Mobile Commerce - Analysis and Investigation of the Online Safety, Privacy, and Data Forensics of Amazon and Etsy Apps

Gokila Dorai
Augusta University
gdorai@augusta.edu

Shinelle Hutchinson
Purdue University
hutchi50@purdue.edu

Beatriz Rodriguez
Augusta University
berodriguez@augusta.edu

Umit Karabiyik
Purdue University
umit@purdue.edu

Abstract

The COVID19 pandemic has led to the proliferation of the use of online shopping applications among millions of customers worldwide. The enormous potential in technological advancements, particularly mobile technology, has directly impacted mobile commerce, where the shopping process has become so convenient. While the benefits of mobile commerce are multi-fold, the current privacy practices and the extent of user data residue in shopping apps have been less explored. In this paper, we conducted an in-depth, systematic analysis of two of the most popular mobile shopping apps - Amazon and Etsy. Our analysis led to the recovery of user data and shopping activity artifacts from Amazon and Etsy buyer and seller apps on Android/iOS devices. Based on the user data and artifacts found, we have also discussed the implications of default privacy settings, the importance of online safety policies prior to product listings, and implications for research and practice.

1. Introduction

As of November 2021, Statista reported that the iOS Amazon shopping application (app) is the most downloaded app in the shopping apps category in the United States, with over 1.7M downloads from the App Store. Amazon is also the third most downloaded shopping app from the Google Play Store (Statista, 2021a). In 2019, Amazon generated 19.21 billion US dollars in revenue through its subscription services (Statista, 2019a), including Amazon Prime, where 60% of Prime members in 2019 were Gen Z consumers (Statista, 2019b).

More than 80 million buyers have purchased goods from the Etsy online commerce store, as of 2020 (Statista, 2021c). Handmade items, vintage goods, and other supplies are the three main categories of items in the Etsy online marketplace. Similarly, about 4.3 million sellers from 234 countries have sold their products through the Etsy platform as of 2020, of which about 62% are from the US. Furthermore, Etsy's annual gross merchandise sales volume (GMV) rose to more than 10 billion US dollars in 2020 Statista (2021d). In 2021, Etsy was also reported to be one of the 5 most popular online marketplaces according to online sellers in the US based on profitability, customer service, communication, and ease of use (Statista, 2021b).

National Center on Sexual Exploitation (NCOSE, 2021b), a non-profit organization that exposes the links between sexual abuse and exploitation, has released several annual lists (called dirty dozen lists (NCOSE, 2022b)) of online platforms that facilitate sexual exploitation and reveal the lack of strict measures/policies. Amazon has made it to the Dirty Dozen List for the past six years (NCOSE, 2021a). Building on the notoriety of certain item listings found in Amazon, there is a need for effective screening of product listings within these shopping apps, considering the effects of inappropriate content sometimes being shown on these apps especially when children or young adults use innocent search terms to browse for products. Etsy has also been listed in the Dirty Dozen List (NCOSE, 2022a) for selling a range of products that normalize sexual exploitation and abuse. Etsy content filters are also reported to be inadequate to prevent pornography and sexually explicit content, resulting in users being traumatized by unsolicited exposure to this content (NCOSE, 2022a).

In our research, the first goal is to identify and analyze the extent of user data residue that can be recovered from Amazon and Etsy apps using digital

URI: https://hdl.handle.net/10125/103165
978-0-9981331-6-4
(CC BY-NC-ND 4.0)

forensics by following the analysis methodology shown in Fig. 1 and a custom interaction model shown in Fig. 2. In Fig. 2, we have used labels such as EIB, EAS, EIS, EAB, AIB, AAS, AIS and AAB. In these labels, the first letter denotes whether the app used is Etsy (E) or Amazon (A); the second letter denotes whether the device is an iPhone (I) or an Android (A) device; the third letter denotes whether the app is the buyer (B) or seller (S) app; finally there are 10 different items used as our product listings and they are labeled as I_1-I_{10}. When using more than one buyer account, it is denoted B_1 and B_2 in order to distinguish. To achieve our first goal, popular forensic tools such as the Cellebrite UFED 4PC and Magnet Axiom Process for data acquisitions from smartphones devices. Next, the Magnet Axiom Examine was used for examination and analysis of both forensic images. The second goal is to report our findings and discuss various implications related to online safety and data privacy.

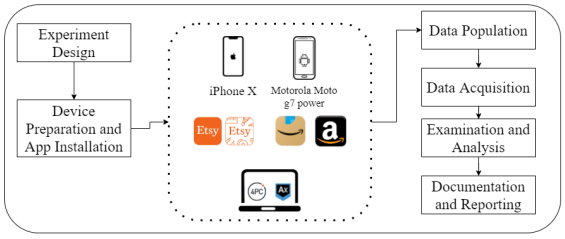


Figure 1. Experimental methodology.

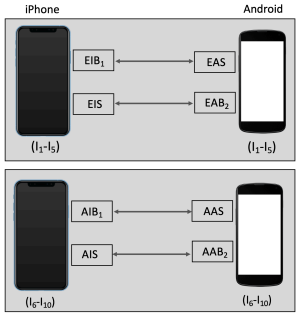


Figure 2. App interaction model.

Our contributions in this paper are multi-fold: (1) we have performed a user data analysis of the Amazon and Etsy buyer and seller mobile shopping apps to identify user data artifacts on Android and iOS smartphones; (2) we have provided a roadmap of user data artifacts for researchers in hopes this information will inform future investigations of these or similar shopping apps; (3) we have discussed the privacy and security concerns due to the presence of raw artifacts in these shopping apps and (4) we have discussed the need for having stricter platform-based regulatory measures to ensure online safety and to avoid unsolicited exposure to inappropriate contents.

2. Related Work

Shopping apps are no exception to privacy and security issues. In 2019, an investigation reported about the security and privacy issues in 30 unnamed shopping apps on both Android and iOS. The report noted that 70% of the apps investigated did not adequately secure the storage of sensitive data (Zimperium, 2019). Kulkarni et al. (2013) addressed privacy issues and how anonymity of a user can be compromised by revealing context-based recommendations in public settings despite safeguarding measures to protect both location and data privacy. Research by Pasha and Saleem (2019) conducted a forensic analysis of the Wish app on Android 7 (Nougat). The authors focused on recovering artifacts related to installation, login, profile, and transaction data. Most notable, the authors recovered the user's email address, phone number, shipping address, and transaction details, including the user's credit/debit card information and shopping activity. Salamh et al. (2021) conducted a forensic analysis of over 30 mobile apps on both Android 10 and iOS 13.3.1. The authors provided a detailed methodology on how they analyzed the forensic images, focusing on the privacy and security-related pitfalls of all the apps investigated. Hutchinson et al. (2020) focused on identifying the privacy and security issues within several dating apps and described the ability for the dating app users' potential matches to become privy to the users' app usage behaviors. Moreover, the authors in Johnson et al. (2022) forensically analyzed nine alternative-tech social applications and identified some security vulnerabilities.

Less has been explored about the extent of user data residue, privacy and online safety of popular mobile commerce applications. Banking and shopping apps are two of the most critical categories of mobile apps that mandate security and privacy protections to safeguard their users' PII. These two categories of apps have access to the same type of data (money transactions and user profile), yet the degree of security and privacy considerations of these apps are disparate. For instance, forensic investigations into and safety assessments of m-shopping apps are limited in the literature at the time of this writing. Alternatively, m-banking apps have been heavily investigated, both in terms of their privacy and security Abdulla Al-Delayel (2022), Bojjagani and Sastry (2016), Chanajitt et al. (2018), Datta et al. (2020),

Nikkel (2020), Osho et al. (2019), and Salamh et al. (2021).

3. Research Methodology

Our methodology follows the guidelines and best practices for populating user data in mobile devices and forensic acquisition that have been published by the National Institute of Standards and Technology (NIST) Rick Ayers and Jansen (2014). In this study, two smartphone devices were used, an Apple iPhone X running iOS 14.3 and a rooted Motorola Moto g7 power running Android 9. The selection criteria for these two operating systems were simply their common use by global smartphone users (Statcounter, 2021) or their availability for jailbreaking/rooting during the acquisition phase (Cellebrite, 2021). The apps we investigated are the buyer and seller apps for Amazon and Etsy. Fig. 1 provides a visual representation of the methodology we followed. In this research, we used only the most recent versions of the applications at that time. The app versions are significant, especially for the reproducibility of the findings. Note that the organization of data inside the structure of sand-boxed mobile applications depends on the operating system version and the app version (Shimmi et al., 2020). Table 1 provides a summary of the apps and their versions used in this study.

Table 1. Version numbers of the apps investigated.

OS	Amazon Seller	Amazon Shopping	Sell on Etsy	Etsy (Buyer)
Android	7.5.1	22.12.2.100	3.60.1	5.76.0
iOS	7.5.4	17.8.0	3.53	5.75.1

3.1. Seller/Buyer Account Registration

Both buyer and seller apps were used on the iPhone X and Moto g7 devices. Fig. 3 shows the activity diagram of the Amazon/Etsy Seller central registration process. User registration, listing the items, user authentication, pricing, and inventory were the various steps in the process of creating seller accounts for Amazon and Etsy, respectively.

3.2. Data Population

In preparation for the data population on the devices in this study, two email accounts were created to serve as buyer accounts, while we have used one seller account.

The roadmap/steps to populating our experimental devices with user data is: (1) Factory resetting the iPhone X device to default. (2) Verifying root access on the Moto g7 smartphone using the Root Checker app. (3) Creating new accounts on both iCloud and Google for the iPhone X and Moto g7, respectively. (4) Abiding by the NIST guidelines for the mobile device population, data was entered in the devices accordingly. This means that we installed the shopping apps from the App Store and the Google Play Store on both devices. For each shopping app, we performed the following data population sub-steps: (4.1) The same seller account was used for each app by following the sequential steps laid out in Fig. 3. In our data population model, as an exception, note that we were unable to list handmade items for sale via the iOS Amazon Seller app. As such, we listed our items by accessing the Amazon Seller Central web page[1] via the iOS Safari browser. (4.2) Created two buyer accounts through the app, one used on the iPhone X and the other on the Moto g7. (4.3) Used each of the smartphone devices to interact with various features of the shopping app and with our buyer/seller accounts. A more detailed description of our exact interactions is provided in Section 3.3.

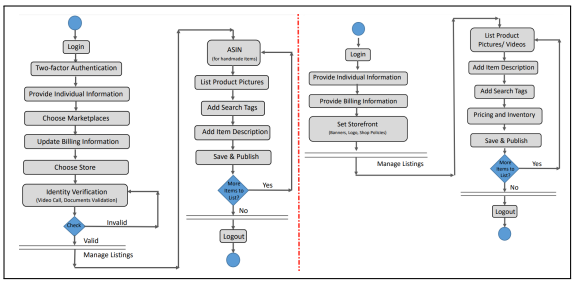


Figure 3. Activity diagrams of user registration and item listing process in Amazon Seller Central (on the left) and Etsy Seller Central (on the right).

Then we performed an advanced logical acquisition of the iPhone X using Cellebrite UFED 4PC and obtained a logical image of the Moto g7 using Magnet Axiom Process followed by examination and analysis of both forensic images using Magnet Axiom Examine.

3.3. Shopping Apps Interactions

In this section, we detail the interactions that we conducted for each shopping app. For example, we set up app accounts, searched for specific items, interacted with our seller account, and purchased item(s) from the seller account. The interactions were completed over the course of two months, after which the devices were prepared to perform forensic acquisition. For each buyer app, we followed the format outlined here: (1) Used the app to create an account; (2) Populated the user profile information; (3) Interacted with various features offered by the app; (4) Searched for specific items; (5)

[1] https://sellercentral.amazon.com

Table 2. List of device/software tools.

Name	Model/Version
iPhone X	A1865(non-jailbroken)
Motorola moto g(7) power	SM-G9201(rooted)
Cellebrite UFED 4PC	7.45.1.43
Checkra1n beta (Cellebrite, 2021)	0.9.6
CyberChef (CyberChef, 2021)	9.32.3
DB Browser for SQLite	3.12.2
DCode	5.1
Magnet Axiom Process	5.2.0.25407
Magnet Axiom Examine	5.2.0.25407

Interacted with our seller account; (6) Purchased five items from our seller account.

3.4. Acquisition

After all interactions with the smartphones were completed, we forensically acquired the iPhone X image using Cellebrite UFED 4PC and the Moto g7 device using Magnet Axiom Process. The Moto g7 smartphone was rooted before starting this study, giving us full access to the filesystem and all the data stored there. Alternatively, during the acquisition of iPhone X, we used the commercial forensic tool Cellebrite which jailbroke the device using Checkra1n beta.

3.5. Examination and Analysis

As discussed earlier, we utilized Magnet Axiom for the forensic examination and analysis processes. Magnet Axiom is a commercial forensic tool and has the ability to process *.dar* images that have been created using Cellebrite's advanced features or from acquiring a device that was jailbroken with Checkra1n. Once we secured the forensic images of both devices, we loaded the *.dar* iPhone X image into Magnet Axiom Process. The analysis was then completed using Magnet Axiom Examine to view all artifacts recovered from both devices. We chose to do this because using Magnet allowed us to collaborate with the analysis phase much more easily. A summary of all devices and software tools used in this study is provided in Table 2. These are also the commonly used commercial tools that are also listed in the NIST software quality group (NIST, 2017). At the time of our research and writing, Checkra1n was the newest available exploit/tool to jailbreak the devices.

4. Discussion on Findings

In this section, we present the findings that reveal to readers how much of these m-shopping app users' private information is actually being stored and discuss how it influences the application activity. Throughout this analysis, a strict log of actions was kept. In order to protect the identity of the sellers, any personal or shop information not associated with our test accounts are excluded. Although we found many listings, there was no direct interaction with other users and no items were purchased from other sellers. Overall, our findings fit into the categories of information related to the user, the interaction with the app, and related artifacts. This includes critical information such as username/login, email, geolocation, user activity, timestamps, thumbnails, and any media file.

All artifacts discussed here were recovered from the apps' packages, whose paths are given in Table 3. The iOS app packages are all found in the *\private\var\mobile\Containers\Data* and all the Android app packages are found in the *\data\data* folders in the respective file systems.

4.1. iOS Artifacts

While analyzing the iPhone X, we were able to identify information about the user to an extent from Etsy Seller, Etsy Buyer, Amazon Seller, and Amazon Buyer apps. Etsy apps store significant amount of user data in plain-text and hence we were able to obtain more user information from Etsy apps than Amazon apps. In the next sections, we will discuss the extent of user data discovered from each app. In Table 4, we have summarized whether or not we were able to recover a list of user data artifacts and provided a summary of iOS artifacts related to Etsy and Amazon apps. We have also specified whether a certain category of information (such as the user's name, email id, user's location details user's shopping activity, and overall app usage) was recoverable or not.

4.1.1. Etsy Buyer & Seller Apps We were able to recover the user's login information and preferences. Specifically, we recovered the user's email, action log, purchased items, shop profiles, and similar items. Information about the user's application activity can be found in the path mentioned in Table 3. The app package folder path showing the unique GUID contains information on when the user accessed the online shop, viewed a listing, timestamp, user ID, and search terms used.

The information shown in Fig. 4 is a gallery of thumbnails stored within the user's device as a result of product searches in the Etsy app. This data can be recovered from the *\Library\Caches\com.etsy.etsyforios\EtsyURLCache\fsCachedData* folder and visualized using the Artifacts View option within Magnet Axiom Examine. However, while reviewing these thumbnails, a few unrelated thumbnails were discovered (e.g., images 403 and 430). They contained NSFW images based on product search terms that we used to find legitimate items.

Table 3. Android and iOS package paths for forensically relevant data for the buyer/seller apps.

Application	Android Package Path	iOS Package Path
Etsy Buyer	\data\data\com.etsy.android	\private\var\mobile\Containers\Data\Application\68604CA6-82C7-457E-97B5-17FEF3433122
Etsy Seller	\data\data\com.etsy.android.soe	\private\var\mobile\Containers\Data\Application\6D4A731E-F792-4BAB-AD3F-E6EFC1C31CB9
Amazon Buyer	\data\data\com.amazon.mShop.android.shopping	\private\var\mobile\Containers\Data\Application\B8D54083-A0BF-47F5-BED0-C23F61B7509E
Amazon Seller	\data\data\com.amazon.sellermobile.android	\private\var\mobile\Containers\Data\Application\37EECDD7-33CC-493F-A4F9-7BF1BDD0D068

Table 4. Summary of recovered iOS artifacts.

Artifact	Etsy Buyer	Etsy Seller	Amazon Buyer	Amazon Seller
User's Name	Yes	Yes	No	No
User's Email	Yes	Yes	No	No
User's Location	No	Yes	Yes	No
Shopping Activity	Yes	Yes	Yes	Yes*
Location (EXIF)	No	Yes	No	No
App Usage	Yes	Yes	Yes*	No

The use of such illicit images and listings is against Etsy's Seller policies and guidelines. However, unless a user explicitly reports such listing(s) to Etsy, they are not removed. Note that pictures with significant levels of skin exposure and those containing identifiable information are blurred for publication purposes.

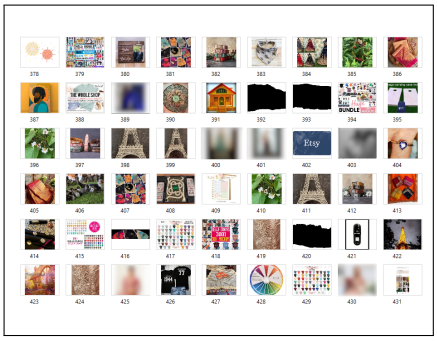


Figure 4. A screenshot of thumbnails obtained from the Etsy Buyer app.

listing_id	state	title	price	quantity	tags
1002633978	sold_out	Photograph Greeting Card for your Loved Ones	50	0	for any occasion,Nature photo card,photo greeting
1016600141	sold_out	Photograph Greeting Card for the Spring Season	50	0	Nature Greeting Card,Flower Card,Seasonal Card,E
1016603855	sold_out	Seasonal Greeting Card	50	0	photo greeting card,white flower,Blank Card,Flower
1016605321	sold_out	Seasonal Greeting Card for Friends and Family	50	0	all occasion card,flower greeting card,photo blank c
1016607559	sold_out	Fresh Photograph Greeting Card	50	0	garden note card,for any occasion,Blank Card,plan
1019562248	sold_out	Photograph Greeting Card for All Occasions	50	0	Flower photo,photo blank card,photo greeting card
1019567714	active	Photograph Greeting Card for Friends and Family	50	1	brass piece,Seasonal Card,Card for mother,photo b
1019569304	active	Seasonal Greeting Card	50	1	Eiffel tower card,Seasonal Card,for any occasion,pl

Figure 5. Reduced screenshot (Part-1) of shop_listings.csv file retrieved from Magnet Axiom.

Other images found are item listings by sellers, product thumbnails, screenshots, and user profile images. These artifacts were recovered from *\Documents\EtsyUserAccounts*. We identified that these artifacts were automatically saved within the app after the user performed some actions on the app. In total, approximately 628 images were recovered as a result of our app interactions during the study.

With respect to the Etsy Seller app, we were able to recover the seller's inventory specific information and listings. The inventory specific details were found in the *shop_listings.csv* file within the Etsy Seller app folder. The screenshot of the shop_listings file content is shown in Fig. 5 and Fig. 6 in detail.

4.1.2. Amazon Buyer & Seller Apps In our analysis, we have retrieved a large portion of the artifacts related to Amazon seller activities from the device's browsing history. And few artifacts were recovered from the *\Library\Caches\com.amazon.AmazonSeller\Cache.db-wal* folder. (The '-wal' file stands for write-ahead logging, a technique where changes are first recorded in the log, to ensure data integrity, before the changes are written to the database.)

Regarding the Amazon Buyer application, we were able to recover the search query terms used by the user from a JSON file called *\Library\Caches\com.amazon.Amazon\fsCachedData\9B687323-19F5-4F77-81CE-8B3ECE888C68.json*. Although this file does not record associated timestamps of when searches were performed, we were able to determine that the last **PAST_SEARCHES** entry in this file corresponds to the first search query performed. The *\fsCachedData* folder also contains a few *.jpg* picture files, a couple of which correspond to items purchased using the Buyer app on the iPhone.

The Amazon Buyer app also stores full, rendered *.html* web pages of various app screens that the user viewed. These web pages were recovered from within the *\Library\Caches\WebKit\NetworkCache\Version 16\Blobs* folder. Some of these web pages correspond to product pages of items the user viewed, the user's private shopping list, and the Amazon home screen. This *Blobs* folder may be worthwhile during a forensic investigation as pertinent data may be visible in it, such as the delivery address and store name.

The *\Version 16\Records\70FF5EF18B43057C8B5157B41BDA19DE47991096\Resource* folder holds various files of HTTP requests, rendered *.html* web pages, and *.jpg* and *.png* pictures, some of which correspond to items the user purchased. The user's browsing history screen was recovered from within this folder.

One of the recovered files from this folder was that of the Android seller's store page which included the business name and full address. Another of these web pages shows the order confirmation page that was shown to the user after purchasing three of the item listings. We were able to recover the street shipping address and view the images of the items that the user purchased. The orders placed by iOS buyers were

creation_tsz	last_modified_tsz	ending_tsz	image_url	currer	url
1620653132	1621447315	1631280332	https://i.etsystatic.com/7121450/r/il/6c1e99/3072411994/il_fullxfull.3072411994_e7jx.jpg	USD	https://www.etsy.com/listing/1002633978/photo
1620653204	1622124872	1631280404	https://i.etsystatic.com/7121450/r/il/b4d635/3058365000/il_fullxfull.3058365000_edxx.jpg	USD	https://www.etsy.com/listing/1016600141/photo
1620653182	1622124872	1631280382	https://i.etsystatic.com/7121450/r/il/947605/3120129845/il_fullxfull.3120129845_g8e4.jpg	USD	https://www.etsy.com/listing/1016603855/seaso
1620653161	1621447315	1631280361	https://i.etsystatic.com/7121450/r/il/14e1af/3120145547/il_fullxfull.3120145547_obz0.jpg	USD	https://www.etsy.com/listing/1016605321/seaso
1620653105	1622124872	1631280305	https://i.etsystatic.com/7121450/r/il/33f1f8/3120150699/il_fullxfull.3120150699_bjou.jpg	USD	https://www.etsy.com/listing/1016607559/fresh-

Figure 6. Reduced screenshot (Part-2) of shop_listings.csv file retrieved from Magnet Axiom.

recoverable from the order confirmation web pages from the *Resource* folder. The HTML files have a naming format of: <**UNIQUE_STRING**>**-blob**. Moreover, the *Library**Preferences**com.amazon.Amazon.plist* file is a property list file with configuration information.

In addition to the order confirmation pages shown to the user after placing an order, we were also able to recover the order details web page, which includes the following: (1) Order Details: Order date, Order number, and Order total. (2) Shipping Details: Delivery status, Items in the order, Full shipping address. (3) Payment Details: The last four digits and the type of payment card used, Full billing address.

A limited number of records of user searches, orders (with Amazon Standard Identification Number (ASIN) numbers), and default shipping address (city and zip code) were also recovered from the *Library**Caches**com.amazon.Amazon**SSNAP**SNP FileStore**Cache.db* database via the Artifacts View. Additionally, live URL links to the product pages of the items purchased by the user were carved from the *Cache.db-wal* file and displayed via the Artifacts View.

4.2. Android Artifacts

We were able to recover varying degrees of artifacts from the four apps on Android. The Etsy Seller provided the most amount of relevant artifacts, while the Amazon Seller app stored the least amount of relevant data. A visual summary of the Android findings is provided in Table 5.

Table 5. Summary of recovered android artifacts.

Artifact	Etsy Buyer	Etsy Seller	Amazon Buyer	Amazon Seller
User's Name	Yes	Yes	Yes	Yes
User's Email	Yes	Yes	No	No
User's Location	No	Yes	No	No
Shopping Activity	Yes*	Yes	Yes*	Yes*
Location (EXIF)	No	Yes	No	No
App Usage	Yes	Yes	Yes*	No

4.2.1. Etsy Buyer App All artifacts discussed here are recovered from the Etsy buyer app folder. The user profile information was recovered from the *shared_prefs**EtsyUserPrefs.xml* file and includes a URL link to the user profile picture, the user's full name, username, login name, email address and Etsy user ID. It is reassuring that the Etsy buyer app does not save the user's location in this file even though it has permission to use location services on the device.

It is possible to determine which user last signed in to the app by viewing the *shared_prefs**com.appboy.offline.storagemap.xml* file to get the userID for the user who last signed in and then using the *EtsyUserPrefs.xml* file to get the user's full name. The pictures of the items our seller account posted were also recovered from the *cache**image_manager_disk_cache* folder, however, there were no EXIF data available for the images.

The *databases**analytics_logs.db-wal* file holds a record of how the user used the app and provides information on when the user viewed the home screen of the Etsy app, viewed shop recommendations, and when the app became active or entered the background state, among others. Similarly, the user's app usage actions relating to which listings and stores the user viewed can also be recovered from the *databases**userActions-wal* file. Logs related to when the app was used, when the app entered a background state, the associated user ID of the person who generated the event log, and the event name were recovered in our analysis.

The timestamp and the last searched term can be partially recovered from the *searchImpressions* table within the *databases**searchImpressionsDB* database. This artifact is partially recovered when we searched using a long search string (*Photography Greeting Card for Friends and Family*).

As shown and discussed in Fig. 4, a few images with higher levels of skin exposure were found among some of the results displayed on the user's screen from various Etsy shop listings based on innocent search terms. For example, search terms such as *jewelry*, *gifts for step daughter*, *gifts for little girls* are some of them to mention. Individually analyzing these image artifacts using Magnet Axiom, we identified that the access date of a particular thumbnail in the list (image 403 in Fig. 4) was related to a product search and it was one of the automatically populated recommended item lists.

4.2.2. Etsy Seller App The pictures associated with the listings posted via both the Android Etsy seller account and the iOS Etsy seller account were recovered through URL links in multiple files within the *cache**volleycache-1935510846* folder. These pictures contained minimal EXIF data (only size,

dimensions, and skin tone percentage). However, the pictures in *.jpg* format associated with listings posted by the Android seller account were recovered from the *\com.etsy.android.soe\files* folder. These pictures were easily viewed using the Thumbnail view available from the Artifacts category in Magnet Examine. Each file was named according to the Epoch timestamp of when the listing was created. For example, one of the recovered pictures was named **1623255211073-3.jpg** which is a picture uploaded for one of our listings posted on Wednesday, 09 June 2021 12:13:31. These pictures contained much more EXIF data, including GPS coordinates, timestamps, and details about the camera used. The seller's account details including their first name, location (city and country), username, login name, email, userID, and their store's name were recovered from the *\shared_prefs\23449143_EtsyUserPrefs.xml* file. The *\databases* folder contained several databases of relevance. All databases and WAL files discussed here are recovered from this folder.

The app stores plain-text messages exchanged between the seller and other users. However, the *ConvoDB* database file was empty in our forensic image. However, we did recover the table schemas that were used to populate the *ConvoDB* database from the *ConvoDB-wal* file. Details such as **userId**, **OtherUserId**, **title**, and **lastMessage**, along with the *convo_drafts* table holding the **message** and **userName** are part of this database.

The seller's listing activity can be recovered from multiple databases and the corresponding WAL files. The *analytics_logs.db-wal* file holds logs of various activities the user performed on the app, including when the user edited a listing or a listing's title, when the app went into the background state or became active, along with a user ID, the model of the device used, and a timestamp of when the app was first opened. A log file containing the seller's actions of editing the listings was also recovered. However, this log does not indicate exactly what was changed.

Another important database is the *soe_data* database. All the tables discussed here are recovered from this database. The tables *listing* and *shop_managed_listings* record the listings the user has posted, including **listing_id**, **title**, **price** and **image_url** in the picture associated with the listing. Similar information about the pictures used for the listings can be recovered from the *images* table. The table *edit_listing_table* provides details about the various listings the seller edited; however, we were unable to determine when and what exactly was altered, as the log does not record an associated timestamp and original value.

A record of how other users interacted with the seller's listings and the shop can be recovered from the *activity* table. This information includes the first name of other users, user ID, a URL link to their profile picture, the action the other user performed (e.g., favorited an item, purchased an item, left feedback), a receipt ID when an item was purchased, the item ID, and the listing ID when an item was favorited. The logs generated when the Etsy Buyer account interacted with our Android seller account, are shown in Fig. 7.

The table *receipt* contains information about all the sales that the seller made. The **receipt_id** can be used to cross reference the buyer's name from the table *activity*. The table *feedback* stores the feedback (comments) other users left about the seller's store along with the rating. However, no userId nor timestamp was recorded and thus to determine who left the comment and when, we had to use the **feedback_transaction_id** in this table with the **feedback_transaction_id** column in the *activity* table.

The **shop_id** and **title** (name) of the Etsy shop and the **user_id** of the shop owner can be recovered from the *shop* table. The usage information can also be recovered from various files within the *\shared_prefs* folder. The last time the app synced was recovered from the *account-info-[userID].xml* file. The access token can be recovered from the *[userID]_EtsyPrefs.xml* file. Finally, the currently logged in userID can be recovered from the *account-info-general-prefs-account.xml* file.

4.2.3. Amazon Buyer The *accounts* table in the *\databases\map_data_storage.db* database holds details about the accounts used with the app, including the user's user ID, display name, the timestamp of when the account was created, and whether the account was deleted or contains old data. The table *userdata* in the same database stores additional details about the user's account, including first name, username, account ID, name attached to the Android device, and multiple authentication tokens. Each row in this table is also labeled according to whether the data have been deleted or are dirty (i.e., not the most recent value that was set). Figure 8 is a snippet of the data recovered from the *userdata* table, as viewed by the DB Browser for SQLite software. The *\shared_prefs\DataStore.xml* file also holds user data, including the user's full name and **accountID**. This file has a tag **userDob** and **userEmail**, but these fields are empty.

The user's browsing and shopping activity can be recovered from URL links within multiple files in the *\cache\WebView\Default\HTTP Cache* folder. This folder also includes URL links to multiple listing pages on Amazon that the user visited. The *\shared_prefs\account_change_observer.xml* file shows

_id	listing_id	receipt_id	item_id	type	creation_time	source_user_id	source_name	source_image	source_sentence
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
485	NULL	2079659222	177389353320	ItemPurchased	1623266157000	484957629	Rea	https://www.etsy.com/images/avatars/...	purchased 3 of your items.
486	1019569304	NULL	177389071850	Listing	1623265454000	484957629	Rea	https://www.etsy.com/images/avatars/...	favorited your item.
487	NULL	2084285327	181274027415	ItemPurchased	1623261061000	489538770	Rea	https://www.etsy.com/images/avatars/...	purchased 2 of your items.
488	1019562248	NULL	177387194852	Listing	1623260648000	489538770	Rea	https://www.etsy.com/images/avatars/...	favorited your item.
489	NULL	2071782775	180909681199	ItemPurchased	1622124889000	489538770	Rea	https://www.etsy.com/images/avatars/...	purchased 3 of your items.
490	1016600141	NULL	177022816712	Listing	1622124098000	489538770	Rea	https://www.etsy.com/images/avatars/...	favorited your item.
491	NULL	2063765127	176802704230	ItemPurchased	1621447335000	484957629	Rea	https://www.etsy.com/images/avatars/...	purchased 2 of your items.

Figure 7. Reduced activity logs generated when the iOS Etsy Buyer interacted with the Android Etsy Seller.

_id	userdata_account_id	userdata_key	userdata_value	userdata_timestamp	userdata_deleted	userdata_dirty
Fil...	Filter	Filter	Filter	Filter	Filter	Filter
7	amzn1.account.AGDJ...	com.amazon.dcp.sso.token.devicedevi...	rh1vKvxd70aCPL9EF4m3xQ...	1621961711835	0	0
8	amzn1.account.AGDJ...	force_refresh_dms_to_oauth_done_on...	true	1621961711835	0	0
9	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.username	Reas urch	1621961711835	0	0
10	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.account...	ATVPDKIKX0DER	1621961711835	0	0
11	amzn1.account.AGDJ...	com.amazon.identity.cookies.xfsn	+w8NAHAmRpPPaIFI0CAUo...	1621961711835	0	0
12	amzn1.account.AGDJ...	com.amazon.dcp.sso.token.device.priv...	dpkrsqOhsZdStZLm7AhlZMO...	1621961711835	0	0
13	amzn1.account.AGDJ...	key_panda_marketplace_header	api.amazon.com	1621961711835	0	0
14	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.account...	c85f06a3-af22-4533-...	1621961711835	0	0
15	amzn1.account.AGDJ...	com.amazon.dcp.sso.token.cookie.xma...	+EgfcEp7xCPJ5gVZT/qc6w=...	1621961711835	0	0
16	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.account...	US	1621961711835	0	0
17	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.account...	NA	1621961711835	0	0
18	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.devicen...	Reas's Android Device	1621961711835	0	0
19	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.session...	true	1621961711835	0	0
20	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.account...	amzn1.account.AGDJIEYNM...	1621961711835	0	0
21	amzn1.account.AGDJ...	com.amazon.dcp.sso.token.device.acc...	40M8VyQOpZsHLfzftZjg==...	1621961711835	0	0
22	amzn1.account.AGDJ...	com.amazon.dcp.sso.property.firstname	Reas	1621961711835	0	0
23	amzn1.account.AGDJ...	isAnonymous	false	1621961711835	0	0

Figure 8. Profile details for the Android, Amazon Buyer account, as viewed on DB Browser for SQLite.

the account ID of last account signed into the app, while the last time the app was started can be determined from the *\shared_prefs\MobileGrowthMetricsDataStore.xml* file.

4.2.4. Amazon Seller App We recovered details about the currently signed in account (account ID and user's display name) from the *accounts* table in the *\databases\map_data_storage_v2.db* database. Additionally, the account ID of the last account that was signed in can be found in the *\shared_prefs\account_change_observer.xml* file. Identifiers about the shop, such as **MARKETPLACE_ID** and **MERCHANT_ID**, can be recovered from the *\shared_prefs\com.amazon.sellermobile.android.USER_PREFERENCES.xml* file.

As Amazon requires sellers to upload their handmade item listings via a Web browser, details regarding this activity can be recovered from the *\data\data\com.android.chrome\app_chrome\Default\History* folder and easily viewed using the Artifacts View on Examine (see Fig. 9). The *.mhtml* webpage for Amazon Seller Central was also recovered, which shows information about the seller's listings. This webpage was recovered from *\data\data\com.android.chrome\cache\Offline Pages\archives\e6ffaee8-d84e-4f16-9071-5b416cda6 2 c0.mhtml*. The pictures used for the listings the seller posted were recovered from within the *\cache\volley* folder that holds multiple files containing URL links to the pictures. These links seem to be still active even after about four months since the data population.

Item	Type	Artifact category	Date and time
https://www.google.com/search?q=amazon&oq=amazon&aqs=chrome..69i...	Chrome Web Visits	Web Related	16/06/2021 8:27:18 AM
https://www.google.com/search?q=amazon+seller+central+login&client=m...	Chrome Web Visits	Web Related	16/06/2021 8:27:18 AM
https://na.account.amazon.com/ap/sso/return?pushSsoState=eyJ6aXAiOiJER...	Chrome Web Visits	Web Related	16/06/2021 8:28:06 AM
https://sellercentral.amazon.com/home?	Chrome Web Visits	Web Related	16/06/2021 8:28:06 AM
https://sellercentral.amazon.com/productsearch/ref=xx_addlisting_dnav_xx	Chrome Web Visits	Web Related	16/06/2021 8:29:42 AM
https://sellercentral.amazon.com/productclassify/handmade	Chrome Web Visits	Web Related	16/06/2021 8:29:42 AM
https://sellercentral.amazon.com/productsearch/ref=xx_addlisting_dnav_xx	Chrome Web Visits	Web Related	16/06/2021 8:30:00 AM
https://sellercentral.amazon.com/productclassify/handmade	Chrome Web Visits	Web Related	16/06/2021 8:30:00 AM
https://sellercentral.amazon.com/home?	Chrome Web Visits	Web Related	16/06/2021 8:30:07 AM
https://sellercentral.amazon.com/productsearch/ref=xx_addlisting_dnav_xx	Chrome Web Visits	Web Related	16/06/2021 8:30:14 AM
https://sellercentral.amazon.com/productclassify/handmade	Chrome Web Visits	Web Related	16/06/2021 8:30:14 AM
https://sellercentral.amazon.com/productsearch/ref=xx_addlisting_dnav_xx	Chrome Web Visits	Web Related	16/06/2021 8:30:29 AM

Figure 9. A snippet of the Android, Amazon Seller's browsing history that is generated when uploading and managing their listings.

The *WorkSpec* table in the *\databases\androidx.work.workdb* database, as well as the corresponding WAL file, contains records of the notifications the app showed the seller pertaining to order status. Some of the notification about the delivery status were also recoverable.

4.3. Key Findings

Many online shoppers rely on businesses to maintain the privacy and security of shopper's information on e-commerce platforms - both in the marketplace's server and in mobile applications used for shopping. The privacy measures of the shopping apps are not all equal; our findings show evidence of user data that is stored/cached in the mobile commerce apps. In spite of the fact that Amazon made an attempt to not store the user's data and usage, our findings show that Etsy app does store a significant amount of user data.

We observed that Etsy's default settings are not privacy-preserving. For instance, when a user follows a shop or adds a shop to their favorite list, the default settings allow any user who is viewing the shop to trace the activities of buyers who follow the shop. All favorite items of a buyer can be viewed publicly by anyone. The user needs to make modifications to the settings of their account in order to keep their favorite listings 'private'. Furthermore, it can be worrisome for the vast majority of frequent online shoppers, depending on the app they

use, as their user information or app usage behavior may be easily accessible or traced by any user browsing items from the online shop.

User's search history, detailed app usage, and approximate location were found on the Etsy Buyer app. Our findings illustrate the severity and lack of privacy measures to safeguard online shopper user information. We could recover the device owner's profile information entered, app usage statistics, and even information about other users. This information can include profile pictures along with their listed items and the location attached to the picture. This demonstrates the need for strong privacy-preserving mobile commerce application deployment.

The authors would also like to mention about the thorough verification process involved in the approval of a seller to become eligible to sell products on the Amazon platform. The Amazon seller registration process involves a video call interview, an identity verification process, and heavy documentation. This should make the process of identifying and tracking down illegitimate sellers for Amazon. In contrast, the seller registration process on the Etsy platform was simple. On Etsy, anyone with valid payment details was allowed to register, list, and sell their items.

While reviewing Amazon's privacy policy, it goes in depth in reference to what information is stored i.e. "URL click-stream, whether it is to or from their site, content downloads", and "device metrics" just to name a few (Amazon, 2021). Although the corporation seems to be upfront regarding what information is accessed and stored, there have been some lawsuits in reference to Amazon violating privacy regulations. Most recently, Amazon has been noted for its processing of personal data that did not comply with the EU General Data Protection Regulation (GDPR) which resulted in a $ 887 million fine[2,3]. Some EU regulators/lawmakers have raised concerns that the company has used what it knows to give itself an unfair advantage in the marketplace. Cases like this call for the evolution of the concepts of privacy, law and regulations and the need for bringing lawyers and technologists together.

4.4. Implications for Research and Practice

This research contributes to the academic literature by conducting an extensive forensic analysis of the most popular mobile shopping apps. Our findings indicate that the recovered artifacts and the product listings of the m-shopping apps contain a significant amount of user data residue. Also, the discovery of certain thumbnails and product listings with unsafe skin exposure levels in response to innocent product search terms without intentional access raises concerns about the lack of online safety measures by m-shopping apps. Stricter policies and standards are required to prevent abusive content from entering public marketplace listings. Behavioral researchers can further explore factors affecting mobile shopping experience and users' perspective of privacy on web shopping platforms in behavioral research.

On the other hand, privacy laws in several parts of the world have set forth requirements for collecting or using personal data, including the European Union's General Data Protection Regulation (GDPR), California Online Privacy Protection Act (CalOPPA), Japan's Act on the Protection of Personal Information, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), etc. The App Store and the Play Store have privacy policy requirements that one must comply with if they are listing their apps. As consumers, over time, use several of these mobile shopping apps, we recommend that whenever a user is ready to download apps from the App Store or Play Store, they must read the Privacy Policy listed through the link available in the information section of the app. Moreover, app developers must list details about the data collected from the app user and the data retained in the app.

Developers must also take measures to implement secure coding practices, such as purging old logs generated by the app. The lack of encryption for user data, including user information, geo-location data, and most timeline activities of buyers, also poses a concern about consumer data privacy. Offering privacy-preserving default settings and data storage encryption in m-shopping apps will improve the user's security and contribute to building trust between consumers and companies, which will benefit both.

5. Conclusion

Regardless of the type of mobile device used, user privacy and information security have always been a concern for mobile application users. In this paper, we performed a user data analysis of two popular mobile shopping apps, Amazon and Etsy. We evaluated these apps' user data privacy concerns on Android and iOS mobile devices. Furthermore, we also compared our findings among the apps investigated, considering the buyer and seller roles.

[2]https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html

[3]https://www.bbc.com/news/business-58024116

References

Abdulla Al-Delayel, S. (2022). Security analysis of mobile banking application in qatar. *arXiv e-prints*, arXiv–2202.

Amazon. (2021). Amazon privacy policy [(Accessed on 06/12/2022)].

Bojjagani, S., & Sastry, V. (2016). Stamba: Security testing for android mobile banking apps. In *Advances in signal processing and intelligent recognition systems* (pp. 671–683). Springer.

Cellebrite. (2021). Checkm8 and checkra1n – full file system extractions for ios devices [(Accessed on 11/23/2021)].

Chanajitt, R., Viriyasitavat, W., & Choo, K.-K. R. (2018). Forensic analysis and security assessment of android m-banking apps. *Australian Journal of Forensic Sciences*, *50*(1), 3–19.

CyberChef. (2021). Cyberchef [(Accessed on 10/21/2021)].

Datta, P., Tanwar, S., Panda, S. N., & Rana, A. (2020). Security and issues of m-banking: A technical report. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 1115–1118.

Hutchinson, S., Shantaram, N., & Karabiyik, U. (2020). Forensic analysis of dating applications on android and ios devices. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 836–847.

Johnson, H., Volk, K., Serafin, R., Grajeda, C., & Baggili, I. (2022). Alt-tech social forensics: Forensic analysis of alternative social networking applications. *Forensic Science International: Digital Investigation*, *42*, 301406.

Kulkarni, S., Kumari, K., & Kittur, N. (2013). Privacy and security issues in mobile social networking and in modern shopping experience. *International Journal of Computers & Technology*, *5*(1), 69–73.

NCOSE. (2021a). Amazon - major contributor to sexual exploitation [(Accessed on 06/12/2022)].

NCOSE. (2021b). National center on sexual exploitation [(Accessed on 06/12/2022)].

NCOSE. (2022a). Encourage etsy to stop selling sexual exploitation [(Accessed on 06/12/2022)].

NCOSE. (2022b). National center on sexual exploitation dirty dozen list 2021 [(Accessed on 06/12/2022)].

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, *33*, 200908.

NIST. (2017). Information technology laboratory, nist software quality group [(Accessed on 02/03/2022)].

Osho, O., Mohammed, U. L., Nimzing, N. N., Uduimoh, A. A., & Misra, S. (2019). Forensic analysis of mobile banking apps. *International Conference on Computational Science and Its Applications*, 613–626.

Pasha, S., & Saleem, S. (2019). Forensics analysis of wish-shopping made fun application on android. *2019 International Conference on Frontiers of Information Technology (FIT)*, 144–1445.

Rick Ayers, S. B., & Jansen, W. (2014). Nist special publication 800-101 revision 1 [(Accessed on 02/10/2022)].

Salamh, F. E., Mirza, M. M., Hutchinson, S., Yoon, Y. H., & Karabiyik, U. (2021). What's on the horizon? an in-depth forensic analysis of android and ios applications. *IEEE Access*, *9*, 99421–99454.

Shimmi, S. S., Dorai, G., Karabiyik, U., & Aggarwal, S. (2020). Analysis of ios sqlite schema evolution for updating forensic data extraction tools. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–7.

Statcounter. (2021). Mobile android version market share worldwide [(Accessed on 11/23/2021)].

Statista. (2019a). Number of amazon prime members in the united states as of december 2019 (in millions) [(Accessed on 03/01/2022)].

Statista. (2019b). Share of online consumers in the united states who are amazon prime members in 2019, by generation [(Accessed on 03/11/2022)].

Statista. (2021a). Leading shopping apps in the google play store in the united states in july 2021, by number of downloads [(Accessed on 10/21/2021)].

Statista. (2021b). Most popular online marketplaces according to online sellers in the united states as of january 2021 [(Accessed on 02/15/2022)].

Statista. (2021c). Number of active etsy buyers from 2012 to 2020 [(Accessed on 02/01/2022)].

Statista. (2021d). Number of active etsy sellers from 2012 to 2020 [(Accessed on 01/10/2022)].

Zimperium. (2019). Privacy and security issues found in shopping apps — app scan [(Accessed on 11/22/2021)].