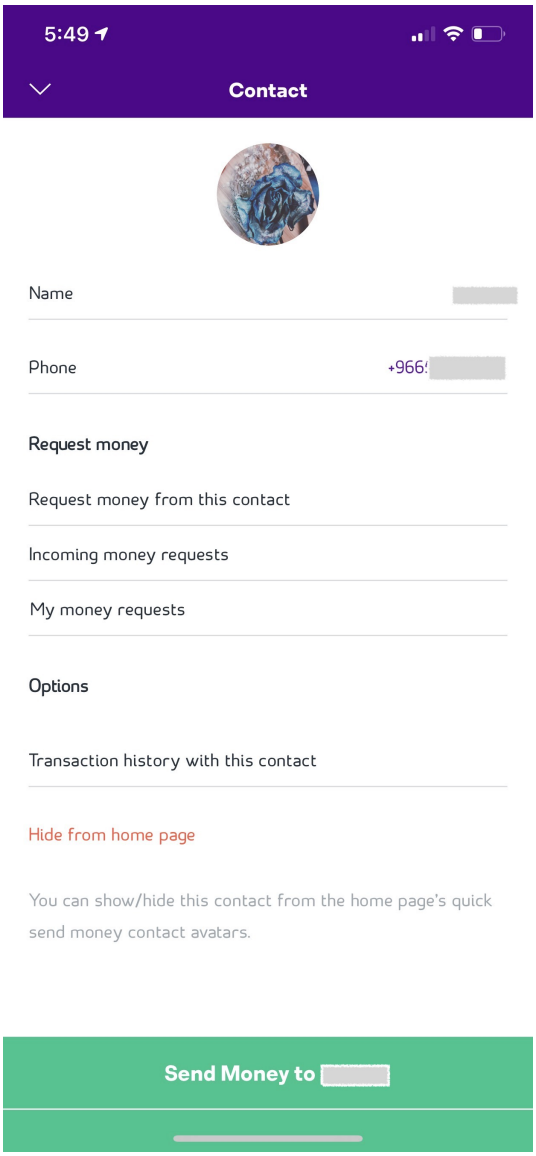


**Figure 3.** A screenshot showing sending money to a user via STC Pay App.

### *2.3. GSMA and FDIC Principles*

The GSMA and FDIC regulations have identified principles that a privacy policy in the financial and mobile sector should implement. We use the following GSMA and FDIC principles compiled by Bowers et al. [9] in our analysis:

**GSMA**

1. *Purpose of Data Collection:*
   Policies should state the reasons for collecting, accessing, and sharing of user data and ensure that it is used for legitimate business purposes.
2. *Children and Adolescents:*
   The service should ensure that the collection, access, and use of children's personal information (if applicable) complies with the national laws.
3. *Accountability and Enforcement:*
   Employees must be held accountable for the proper use and protection of user information.

**FDIC**

4. *Collection Process:*
   A privacy policy should provide the types of personal information that will be collected.
5. *Definitions:*
   A privacy policy should define terms related to collection process, opt-out, information disclosure, etc.
6. *Examples:*
   A privacy policy should specify examples of the collection process, opt-out, and information disclosure, etc.
7. *Third Parties:*
   A privacy policy should specify the third parties with whom the bank shares users' non-public personal information.

**GSMA & FDIC**

8. *User Choice and Control:*
   A privacy policy should clearly mention the user's right to opt-out and control the collection/use of their personal information.
9. *Security:*
   A privacy policy should clearly state how the personal information of users will be protected and safeguarded.
10. *Sharing Process:*
    A privacy policy should specify the personal data of users that may be shared with third parties.
11. *Data Minimization/Retention:*
    Only the minimum amount of personal information should be collected, accessed, and used, and only for as long as required to achieve the purpose.

### *2.4. Readability*

Readability measures how easy it is to understand a piece of text by an average person. Several metrics [20–22] have been proposed to evaluate the readability of a piece of English text. The popular ones are discussed as follows:

1. Flesch Reading Ease: This metric specifies the level of education needed to be able to comprehend a piece of text. A score between 0 and 100 is calculated (though scores outside of that range are possible). A higher score means better readability.
   Flesch Reading Ease is one of the most widely established text readability computation metrics, and has been incorporated into law in several countries.
2. Flesch–Kincaid (FK) Grade Level: The Flesch Reading Ease metric was revised in 1970s to create the Flesch–Kincaid Grade Level. This metric works in the same way, but produces a grade level rather than a score between 0 and 100. The values range from 0 to 20, where lower value means that the text is easier to comprehend, whereas a higher value means that the text is hard to read. The FK Grade Level score is based on sentence length and word length.
3. Automated Readability Index: This metric was developed in the 1960s to assist in analyzing the readability of technical manuals, reports, and training documents. It focuses on letter and word count instead of syllable count.
4. SMOG Index: The Simple Measure of Gobbledygook (SMOG) index is used in consumer-oriented healthcare material and is based on the number of words in the text with more than one syllable. Any word with three or more syllables is counted as difficult, and the number of such words in the text determines the SMOG index.
5. Gunning Fog Index: This metric generates a grade level between 0 and 20 to estimate the years of education the reader requires to understand the text on single read. If a text has Gunning Fox Index of 5, then it requires atleast 5 years of education (in the US schooling system) to understand the text.

6. Coleman–Liau Index: This metric also calculates the US grade level needed to understand the text. However, it doesn't involve any syllable counting, but instead concentrates on characters per word.

In addition to the English language, readability metrics for other languages that correlate well with English have been proposed. This includes Open Source Metric for Measuring Arabic Narratives (OSMAN) [23] for Arabic text, which is a modified version of Flesch and Fog formulas. Similarly, the Atesman Reading Ease Formula [24] has been proposed for Turkish text. However, these metrics have not been widely used yet.

## 3. Related Work

In this section, we present the literature that is most relevant to this research. We first discuss the existing studies that have analyzed the privacy policies of financial institutions in the West and the Middle East with regard to compliance with applicable laws and regulations. Next, we discuss existing work evaluating the readability of privacy statements of financial institutions.

Privacy compliance by financial institutions in the West has been widely explored. For instance, Cranor et al. [25] evaluated privacy the notices of 6191 U.S. financial institutions regarding data-sharing practices, opt-out of data sharing, and the collection of personal information stated in the privacy policy. Their findings indicated that large institutions are more likely to share consumers' personal information with third parties for marketing reasons. Similarly, Bowers et al. [9] evaluated the privacy policies of 54 mobile money services from 32 countries. They compared the privacy compliance of these applications with that of the top 50 U.S. financial institutions that have a well-established regulatory structure. The privacy statements of the mobile money services and US banks were evaluated against the 11 principles from GSMA and FDIC regulations demonstrating that overall banks have better compliance compared to the mobile money services.

The literature on privacy compliance in the Middle East is scarce. The existing studies on this topic show that privacy policy availability in e-commerce and e-government websites in the Middle East is low. Shalhoub et al. [11] evaluated the privacy policies of 183 e-commerce websites in Gulf Cooperation Council countries against the Federal Trade Commission's Fair Information Practice Principles (FIPPs). They found that 73.2% of these websites had no privacy policy available. Similarly, Alhomod et al. [10] evaluated the privacy policies of 54 e-government websites in Saudi Arabia against FIPPs and found that 72% websites did not have a privacy policy. In addition, 40% of the websites that had a privacy policy complied with two or less of the five privacy principles. We add to this literature by studying the privacy compliance of Middle Eastern banks and mobile money services.

Several studies have investigated the readability of privacy statements of financial institutions. For instance, Lewis et al. [26] evaluated the readability of privacy policies of financial institutions (25 banks) and compared them to policies of companies offering financial services (25 check cashing companies and 25 credit counseling companies) using the Flesch–Kincaid Grade Level score. They found that the average reading grade levels are above 12 for privacy policies of all three business sectors. Bowers et al. [9] calculated the readability of privacy statements from banks and mobile money services using the Flesch–Kincaid score, showing that mobile money policies, on average, seemed harder to understand compared to their traditional banking peers. Similarly, McDonald and Cranor [27] estimated that an average American Internet user needs to spend 201 h per year to read the privacy policies of all the websites they have visited. Our work extends these studies by measuring the readability of the privacy statements of Middle Eastern banks and mobile money services.

## 4. Methodology

We used a study methodology similar to Bowers et al. [9] which evaluated the privacy policies of 54 mobile money services from 32 countries. These apps were collected from

GSMA Mobile Money Tracker and mobile money websites [28]. The authors compared the privacy compliance of these applications with that of the top 50 U.S. financial institutions that have a well-established regulatory structure. The privacy statements of these mobile money services and US banks were evaluated against the 11 principles from GSMA and FDIC regulations (Section 2.3). They also evaluated the readability and update frequency of the privacy policies as well as their availability in the official language of the countries where the mobile money applications were deployed.

We evaluate the privacy policies of top 25 Middle Eastern banks and 30 mobile money services against the same 11 principles to have an objective basis of comparison. We also compute the readability score and word count, and check the privacy policy's availability in English and the official language.

### *4.1. Dataset*

To build our dataset, we first compiled a list of mobile money services that were developed in the Middle East [29] (Figure 4), by searching the Apple and Google Play stores, websites of mobile money providers, and the GSMA Mobile Money Tracker [28]. This resulted in a comprehensive list of 30 mobile money services. We then leveraged the Banker database [30] to retrieve a similar number of top Middle Eastern banks which were rated globally on attributes, such as digital and financial services. This resulted in a list of 25 banks. We then retrieved the privacy policy URL (if available) from the websites of banks and mobile money services in our dataset. Table 1 shows the Middle Eastern banks and mobile money services used in our dataset. The complete Middle Eastern banks and mobile money services dataset with links to privacy policies is available at (https://bit.ly/2CyZKoI).

**Table 1.** Middle Eastern Banks and Mobile Money Services Dataset.

| Country | Mobile Money Services | Banks |
|---|---|---|
| Bahrain | BenefitPay, bwallet | Ahli United Bank |
| Cyprus | MTN Mobile Money | - |
| Egypt | NBE-PhoneCash, Vodafone Cash, Flous, Orange Money | - |
| Iraq | ZainCash, AsiaHawala | - |
| Jordan | Dinarak, Mahfazti by Umniah, Orange Money, AYA PAY | Arab Bank |
| Lebanon | PinPay | - |
| Oman | Pay+, Ooredoo Oman, efloos | BankMuscat |
| Qatar | Thawani Pay, Ooredoo Qatar | Qatar National Bank, Qatar Islamic Bank (QIB), Commercial Bank |
| Saudi Arabia | STC Pay, BayanPay, Halalah, Careem Pay, AlinmaPay | National Commercial Bank (AlAhli Bank), Al Rajhi Bank, Samba Financial Group, Riyadh Bank, Saudi British Bank (SABB), Banque Saudi Fransi, Arab National Bank, AlInma Bank |
| Turkey | BKM Express, fastPay, Paycell | - |
| UAE | eWalletAE, mePay | First, Abu Dhabi Bank, Emirates NBD, Abu Dhabi Commercial Bank, Dubai Islamic Bank, Mashreqbank, Union National Bank |
| Yemen | Floosak | |
| Israel | - | Bank Hapoalim, Bank Leumi, Israel Discount Bank |
| Kuwait | - | National Bank of Kuwait, Kuwait Finance House |


**Figure 4.** Middle Eastern countries covered in our dataset (highlighted in green).

### *4.2. Privacy Compliance*

To evaluate the privacy compliance of mobile money services and banks in the Middle East, we leveraged the 11 principles mentioned in Section 2.3. To determine how well each of these principles are being implemented in the policies, we used the set of keywords compiled by Bowers et al. [9] for each principle. For instance, the keywords used for the *User Choice and Control* principle include *disable, edit, user can, change*. The complete list of keywords for each principle is shown in Table 2 below. First, the keywords for each principle were searched in the policy statement text. If any of the keywords matched for a particular principle, the corresponding paragraphs were read by the authors to agree on whether the information for the corresponding principle is included in the policy. If one of these paragraphs contained such information, the corresponding bank or mobile money service was considered as compliant for that particular principle. This method was followed for each of the 11 principles. Based on this, a privacy compliance score out of 11 was computed for each bank and mobile money service. We also calculated the overall percentage of banks and mobile money services that complied with each principle.

**Table 2.** Keywords and phrases used in analysis.

| Principle | Keywords |
|---|---|
| Purpose of Data Collection | Reasoning, User Experience, Enhance User Experience |
| Children and Adolescents | Children, Children's Privacy |
| Accountability and Enforcement | Employee, Accountability, Accountable |
| Collection Process | Collect |
| Definitions | Means, Is, Are |
| Examples | Types of Personal Information, For Example, Includes |
| Third Parties | Third Party, Third Parties |
| User Choice and Control | Disable, Edit, User Can, Change |
| Security | Security |
| Sharing Process | Share, Sharing Process |
| Data Minimization and Retention | Minimization, Termination, Continue to share, Retention, Retain |

### *4.3. Readability*

To evaluate the readability of privacy policies, we leveraged the popular and widely used Flesch–Kinkaid readability tests, namely, reading grade level score and reading ease score [20]. The Flesch–Kinkaid reading grade level determines the required US grade-level education to understand a piece of text. The metric's values range from 0 to 20, where a lower value means that the text is easier to comprehend for the reader, whereas a higher value means that the text is hard to read. The Flesch reading ease score gives a score between 1 and 100, with 100 being the highest readability score. A score between 70 to 80 is equivalent to school grade level 8. Higher reading ease scores, therefore, indicate that text is easier to read, whereas, lower numbers mark passages that are more difficult to read.

We calculated the readability metrics using a publicly available online tool [31]. This tool also computes other readability scores, such as the Coleman–Liau index, Automated Readability Index, and SMOG index. We also leveraged the basic text statistics generated by this tool such as the word count of a policy statement.

Moreover, we looked at the language distribution of a privacy policy, i.e., whether the privacy policy is available in English, the official language of the country where the bank or mobile money service is deployed, or both. The official languages of Middle Eastern countries are Arabic, Turkish, Persian, or Hebrew, and the common second language in these countries is English [32]. We performed our analysis on the English version of the privacy policies for the following reasons:

1. English was a common language among the investigators. Moreover, the majority of mobile money services and banks in the Middle East provide their policy statements in English as well as the official language. Only three Turkish apps in our dataset did not have an English version of the policy. Therefore, we used their English translated versions.
2. There is no widely used readability metric for the official languages of Middle East. Although there has been some work on developing a readability metric (e.g., OSMAN proposed by Mahmoud et al. [23]),for Arabic, this work shows that the readability of Arabic text was similar to the readability of its English version. Similarly, for Turkish, Acar et al. [24] found that the Atesman Reading Ease Formula for Turkish text was compatible with the Flesch Reading ease score of its English translation.

## 5. Evaluation

This section presents the results of our privacy policy analysis. We first looked at how many of the investigated banks and mobile money services provide a privacy policy to their users. We found that the availability of privacy policy for the studied banks and mobile money services was high. In addition, 100% of the banks and 83% of the mobile money services provided a privacy policy on their website/mobile app.

Below, we discuss the results regarding privacy policy compliance and readability.

### *5.1. Privacy Compliance*

The banks in our dataset complied with $\sim$8 out of the 11 privacy principles on average, whereas the mobile money services complied with only $\sim$6 of them. A Mann–Whitney U Test between the privacy compliance score of the banks and mobile money services showed that this difference is significant with a $p$-value of 0.02.

The overall compliance percentage per principle was also higher for banks as compared to the mobile money services. Table 3 provides a summary of the compliance analysis. We discuss the results for each of the principles separately.

**Table 3.** Overall percentage (%) of investigated banks and mobile money services complying with each of the GSMA and FDIC principles.

| | GSMA | | | FDIC | | | | GSMA & FDIC | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Purpose of Data Collection | Children and Adolescents | Accountability & Enforcement | Collection Process | Definitions | Examples | Third Parties | User Choice & Control | Security | Sharing Process | Data Minimization/Retention |
| Banks | 100 | 16 | 56 | 96 | 84 | 84 | 92 | 72 | 88 | 96 | 56 |
| Mobile money service | 87 | 20 | 27 | 83 | 83 | 73 | 47 | 50 | 67 | 83 | 43 |

#### 5.1.1. Purpose of Data Collection

This principle had the highest compliance by both the banks and mobile money services compared to other principles. In addition, 100% banks and ∼86% mobile money services in our dataset clearly specified how the collected personal information will be used.

#### 5.1.2. Children and Adolescents

Both the banks and mobile money services were least compliant with this principle, with only 16% and 20% of each respectively specifying whether and how the child's personal information is being collected and protected.

#### 5.1.3. Accountability and Enforcement

Nearly half of the banks (56%), and 27% of mobile money services mentioned in their privacy statements that they hold their employees accountable for proper use and protection of user data.

#### 5.1.4. Collection Process

Both the banks and mobile money services in our dataset did well in terms of listing the types of personal information collected from the user. The percentage compliance of banks and mobile money services was over 80%.

#### 5.1.5. Definitions

About 84% of banks and mobile money services defined the terms concerning the collection process, and information disclosure, etc. in their privacy statement to assist the reader.

#### 5.1.6. Examples

84% of the banks and 73% of the mobile money services provided examples of the collection process and information disclosure. For instance, if information was collected from registration form, the name and email address was specified.

#### 5.1.7. Third Parties

The banks did quite well (92% compliance) in terms of specifying which third-parties they share the collected personal information with. However, only 47% of the mobile money services complied with this principle.

#### 5.1.8. User Choice and Control

72% banks and 50% mobile money services mentioned to some extent that the users can opt-out of providing information and explained how users can control the use of their personal information.

#### 5.1.9. Security

A majority of the banks (88%) clearly stated the measures (e.g., encryption) taken to protect confidentiality and integrity of user data. However, only 67% of mobile money services implemented this principle completely.

#### 5.1.10. Sharing Process

Both the banks (96%) and mobile money services (83%) did well in terms of specifying the personal information of users that will be disclosed to third parties.

#### 5.1.11. Data Minimization/Retention

The compliance of this principle was low by both banks and mobile money services. Only 56% and 43% of banks and mobile money services, respectively, clearly stated that only a minimum amount of user information will be collected, and that it will only be retained for the duration required to fulfill the purpose.

### *5.2. Readability*

Our readability analysis shows that the privacy policies of Middle Eastern banks and mobile money services are difficult to understand since their average reading grade level was high (14.5 and 15.2, respectively), and their average reading ease score was low (31.16 and 28.26, respectively). A Mann–Whitney U test between the reading grade level of the banks and mobile money services showed that this difference is not significant ($p$-value = 0.37). Therefore, a reader needs greater than 14 years of education to understand the privacy policy texts of Middle Eastern banks and mobile money services. Similarly, a Mann–Whitney U test between the reading ease score of the banks and mobile money services showed that this difference is not significant ($p$-value = 0.30).

In addition, these privacy statements are long, with the average length for banks and mobile money services being ∼1514 and ∼1672 words, respectively. A Mann–Whitney U test, however, showed that the policy text word count difference between banks and mobile money services was not significant at $p$-value = 0.48.

Figure 5 shows the relationship between the length of privacy statements and their reading grade levels. For banks, it appears that longer privacy statements are easier to understand compared to shorter ones (as shown by the linear regression line in red). However, for mobile money services, the reading difficulty is increasing linearly with the length of the privacy statements (as shown by the linear regression line in blue). Similarly, Figure 6 shows the relationship between the length of privacy statements and their reading ease scores and demonstrates a similar trend. For banks, it appears that longer privacy statements are easier to understand compared to shorter ones since higher reading ease score means better readability. However, for mobile money services, the reading difficulty is increasing with the length of the privacy statements since longer policies have low reading ease scores.

The language distribution (Figure 7) shows that more than 50% of the privacy policies of banks and mobile money services were available in both English and the official language. Thus, making them accessible to users who are comfortable with only one of the two languages.

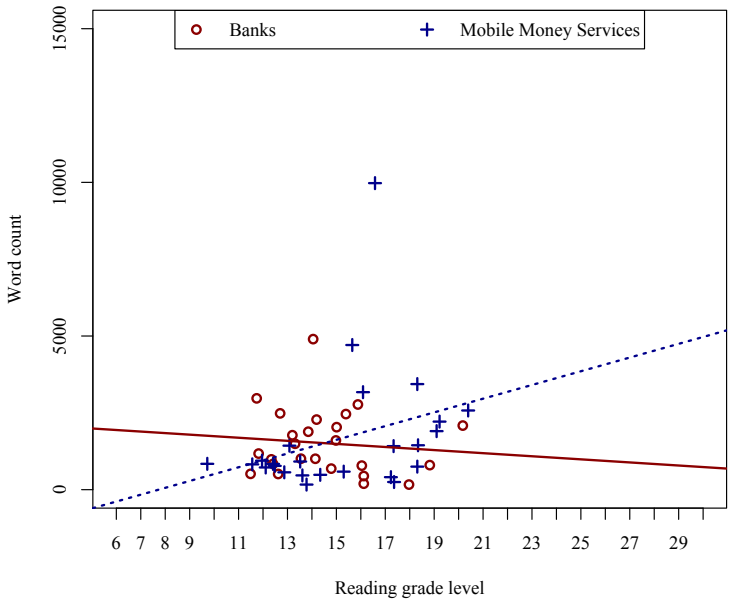


**Figure 5.** Reading grade level vs. word count of Middle Eastern bank and mobile money policies.

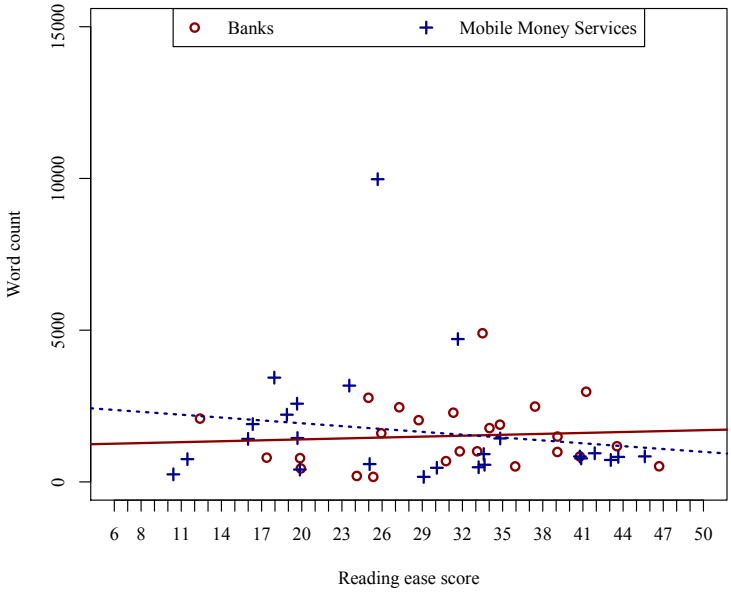


**Figure 6.** Reading ease score vs. word count of Middle Eastern bank and mobile money policies.

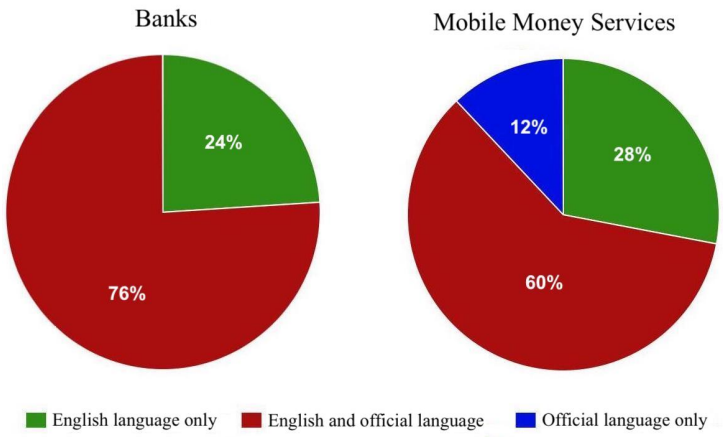


**Figure 7.** Language distribution of privacy policy for Middle Eastern banks and mobile money services.

## 6. Discussion

This section provides a comparative discussion of our findings with the existing literature and elaborates on the practical implications of our work, i.e., how our findings can be useful for end-users and financial organizations. We also discuss the limitations of our work along with future research directions.

### *6.1. Summary of Findings*

#### 6.1.1. Availability

The privacy policy availability results of our dataset are consistent with that of Bowers et al., i.e., banks have better privacy policy availability compared to mobile money services [9]. They found that all U.S. banks had privacy policies; however, 44% of the international mobile money services did not provide a privacy policy. Similarly, all the banks in our dataset provided a privacy policy, whereas only 17% of the mobile money services did not. Thus, privacy statement availability statistics for financial sector in the Middle East seem better compared to the other sectors [10,11].

#### 6.1.2. Compliance

Similar to Bowers et al., overall, the banks in our dataset were more privacy compliant as compared to the mobile money services. The principles with the highest compliance were purpose of data collection, collection process, and sharing process, whereas the principles with the lowest compliance by both banks and mobile money services were children and adolescents, accountability and enforcement, and data minimization/retention. However, unlike Bowers et al., more than (70%) mobile money services in our dataset clearly stated what type of data they collect from users.

#### 6.1.3. Readability

Regarding readability, we observed that the privacy statements of Middle Eastern banks and mobile money services (14.5 and 15.2 reading grade levels, respectively) are much more difficult to understand compared to the US banks and other international mobile money services (10.8 and 12.1 reading grade levels, respectively). However, consistent with Bowers et al., we found that banks' privacy statements are relatively easier to understand compared to those of mobile money services.

Our language distribution results are also similar to Bowers et al. Amongst the banks and mobile money services that provide a privacy statement, ∼(40%) have failed to include a version in English as well the official language.

### *6.2. Practical Implications*

We believe that financial organizations can benefit from the gaps pointed out by our analysis in order to improve compliance of their privacy policies. For instance, both banks and mobile money services in the Middle East need to improve compliance with the principles of children/adolescents' data protection, accountability and enforcement, and data minimization/retention. Similarly, they also need to improve the readability of their privacy statement texts so that they are comprehensible for a reader with eight years of education or less.

Our findings can be helpful for end-users in understanding the current state of privacy practices by banks and mobile money services. For instance, the fact that banks are more privacy compliant than mobile money services. User perceptions about the current privacy practices of mobile money services and banks can be studied, and these expectations can be compared with the actual practices to further increase awareness.

### *6.3. Limitations and Future Work*

Our work is not without limitations. Our primary focus was to analyze the privacy policy statement text to understand compliance with established privacy principles. However, this does not necessarily prove the extent to which the banks and mobile money

services under investigation are actually following the policies specified in their statements. Our future work will focus on analyzing the match between actual data collection, storage, usage, and sharing practice of banks and mobile money services with that mentioned in their privacy statements.

Our analysis is manual in its current state. The lack of automated analysis stems from the fact that a privacy statement is written in natural language and there is no standard template followed which increases the difficulty of parsing. This can be observed in Figures 1 and 2. However, automated analysis is an avenue that can be explored. A browser extension can be developed that can detect a privacy policy on the website and automatically calculate a compliance and readability score.

The involvement of users to validate the readability metric results was out of scope of this work. However, it is crucial to analyze the match between the leveraged tool's readability metric and the actual user rating of the privacy policy text in terms of understanding data collection, storage, usage, and sharing practice of banks and mobile money services. Moreover, since our analysis is on English text, it is imperative to analyze (through a survey) the percentage of Middle Eastern users who read a privacy policy and whether they prefer to read in English or their native language.

## 7. Conclusions

Our preliminary analysis of mobile money services and banks in the Middle East shows that mobile money services are far behind the banks in terms of privacy compliance. Therefore, policy makers in the Middle East should amend their laws to improve compliance by mobile money services. Both banks and mobile money services, however, should improve the readability of their privacy statements and give as much importance to the principles of children/adolescents' data protection, accountability and enforcement, and data minimization/retention, as the principles of data collection, purpose, and sharing. However, a larger study is needed to confirm these findings.

**Author Contributions:** Y.J. contributed towards conceptualization, methodology, data curation, analysis and visualization, and writing—original draft preparation. E.A.Q. contributed towards methodology, investigation, data curation, validation, and writing—review & editing. M.S. contributed towards supervision, validation, and writing—review & editing. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The Middle Eastern banks and mobile money services dataset compiled for this research (with links to privacy policies) is available at (https://bit.ly/2CyZKoI).

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

## References

1. Seemungal, D. Mobile Consumption in a Post-Growth World. 2019. Available online: deloitte.com (accessed on 1 January 2021).
2. Mobile Payments Today. COVID-19 Pushing Consumers Toward Mobile Banking, Online Shopping. 2020. Available online: mobilepaymentstoday.com (accessed on 1 January 2021).
3. Oxford Business Group. Will Covid-19 Containment Measures Accelerate the Transition of Saudi Arabia into a Cashless Society? 2020. Available online: oxfordbusinessgroup.com (accessed on 1 January 2021).
4. BENEFIT. Bahrain's Electronic Network for Financial Transactions. 2016. Available online: https://www.benefit.bh/ (accessed on 1 January 2021).
5. Orange Money Mobile. Available online: https://www.orange.eg/ar/ (accessed on 1 January 2021).
6. InvestBank UAE Suffers Data Breach. 2016. Available online: https://www.arabianindustry.com/technology/united-arab-emirates/news/2016/may/8/investbank-uae-suffers-data-breach-5367726/ (accessed on 1 January 2021).
7. Qatar National Bank: Database Leak Gives Data on Al-Jazeera Journalists and British 'Spies'. 2016. Available online: http://www.ibtimes.co.uk/qatar-national-bank-1-4gb-database-leak-gives-data-customers-journalists-spies-1556787 (accessed on 1 January 2021).
8. Iran Banks Burned, then, Customer Accounts Were Exposed Online. 2019. Available online: https://www.nytimes.com/2019/12/10/world/middleeast/Iran-bank-hacking-protests.html (accessed on 1 January 2021).

9. Bowers, J.; Reaves, B.; Sherman, I.N.; Traynor, P.; Butler, K. Regulators, mount up! Analysis of privacy policies for mobile money services. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security, Santa Clara, CA, USA, 12–14 July 2017; pp. 97–114.
10. Alhomod, S.M.; Shafi, M.M. Privacy Policy in E Government Websites: A Case Study of Saudi Arabia. *Comput. Inf. Sci.* **2012**, *5*, 88. [CrossRef]
11. Shalhoub, Z.K. Content Analysis of Web Privacy Policies in the GCC Countries. *Inf. Secur. J. A Glob. Perspect.* **2006**, *15*, 36–45. [CrossRef]
12. GSMA. Mobile Privacy Principles: Promoting Consumer Privacy in the Mobile Ecosystem. 2016. Available online: http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf (accessed on 1 January 2021).
13. FDIC. Privacy Rule Handbook. 2001. Available online: https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/ (accessed on 1 January 2021).
14. GSMA. Data Privacy Frameworks in MENA. 2019. Available online: https://www.gsma.com/mena/wp-content/uploads/2019/07/GSMA-Data-Privacy-in-MENA-Exec-Summary.pdf (accessed on 1 January 2021).
15. GSMA. 2017. Available online: https://www.gsma.com/mena/resources/state-industry-report-mobile-money (accessed on 1 January 2021).
16. Mas, I.; Morawczynski, O. Designing mobile money services lessons from M-PESA. *Innov. Technol. Gov. Glob.* **2009**, *4*, 77–91.
17. Middle East & North Africa Digital Payments Market-Growth, Trends, Forecasts (2020–2025). 2020. Available online: shorturl.at/nxIJL (accessed on 1 January 2021).
18. MENA: The Final Mobile Money Frontier. 2018. Available online: https://bassiounigroup.com/mena-the-final-mobile-money-frontier/ (accessed on 1 January 2021).
19. Paracha, B.N. NEWSSaudi Mobile Wallet STC Pay Launches International Remittance Service in Partnership with Western Union. 2019. Available online: https://www.menabytes.com/stc-pay-international-remmitances/ (accessed on 1 January 2021).
20. Kincaid, J.P.; Fishburne, R.P., Jr.; Rogers, R.L.; Chissom, B.S. *Derivation of New Readability Formulas (Automated Readability Index, Fog Count and Flesch Reading Ease Formula) for Navy Enlisted Personnel*; Technical Report; Naval Technical Training Command Millington TN Research Branch: Monterey, CA, USA, 1975.
21. Mc Laughlin, G.H. SMOG grading-a new readability formula. *J. Read.* **1969**, *12*, 639–646.
22. Coleman, M.; Liau, T.L. A computer readability formula designed for machine scoring. *J. Appl. Psychol.* **1975**, *60*, 283–284. [CrossRef]
23. El-Haj, M.; Rayson, P. OSMAN—A Novel Arabic Readability Metric. In Proceedings of the Tenth International Conference on Language Resources and Evaluation (LREC'16), Portoroz, Slovenia, 23–28 May 2016; pp. 250–255.
24. Acar, A.; İŞİSAĞ, K.U. Readability and comprehensibility in translation using reading ease and grade indices. *Int. J. Comp. Lit. Transl. Stud.* **2017**, *5*, 47–53. [CrossRef]
25. Cranor, L.F.; Leon, P.G.; Ur, B. A large-scale evaluation of US financial institutions' standardized privacy notices. *ACM Trans. Web* **2016**, *10*, 1–33. [CrossRef]
26. Lewis, S.D.; Colvard, R.G.; Adams, C.N. A comparison of the readability of privacy statements of banks, credit counseling companies, and check cashing companies. *J. Organ. Cult. Commun. Confl.* **2008**, *12*, 87.
27. McDonald, A.M.; Cranor, L.F. The cost of reading privacy policies. *I/S J. Law Policy Inf. Soc.* **2008**, *4*, 543.
28. Mobile Money Deployment Tracker. 2010. Available online: https://www.gsma.com/mobilemoneymetrics/#deployment-tracker (accessed on 1 January 2021).
29. World Population Review. Middle East Countries 2020. 2020. Available online: worldpopulationreview.com (accessed on 1 January 2021).
30. Everington, J. Top 1000 World Banks—QNB Returns to the Top of Middle East Table. 2019. Available online: thebanker.com (accessed on 1 January 2021).
31. Adamovic, M. Online Utility—Free Online Software Utilities. 2009. Available online: https://www.online-utility.org/english/readability_test_and_improve.jsp (accessed on 1 January 2021).
32. Sawe, B. What Languages Are Spoken in the Middle East? 2019. Available online: https://www.worldatlas.com/articles/what-languages-are-spoken-in-the-middle-east.html (accessed on 1 January 2021).