Try on, Spied on?: Privacy Analysis of Virtual Try-On Websites and Android Apps

Abdelrahman Ragab, Mohammad Mannan, and Amr Youssef

Concordia University, Montreal, Canada
{abdelrahman.ragab, m.mannan, amr.youssef}@concordia.ca

Abstract. The use of augmented reality (AR) technology for virtual try-on (VTO) in online shopping is on the rise but its current state of privacy is not well explored. To examine privacy issues in VTO websites and apps, we analyze 138 websites and 28 Android apps that offer VTO. By capturing and analyzing the network traffic, we found that 65% of the websites send user images to a server: 8% to first-party (FP) servers only, and 57% to third-party (TP) servers only or both FP and TP. 18% of apps send user images to a server: 4% to FP servers only, and 14% to TP servers only or both FP and TP. Additionally, 43 websites and 2 apps are confirmed to get the users' images stored, either by the FP website or a TP. 37% of websites are confirmed to use VTO providers which extract facial geometry from received users' images. We also found that 11% of websites featuring VTO violate their own privacy policies, and 25% use a VTO provider that violates its own privacy policy. Privacy policy violations include sharing the user's image to a website's own server, or to a TP server, despite denying so in the privacy policy. Furthermore, 22% of websites use disclaimers that mislead users about what happens to their data when using VTO. We also found 1446 and 931 TP tracking scripts and cookies, respectively, in the analyzed websites. Finally, we identified security vulnerabilities, such as broken authentication, in a VTO provider that can compromise its merchants. These findings underscore the need for greater transparency and clarity from companies using VTO features, and highlight the potential risks to user privacy, even from top brands.

Keywords: virtual try-on · VTO · augmented reality · privacy · security.

1 INTRODUCTION

According to market research firm `Technavio.com`, the virtual reality (VR), augmented reality (AR), and mixed reality markets are set to grow by US$162.71 billion, between 2021 and 2025 [24]. These technologies enhance the online shopping experience by allowing customers to interact with the product virtually, e.g., to virtually try on clothes [26], visualize products in their own space, and interact with products in a more immersive and realistic way. In June 2020, a survey of U.S. retailers revealed that 20% planned to invest in AR or VR for their online stores, up from 8% six months earlier [3]. AR shopping via VTO can also provide benefits for retailers, including increased sales, reduced costs, and improved customer engagement. VTO on websites/apps is very accessible as it does not require expensive headsets; just a web/phone camera. While the popularity of this technology continues to grow, we know little about the current state of privacy and security of such solutions. Feng et al. [6] examined consumers' responses to VTO apps. The results of their study demonstrate that when users have high levels of privacy concerns, they tend to show higher levels of perceived intrusiveness and more negative attitudes towards the app when viewing themselves trying a product using VTO than when viewing professional in-app models wearing the product. This perceived intrusiveness is justified considering that personal data such as user's facial images, body images, or room images become the subject of interest (we refer to any of those types of images as user's image in this study). If these users' images fall into the wrong hands, e.g., by means of leakage, selling, or otherwise, they can be used in nefarious ways such as in fake or depictive videos/images, especially with the advancement of deepfake technologies. Biometric data such as face geometry, which can be obtained from facial images, is particularly used in facial recognition to identify individuals [10]. Additionally, face geometry can be used to extract other information such as age, gender, and health attributes of the individual [14].

Furthermore, it is not well established whether VTO websites and apps are in line with their privacy policies, or if they receive users' images on their servers, process them, or share them with third parties. Previous work such as [23] investigated security and privacy aspects of AR applications and their supporting technologies. They identified some issues, such as the possibility of deception attacks, overload attacks, access control for sensor data, and bystander privacy. Other work [19] investigated authentication mechanisms for AR/VR devices.

In this work, we present a framework (see overview in Fig. 1) for measuring the privacy of websites and Android apps featuring VTO, as well as testing the security of VTO service providers. We analyze 138 websites and 28 Android apps featuring VTO, and we analyze 3 VTO service providers. For the websites featuring VTO, we check if users' images or videos are shared while using the VTO feature, and we check if the observed behavior is in line with the website's privacy policy. In addition to addressing the privacy aspect of the VTO feature, we quantify and classify the third-party cookies and scripts present on each website using an extension that we created and released[1] for the web privacy measurement framework, OpenWPM [5]. We do the same for the apps, but instead of the quantification and classification of cookies and scripts, we check for the presence of tracking libraries. We also test the VTO service providers for security issues such as broken authentication, unauthorized access, and Cross-Site Request Forgery (CSRF). We also check if there are any misconfigurations which can leak users' data.

[1] https://github.com/virtualtryon2023/openwpm-cookies-and-scripts-extension

Contributions and notable findings.

1. We develop a framework to evaluate the privacy of VTO websites and apps (including top brands), and to test the security of VTO service providers.
2. 90 out of 138 (65%) of the tested websites send the user's image to a server when using the VTO feature, and 79 out of 90 particularly to TP servers including VTO providers, analytics services, and session replay services. For 43 out of 138 (31%) of the websites, the user's image is stored during the VTO. 10 user images are still accessible, with 3 of them still accessible over 2 months after testing. 15 out of 90 (17%) of websites - that send the user's image to a server - violate their own privacy policy and 35 out of 90 (39%) use a VTO service provider that violates its own privacy policy.
3. 6 out of 90 (7%) of websites that send the user's image to a server showed a misleading and false disclaimer that denies the processing, storage or collection of the user's image, or claims that the user's image is not shared and remains on the local device, despite the reality being the opposite. For example, `Prada.com` states"Your Image will not be communicated to PRADA or anyone else and will not be stored by Luxottica. The Image is processed live.", even though it sends the user's image to Adobe Ads.
4. 51 out of 138 (37%) of websites are confirmed to use VTO providers which extract face geometry from received users' images.
5. 1446 out of 2609 (55%) of TP scripts found in 138 websites are trackers. Popular brands such as `Elfcosmetics.com` had the largest number of TP tracking scripts: 29. 931 out of 2487 (37%) of TP cookies found in 138 websites are trackers. E.l.f Cosmetics had the largest number of TP tracking cookies: 40. 55 out of 931 (6%) of cookies are set to the year 9999, and 403 out of 931 (43%) to more than 1 year but less than 5.
6. 5 out of 28 (18%) of tested apps with an overall of 20.5+ million downloads are found to send the user's image to a server, and 4 out of 28 (14%) send it to a TP server. 2 out of 28 (7%) apps get the user's image stored on a server when using the VTO feature. 2 out of 5 of apps that send the user's image to a server violate their own privacy policy.
7. The VTO service provider `Vossle.com` is found to suffer from broken authentication and authorization, where an attacker can get personal information of all merchants using the platform, and can modify the VTO collection of a victim. On sign-up, the user's email and password are leaked to `sentry.io` session replay service.

2 RELATED WORK

Augmented and virtual reality. Liebers et al. [12] investigated the use of gaze behavior and head orientation for implicit identification in virtual reality. The personal identifiability of user tracking data during observation of VR videos has also been studied [13,18]. Trimananda et al. [25] focused on Oculus VR (OVR) and provided the first comprehensive analysis of personal data exposed by OVR apps and the platform itself, from a networking and privacy policy perspective. By comparing the data flows collected from the network traffic of 140 apps with statements made in the apps' privacy policies, they found that 68% of OVR data flows were inconsistently disclosed in the privacy policy. Furthermore, they extracted additional context from the privacy policies, and observed that 69% of the consistent data flows have purposes unrelated to the core functionality of apps (i.e., advertising, analytics, marketing, and additional features). Lebeck et al. [11] conducted a qualitative lab study with an immersive AR headset, the Microsoft HoloLens. Through semi-structured interviews, they explored participants' security, privacy, and other concerns.

Virtual try-on. To the best of our knowledge, this is the first measurement study to look into the privacy and security of websites and apps featuring VTO. Past literature focused on users' perception of VTO technology when shopping online. Feng et al. [6] studied the effect of the users' privacy concerns on their perceived intrusiveness of VTO features, and how it affects their attitude towards VTO apps. Smink et al. [22] studied the perceived informativeness and enjoyment when using VTO in online shopping. Ivanov et al. [9] examined the impact of users' privacy concerns on the intent of adoption of VTO for clothes. They found that a majority of their participants (110 out of 192) "would *ideally* use their own avatar, but choose not to due to privacy concern".

3 METHODOLOGY

3.1 Collection of VTO Providers, Websites and Apps

In this section, we outline how we collect our list of VTO service providers' websites, websites featuring VTO, and Android apps featuring VTO. By *VTO service provider's website*, we mean the website of the company providing VTO technology for other websites (clients) to use. A *website/app featuring VTO* is a website/app making use of the VTO feature that is used by end-users. In some cases, some VTO providers have a demo on their website which allows end-users to use the VTO feature. We count such cases under *websites featuring VTO* too and we analyze them as such.

VTO service providers. Despite the increasing popularity of VTO, it is still not as ubiquitous, and there are not many VTO service providers. We collect our list of VTO service providers manually using search queries (e.g,'virtual try on solution') on Google. In total, we find 18 providers. However, we test the security of 3 only because they were the only ones which offer a free trial.

Websites featuring VTO. In addition to using Google search queries, we see the list of clients on VTO service provider's websites to collect websites featuring VTO. We collect a non-exhaustive list of 138 websites which mostly either offer glasses VTO or makeup VTO. A few websites offered other VTO such as hair and fingernail VTO. We also count websites with features to evaluate skin health - by capturing a user's facial image - as websites featuring VTO.

Android apps featuring VTO. To collect Android apps featuring VTO, we query Google's Play Store with relevant keywords (e.g, try on, virtual try on, AR glasses, AR furniture). We also look into the *related apps* section on the app's page, and the list of apps by the same developer. For apps, we look beyond glasses and makeup stores. For example, we also count in apps with clothes try-on, tattoo try-on, furniture AR visualization, hair try-on, shoes try-on, and jewelry try-on. Only apps with at least 1 thousand downloads are considered. We also classify apps to be either *pure VTO* or not.

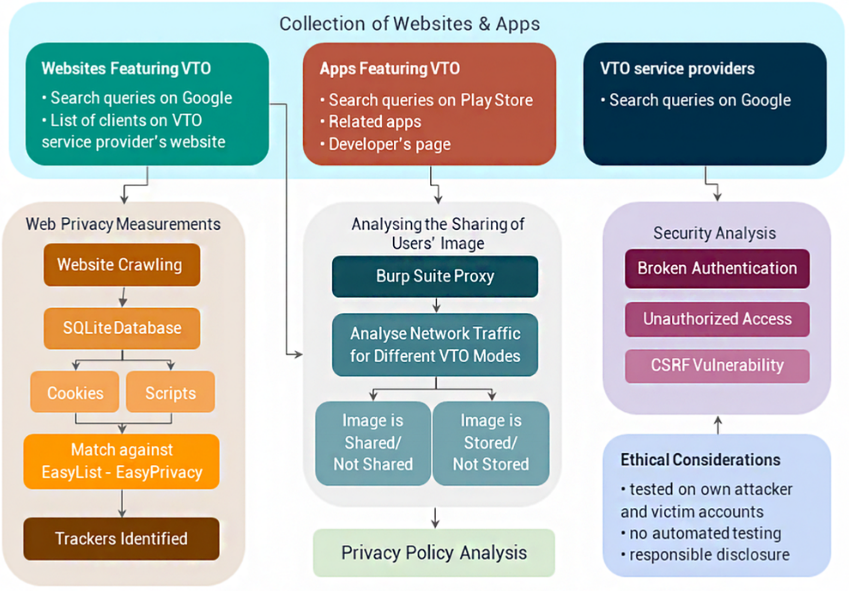

Collection of Websites & Apps
Websites Featuring VTO
• Search queries on Google
• List of clients on VTO service provider's website
Apps Featuring VTO
• Search queries on Play Store
• Related apps
• Developer's page
VTO service providers
• Search queries on Google
Web Privacy Measurements
Website Crawling
SQLite Database
Cookies
Scripts
Match against EasyList - EasyPrivacy
Trackers Identified
Analysing the Sharing of Users' Image
Burp Suite Proxy
Analyse Network Traffic for Different VTO Modes
Image is Shared/ Not Shared
Image is Stored/ Not Stored
Privacy Policy Analysis
Security Analysis
Broken Authentication
Unauthorized Access
CSRF Vulnerability
Ethical Considerations
• tested on own attacker and victim accounts
• no automated testing
• responsible disclosure

Fig. 1: Overview of analysis framework.

3.2 Analyzing the Sharing of Users' Images on VTO Websites/Apps

We identify 3 different modes through which customers can use the VTO feature. First is live mode, where as long as a user's camera is open, virtual products are placed on their face/body or in the room in real-time. The second mode is image capture, where an image is first captured, then the virtual product is applied. The third mode is image upload, where the user uploads their image from their device before applying the product. We also identify an option to the second and third modes: download/share image, where a user clicks a download/share (to Facebook, WhatsApp, etc.) image button, after applying the VTO effect. We set up a man-in-the-middle-proxy to capture and decrypt HTTP/HTTPS traffic while using the VTO feature in a website/app. For each available mode in a website/app, we capture the network traffic, then analyze the requests and responses. Throughout the experiment for websites, we did not sign-up/in to the website, as it is not required; the VTO feature is available for use without signing in.

To confirm the sending of the users' image, we analyze every request to see if the payload contains the user's image. The payloads containing images are either in JSON format or multi-part file (form-data) format. We look for the strings '*image/jpeg*' and '*image/png*' in the payload. These strings indicate the beginning of an image encoded in base64 in the case of a JSON payload, and they indicate the field for an image in the form-data payload. To verify it is indeed the user's image, in the case of an image in base64, we convert it to JPEG/PNG format respectively using online tools [15][16]. If the image is in a form-data type of payload, we just save the binary bytes to a JPEG/PNG file. If the image is found to be of the user, then it is confirmed that the user's image is sent to a server. In several cases, the entire request payload is encoded in gzip or zlib format. For gzip, we use Burp Suite's decoder module to decode the payload. In the case of zlib, we use the open source tool *zlib*[1] to decode the payload. A limitation of our method is that although it considers payloads encoded in gzip and zlib, it does not consider other cases such as where the payload is encrypted, in another encoding method, or in other device dependent formats.

We consider that a user's image has been stored in a server in two cases. The first case is when any of the captured outgoing requests (which do not contain the user's image) retrieves the user's image in the response. In the second case, we analyze responses to captured requests after the user's image has been sent to the server for the first time. If any response payload contains a link enabling the viewing or downloading of the user's image or a modified version of it, we infer that the user's image is stored on a server. We do not consider cases where the user's image is obtained from the browser's cache as storing the user's image on a server.

Test setup. For testing websites, we set up the Burp Suite proxy on a Windows 11 machine, and use Google Chrome to test the websites. For testing Android apps, we use a rooted Samsung Galaxy M02 phone running on Android 13. Communication is established between the Windows 11 machine and the phone via USB connection and ADB (Android Debug Bridge). Burp Suite proxy is used for traffic interception. We use the dynamic instrumentation toolkit Frida[7] to execute scripts to attempt bypassing SSL-pinning where needed.

3.3 Analyzing Privacy Policies w.r.t VTO Feature

Based on our observation while testing the VTO feature of websites/apps, we analyze their privacy policy to see if there is any inconsistency or violation. We classify the standing of a website/app with respect to its privacy policy into *not violated*, *vague*, *ambiguous*, or *violated*. We consider that a website has *not violated* its privacy policy if the user's image is not detected to be shared at all, or if no criterion mentioned below is matched. A website with a *vague* standing still does not violate the privacy policy, but there is no direct mention of image collection in the privacy policy. A website will be given an *ambiguous* standing if the privacy policy has contradicting terms, makes no mention of data collection at all, or if the privacy policy is inaccessible. We consider that a website has *violated* its own privacy policy if any of the following defined criteria is matched: (1) *image sharing to server*: the user's image is sent to the website's server despite the privacy policy denying it. (2) *image storing*: the user's image is stored on the website's own server, or an associated cloud storage, despite the privacy policy denying the storing of users' images. (3) *image storage duration*: the duration of storing the user's image exceeds that which is mentioned in the privacy policy. (4) *image sharing to third party*: the user's image is shared with a third-party without consent, despite the privacy policy denying it unless consent is given. (5) *image sharing to analytics services*: the privacy policy mentions the use of tracking and analytics services such as Google Analytics for automatic collection and analysis of the user's behavior and/or system settings, however, the user's image ends up being sent to that service provider. We do not consider the user's image to be normal information nor behavior to be automatically collected and sent to such third-party services.

Based on the above criteria, we also report on websites (clients) which use VTO providers that violate their own privacy policy when being used by the client websites.

3.4 Measurement of Trackers

For websites featuring VTO, we create an extension to the OpenWPM open-source framework [5] and use it to measure third-party (TP) scripts and cookies, and identify trackers. OpenWPM provides raw structured data regarding the crawls and stores it in an SQLite database. Our extension allows us to get the following information about the crawled websites: (1) the number (and details) of distinct first-party and TP cookies per website, (2) the overall number of occurrences of TP cookies across the list of websites, (3) the expiry dates statistics for every TP cookie host domain, (4) the categorization of TP cookies across websites, and (5) the categorization of TP scripts across websites.

To identify TP cookies/scripts, we check their source URL. If the source does not contain the domain name of the first-party website, we consider the cookie/script to be originating from a TP source. We further categorize TP cookies and scripts into one of three categories: *advertisers*, *trackers*, and *unknown*. To categorize advertisers and trackers, we match the source of the detected TP scripts and cookies with the EasyList and EasyPrivacy lists respectively [4], which are lists for known sources of trackers and advertisers. If the source of a cookie/script does not match any entry in the lists, it is categorized as unknown. While it is true that the presented methodology may have misclassified some FP cookies and tracking scripts as TP due to the use of a different domain name by the FP, we mitigate this to some extent by not using exact matching. Rather, we check for the presence of the original FP domain as a substring. So, misclassification may occur only in case the FP uses domain names that do not intersect.

Practically, we found through manual observation that the cookies and trackers that were classified as TP do originate from third parties like analytics, advertising, marketing, and social media companies; there was no misclassification. Also, it should be noted that *Easylist* and *Easy Privacy* lists are not exhaustive and may therefore miss proper classification of some TP scripts and cookies. For Android apps, we check for the presence of tracking libraries (i.e., analytics and session replay services).

Test setup. We run OpenWPM on an Ubuntu 22 virtual machine (connected to a home network) with 9GB RAM, 32GB HDD, AMD Ryzen 5 4600H 6-core processor (host) for our measurement on June 5, 2023. We run 1 windowed browser (as opposed to a headless browser) and enable the instrumentation for HTTP traffic, cookies, navigation, JavaScript, DNS requests and callstack. We performed stateless crawls (each new page visit uses a fresh browser profile) and enabled bot-mitigation for less bot-like behavior. The crawled data is saved to an SQLite database, which we then process using our extension. For checking tracking libraries in Android apps, we unpack the APK files using the Jadx tool[21] and inspect the libraries used in the source files. The limitation of this approach is that there might be tracking libraries which we were not able to identify due to obfuscation of their names.

3.5 Analysing VTO Service Providers

We consider several security issues for VTO service providers:

Broken authentication. We remove authentication credentials from sensitive/state changing (e.g, modifying VTO collection) requests and replay them. If the response is the same as when the requests were sent with the credentials, then the website would be considered vulnerable to broken authentication.

Unauthorized access. We sign in using two accounts: an attacker account and victim account (both belonging to us). We capture a request made by the victim account and replace the credentials with that of the attacker. If the response indicates success, and the victim's account state is changed, then we consider that there is an unauthorized access vulnerability.

CSRF vulnerability. For a website to be considered vulnerable to CSRF, (1) the server and client should not be communicating via JSON,(2) requests should not require custom headers, and (3) there should be no anti-CSRF token in the request [17]. So, for any PUT and POST request that matches the mentioned criteria, we count the request to be vulnerable to CSRF.

Ethical considerations and responsible disclosure. To not infringe other users' privacy, we create two merchant accounts for the platforms we test: one to represent the attacker and the other to represent the victim. So, whatever test that appears to be intrusive (e.g., modifying the VTO collection of another merchant or retrieving personal information of another merchant) has been done against our own victim account. We also refrain from using active scanning and automated tools when testing for security vulnerabilities. Furthermore, we disclosed the discovered issues with the affected VTO provider, Vossle, in accordance with the CERT Guide to Coordinated Vulnerability Disclosure [8].

4 RESULTS

4.1 Sharing of Users' Images on VTO Featuring Websites

Sending images to servers. For all tested websites, upon using the VTO feature, the browser requests the user's permission to use the camera. We found that 90 out of 138 (65%) of the websites send the user's images to a server when using the VTO feature. 79 of them send the user's image to a third-party server. We consider any website or service other than the website being visited to be a third party. For example, VTO service providers, analytics services and session replay services are considered third parties. The majority of the third parties - to which the user's image is sent - are VTO service providers (71 incidents), followed by Google Analytics (9 incidents). Also, there are 2 incidents where the user's image is sent in a Facebook Pixel to `Facebook.com`. We do not know the intention behind sharing users' images with analytics services. Possible reasons include: VTO websites/apps are gathering users' images through an analytics service to e.g., analyze their customer base by inferring users' demographics (e.g., age, gender, ethnicity, etc.), or to feed them into machine learning models for improved user profiling. Besides images, there was one incident where a video of the user is sent to Luxottica server while using its VTO[2] in video capture mode. We found that a user's image can be sent to a server through more than one mode per website. User images are sent to a server in each mode as follows: live mode (40 out of 90, 44%), image upload (41 out of 90, 46%), capture mode (28 out of 90, 31%), and download/share image option (27 out of 138, 30%), respectively.

Image storing. After analyzing the traffic, we were able to confirm that 43 out of 138 (31%) of the websites either store the user's image themselves or a third-party (associated with the website) stores the image. For 24 of these 43 websites, we detected 25 links (in total) - to access the user's stored image - being sent back from the server. For 10 out of 25 of the links we observed, the user's image is still accessible: 7 over three weeks and 3 over two months since testing. For 6 out of 25 of the links, they expired and accessing them would give an *access denied* error. Access being denied, however, does not necessarily mean that the image is actually deleted. For 9 out of 25 of the links, accessing them after some time gave a *not found* error, which can indicate that the image is deleted.

Session replay services. There are 4 incidents on 4 websites where users' images are sent to session replay services: `Transitions.com` sends the user's image to `Contentsquare.com`, `Bvlgari.com` to *Quantum Metric*, `Paireyewear.com` to `Datadoghq.com` and `Lenskart.com` to *Microsoft Clarity*[3] session replay services.

[2] `https://virtualmirror-xp.luxottica.com/kvbkF86bZsvnGqLmsfUdGj`

[3] `https://clarity.microsoft.com/`

Face geometry data. By inspecting the network traffic, we found that 51 websites use VTO providers (including `Fittingbox.com` and `Luna.io`, formerly *Ditto*) which process users' images and extract facial geometry from them. This was confirmed by observing the facial geometry being sent back from the VTO providers' servers to the browser.

4.2 Privacy Policy Analysis w.r.t VTO Feature on Websites

After analysing the privacy policy of the 90 websites which sent the user's image to a server, we found that 15 out of 90 (17%) violate their own privacy policy. 7 out of 15 of them violate their privacy policy on the basis of the criterion *image sharing to analytics services*, as defined in Section 3.3, where the websites share the user's images with third-party services such as Google Analytics and Contentsquare session replay service. 6 out of 15 of the violations are on the basis of the criterion *image sharing to third party.* The remaining 2 websites violate their privacy policy on the basis of the criterion *image sharing to server*, and *image storing*, respectively. 36 out of 90 (40%) have a vague standing with regards to their privacy policy. 3 websites have ambiguous standing, and the remaining 36 out of 90 (40%) do not appear to violate their privacy policy.

We found that 35 out of 90 (39%) of the websites - that send the user's image to a server - use a VTO provider which violates its own privacy policy. For example, the VTO provider *Fittingbox* states in its privacy policy "FITTINGBOX will not disclose or store your image; your image is processed live, on your device and only for the duration of the virtual try on experience.". Despite that, we found from the network traffic analysis that it does receive users' images to process them. Many top brands such as `Gunnar.com`, `Fielmann.at`, `Hansanders.nl`, and *Jins*[4] are found to be using *Fittingbox.* Out of the 35 cases where a website uses a VTO provider that violated its own privacy policy, 30 are on the basis of the criterion *image sharing to server* as defined in Section 3.3, while the remaining 5 violate the privacy policy on the basis of the criterion *image storage duration*, where the VTO provider (*Perfect Corp*) stores the user's image longer than it claimed. Perfect Corp states in its privacy policy that "If Facebook 'share' function enabled, photo is temporarily stored on Perfect server for 24 hours", however, it was still possible to access the image over 24 hours later. After expiring a while beyond the 24 hours, it would give an *access denied* error, which may not mean that it has been actually deleted. 46 out of 90 (51%) of the websites - that sent the user's image to a server - do not use VTO providers that violate their own privacy policy. 8 of the websites have a VTO provider which has a vague privacy policy, while just 1 has a VTO provider that has an ambiguous privacy policy.

An alarming observation is that 6 websites (see Table 1) show a pop-up kind of disclaimer upon using the VTO feature which tells the user that their image: will not be uploaded to a server, shared, stored, or that it will be deleted. This disclaimer is made regardless of what is actually stated in the privacy policy.

[4] `https://us.jins.com`

Despite this disclaimer, exactly the opposite occurs; the user's image gets infact sent to a server, stored, or shared with another party. Such disclaimer gives the user false confidence in the website.

We also calculated the overall readability of the privacy policies of the VTO websites which share user's images to a server. We utilized the Flesch-Kincaid Reading Ease metric [2] with readability scores *very easy*, *easy*, *fairly easy*, *standard*, *fairly difficult*, *difficult*, *and very confusing.* Out of the 87 tested privacy policies (3 websites had missing privacy policies), 23, 62 and 2 privacy policies obtained a readability score of very confusing, difficult, and fairly difficult, respectively.

Table 1: Example of tested VTO websites. *PP* in the table header means *privacy policy* and *TP* means *third-party.* A ✓means *yes.* A blank means *no.* For the privacy policy columns, a ● means *violated*, a ◑ means *ambiguous*, a ◍ means *vague* and a ○ means *not violated.* For the 'violation type' columns, the numbers denote the violations as specified by the criteria defined in Section 3.3. The mapping is as follows: (1) *image sharing to server*, (2) *image storing*, (3) *image storage duration*, (4) *image sharing to third party*, (5) *image sharing to analytics services.* A dash '-' means not applicable. The full list of tested websites is available at `https://github.com/virtualtryon2023/VTO-Privacy-Analysis`.

Website URL	**Image sent to TP**	**Image stored**	**Own PP**	**Violation type**	**VTO provider's PP**	**Violation type**	**Misleading disclaimer**
www.elfcosmetics.com	✓	✓	○	-	●	3	
virtual-cosme.net	✓		●	4	○	-	
www.aveda.ca	✓	✓	●	5	●	3	
www.madison-reed.com	✓		○	-	●	3	✓
www.punky.com	✓	✓	◍	-	●	3	
www.benefitcosmetics.com	✓		●	5	○	-	✓
vto.gunnar.com	✓		◍	-	●	1	
www.fittingbox.com			●	1	○	-	
www.transitions.com	✓		●	5	●	1	✓
virtualmirror-xp.luxottica.com		✓	●	2	○	-	
www.bulgari.com	✓		○	-	○	-	✓
www.prada.com	✓		◍	-	○	-	✓
drbishop.com	✓		●	4	●	1	
www.peepers.com	✓		●	5	●	1	
edandsarna.com	✓	✓	◍	-	◍	-	
www.alensa.ie	✓	✓	●	4	●	1	
www.lensmartonline.com	✓	✓	◍	-	◑	-	
fyidoctors.com	✓		●	4	●	1	
anrri.com	✓	✓	◑	-	◍	-	

4.3 Sharing of Users' Images on VTO Featuring Apps

We had an initial collection of 44 Android apps. 28 out of 44 were deemed to be successfully tested (see the full list of tested apps on our GitHub repository[5]). The others failed due to one of the following reasons: (i) the app does not load even after applying SSL-pinning bypass, (ii) the app not does not load due to

[5] `https://github.com/virtualtryon2023/VTO-Privacy-Analysis`

unavailability in country or phone compatibility, (iii) the VTO feature is there but does not work, (iv) could not find the button or place within the app to use the VTO feature.

For the successful 28 tests, 5 out of 28 (18%) apps with an overall of 20.5+ million downloads are found to send the user's image to a server, 4 out of 28 (14%) send the image to a third-party server, and 2 out of 28 (7%) are confirmed to store the user's image. 4 out of 5 apps send the user's image to a server in capture mode, and 1 out of 5 send the image in both capture and upload modes. The third parties with which the user's image is shared are: *LogRocket*[6] session replay service, VTO service provider *Luna* (for 2 apps), and some IP address. The image that is sent to a server with an IP address and no domain name is sent over non secure HTTP, which allows any intermediate device between the client and server to intercept and access the image[7]. *Ikea* and *Lenskart* apps are confirmed to store the user's room and personal image, respectively. For *Ikea*, it is confirmed on the basis that an image of the full room view is returned from the backend after processing and remains available afterwards to add AR furniture. Concerning room images, machine learning techniques can now be used for object detection, which can be leveraged to infer information such as the presence of kids (if toys are detected), habits or hobbies (e.g., due to the presence of musical instruments), financial status (if expensive objects or electronics are detected), etc. This data can be used in customer base segmentation. For *Lenskart*, it is confirmed on the basis that an AWS S3 link to access the image is sent back from the backend.

4.4 Privacy Policy Analysis w.r.t VTO Feature on Apps

2 of the 5 apps - that send the user's image to a server - violate their own privacy policy. The app *Yourfit By 3DLook*[8] states in its privacy statement “We will not disclose or share your images with third parties”, however, we detected that it did send the user's image to LogRocket session replay service. This violation is on the basis of the criterion *image sharing to third party* as defined in Section 3.3. The app *Lenskart : Eyeglasses & More*, which has over 10 million downloads, states “we do not store any personal/sensitive information on our server. This remains safely with you on your phone/other devices.”, however, we found that the user's image is sent to a URL with the *lenskart.com* domain, and an accessible AWS S3 link to the image is sent back, proving that the image is in fact stored beyond the user's device. This violation is on the basis of the criterion *image storing*. 2 out of 5 of the apps - which send the user's image to a server - have a vague and ambiguous privacy policy, respectively. The final app does not violate its privacy policy.

[6] https://logrocket.com/

[7] The app has been removed from Google Play as of August 10

[8] https://3dlook.me/

4.5 Measurement of Trackers

Scripts. Overall, we found 2609 third-party (TP) scripts in the 138 websites that we crawled. Using the method described in Section 3.4, we categorized 1446 (55%) out of 2609 as trackers, 78 (3%) as advertisers, and the rest are unknown. The top 4 most frequently detected trackers are *googletagmanager.com* (393 out of 1446, 27%), *facebook.net* (180 out of 1446, 12%), *google-analytics.com* (133 out of 1446, 9%), and *hotjar.com* (55 out of 1446, 4%). The *facebook.net* tracker can track user's behavior and share it with third parties [20]. Among the websites with the most TP tracking scripts are websites of popular brands. For example, *E.l.f Cosmetics* has the largest number of TP scripts: 29. See Fig. 3(a) for the top 20 websites with tracking scripts. Furthermore, we found that *E.l.f Cosmetics*'s website has TP tracking scripts from 20 distinct domains, which is the highest number among tested websites. 23 other websites, including *Nars Cosmetics, Jane Iredale, Kits, Madison Reed, Lenscrafter, and Oakley,* have TP tracking scripts from over 10 distinct domains.

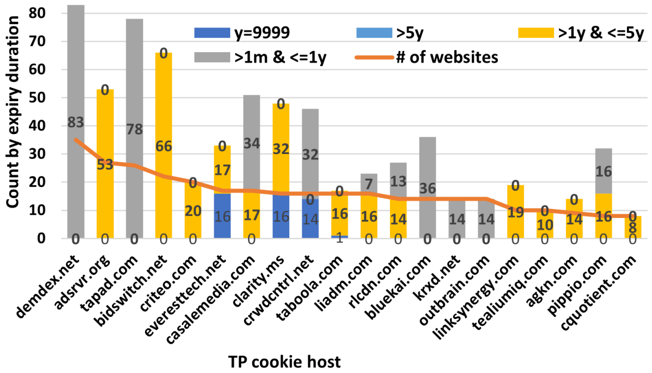
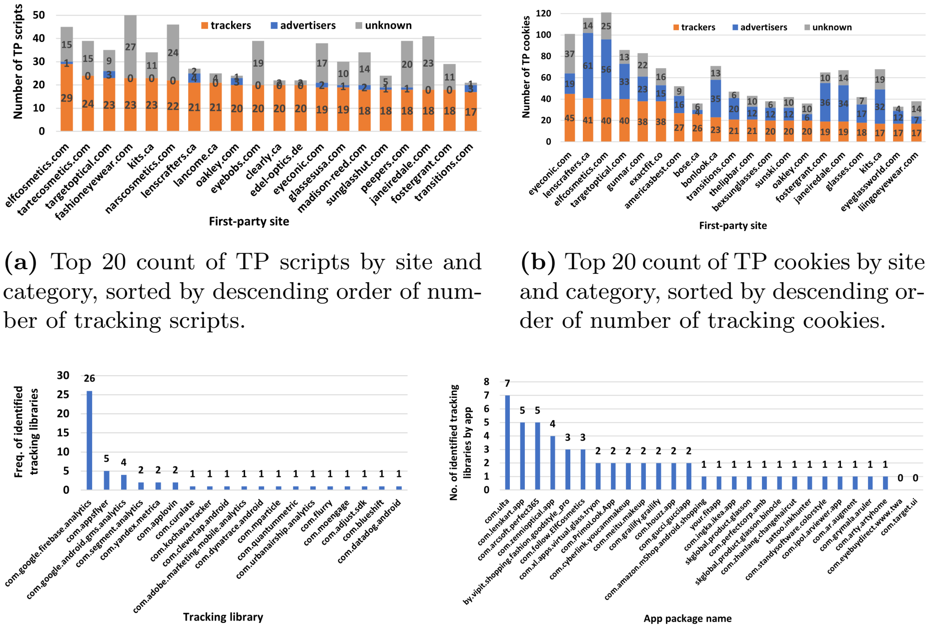


Fig. 2: Expiry of top 20 TP tracker domains sorted by frequency in distinct websites, and the no. of websites in which the top 20 tracker domains are present.

Cookies. We found an overall of 2487 TP cookies in the 138 websites we crawled. 931 (37%) are categorized as trackers, 708 (28%) as advertisers, and the rest are unknown. The most frequently detected tracking domains that have set TP tracking cookies are *demdex.net* (83 out of 931, 8.9%), followed by *clarity.ms* (80 out of 931, 8.6%), then *tapad.com* (78 out of 931, 7.8%). Again, we found popular brands to have a large number of TP cookies in general, and TP tracking cookies in particular. *E.l.f Cosmetics* has the largest number of TP cookies, 121: 40 of which are trackers, and 56 are advertisers (the rest are unknown). Other popular brands such as *Eyeconic*[9] and *Lenscrafters*[10] for eye-wear have 45 and 41 TP tracking cookies, respectively. See Fig. 3(b) for the top 20 websites with tracking cookies. *E.l.f Cosmetics* has its TP tracking cookies from 24 different domains, *Lenscrafters* from 22, and *Eyeconic* from 21. The top three TP tracker domains which occurred in most websites are *demdex.net* (35 out of 138, 25%), *adsrvr.org* (27 out of 138, 20%) and *tapad.com* (26 out of 138, 19%). See Fig. 2 for the number of websites in which the top 20 TP tracker domains are found. We found several TP tracker domains which set cookies with expiry dates to the year 9999. For example, *everesttech.net* and *clarity.ms* have each set such tracking cookies in 16 websites. In the crawled websites, a total of 55 out of 931 (6%) TP tracking cookies are set to the year 9999, 0 to more than 5 years but not 9999, 403 out of 931 (43%) to more than 1 year but less than 5, and 358 out of 931 (38%) to more than one month but less than 1 year. The remaining 115 are less than or equal to 1 month.

Tracking libraries in Android apps. We found 19 distinct tracking libraries in the 28 Android apps we tested. Fig. 3(c) and Fig. 3(d) summarize our findings.



(a) Top 20 count of TP scripts by site and category, sorted by descending order of number of tracking scripts.

(b) Top 20 count of TP cookies by site and category, sorted by descending order of number of tracking cookies.

(c) Overall frequency of identified tracking libraries in tested apps.

(d) Number of identified tracking libraries by app.

Fig. 3: Summary of main findings for tracking scripts (a) and cookies (b) in websites, and tracking libraries in apps (c, d).

[9] https://www.eyeconic.com/

[10] https://www.lenscrafters.ca

4.6 Analysis of VTO Service Providers

Out of the the 3 VTO service providers we tested (*Perfect Corp*[11], *Deep AR*[12], *Vossle*), only *Vossle* is found to have major issues. As an end-user who clicks on a generated link for a particular VTO experience of a merchant, the end-user can view (in the response to the GET request) the merchant's personal details such as name, email, mobile number, user id, and the login code associated with the account on sign up, as well as *Shopify*, *Magento* and *WordPress* plugin keys. Assuming a key can be used more than once or a Merchant has not used their key, a non-*Vossle* subscriber could possibly steal a merchant's *Magento* key to use the *Vossle* plugin in their own store. We also found an instance of broken authentication and authorization. Merchants' account IDs are integers starting from 0 onward; meaning, they can be enumerated. This makes it possible to collect personal information of all merchants who use the platform, as there exists an API which retrieves the details of all VTO experiences of a particular merchant using the account ID. The retrieved details include the URL slug of the VTO experience. The URL slug can be used with the previously mentioned API - which requests the VTO experience - to get the personal details of the merchant.

Another instance of broken authentication and authorization is that given the account ID of a victim and removing the authentication parameters from the request, an attacker can create a new VTO experience on behalf of the victim. This can cause confusion to the victim with regards to their VTO collection, and it can be used - for example - to create inappropriate VTO experiences and share it in the name of the victim.

We also observed that no anti-CSRF tokens were used on the *Vossle* website. However, the use of a JWT token instead of session cookies made CSRF attacks possible only in one operation: creating a new VTO experience, where the JWT authentication token is not checked by the website.

A privacy issue we found during sign-up on the platform is that the typed password and email are sent to the session replay service *sentry.io*. The state of the email and password fields gets captured after every character change, including deletion and addition. The different captured states of the email and password fields (as well as other fields) are then sent in one request, resulting in the final state of the email and password being sent to the session replay service.

We informed Vossle about the vulnerabilities but they did not reply. We emailed them again after over two months since the first notification, but again, we did not receive any response (as of September 30, 2023).

5 CONCLUSION

Based on our analysis, we can conclude that there are concerns regarding the manner in which websites and apps featuring VTO technology manage the privacy of their users, particularly in relation to their images. The majority of tested

[11] https://www.perfectcorp.com/business

[12] https://www.deepar.ai/

websites send users' images not only to their servers, but also to third-parties as well. The images are stored in many cases, and VTO providers of websites can extract face geometry from users' images. Many VTO featuring websites/apps either violate their own privacy policy or they use a VTO provider that violates its own privacy policy. Furthermore, several websites are found to mislead users by displaying disclaimers - upon using the VTO feature - which are opposite to the reality and do not represent their privacy policies. This is in addition to the lack of clarity in privacy policies as of what really happens to the user's data while using the VTO feature. We also show that there are many third-party tracking scripts and cookies present in VTO websites. Lastly, we found one VTO service provider to be compromising the privacy of its clients by sharing their email and password with a session replay service, and compromising the security of their accounts due to vulnerabilities broken authentication and unauthorized access.

6 ACKNOWLEDGMENT

This work was supported by the Office of the Privacy Commissioner of Canada (OPC). We also thank the anonymous DPM 2023 reviewers for their insightful feedback and suggestions.

References

1. K. Cantwell. Zlib: A command-line utility for quickly compressing or decompressing zlib data. `https://github.com/kevin-cantwell/zlib`.
2. Cdimascio. py-readability-metrics. `https://github.com/cdimascio/py-readability-metrics/tree/master#flesch-kincaid-grade-level`.
3. J. Davis. How 5g will change retail. `https://www.insiderintelligence.com/content/how-5g-will-change-retail`, Mar 2021.
4. EasyList. Easylist. `https://easylist.to/`.
5. S. Englehardt and A. Narayanan. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, New York, NY, USA, 2016. ACM.
6. Y. Feng and Q. Xie. Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps. *Journal of Interactive Advertising*, 19(1), 2019.
7. Frida. Frida. `https://github.com/frida/frida`.
8. A. Householder, G. Wassermann, A. Manion, and C. King. CERT® Guide to Coordinated Vulnerability Disclosure. `https://resources.sei.cmu.edu/asset_files/specialreport/2017_003_001_503340.pdf`, 9 2020.
9. A. Ivanov, Y. Mou, and L. Tawira. Avatar personalisation vs. privacy in a virtual try-on app for apparel shopping. *International Journal of Fashion Design, Technology and Education*, 16(1), 2023.
10. Kaspersky. What is facial recognition – definition and explanation. `https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition`.
11. K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy*. IEEE, 2018.

12. J. Liebers, P. Horn, C. Burschik, U. Gruenefeld, and S. Schneegass. Using gaze behavior and head orientation for implicit identification in virtual reality. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology*, New York, NY, USA, 2021.
13. M. R. Miller, F. Herrera, H. Jun, J. A. Landay, and J. N. Bailenson. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports*, 10(1), 2020.
14. V. Mirjalili and A. Ross. Soft biometric privacy: Retaining biometric utility of face images while perturbing gender. In *2017 IEEE IJCB*, Denver, CO, USA, 2017.
15. OnlineJPGTools. Convert base64 to jpeg. `https://onlinejpgtools.com/convert-base64-to-jpg`.
16. OnlinePNGTools. Convert base64 to png. `https://onlinepngtools.com/convert-base64-to-png`.
17. R. Pagey, M. Mannan, and A. Youssef. All your shops are belong to us: Security weaknesses in e-commerce platforms. In *Proceedings of the ACM Web Conference 2023*, WWW '23, New York, NY, USA, 2023. ACM.
18. K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, and F. Alt. Behavioural biometrics in VR: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2019.
19. F. Roesner, T. Kohno, and D. Molnar. Security and privacy for augmented reality systems. *Communications of the ACM*, 57(4), 2014.
20. N. Samarasinghe, P. Kapoor, M. Mannan, and A. Youssef. No salvation from trackers: Privacy analysis of religious websites and mobile apps. In *DPM, ESORICS 2022 International Workshops, DPM 2022 and CBT 2022*, Berlin, Heidelberg, 2023. Springer-Verlag.
21. Skylot. Jadx. `https://github.com/skylot/jadx`.
22. A. R. Smink, S. Frowijn, E. A. van Reijmersdal, G. van Noort, and P. C. Neijens. Try online before you buy: How does shopping with augmented reality affect brand responses and personal data disclosure. *Electronic Commerce Research and Applications*, 35, 2019.
23. S. Stephenson, B. Pal, S. Fan, E. Fernandes, Y. Zhao, and R. Chatterjee. SoK: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2022.
24. Technavio. Augmented reality and virtual reality market by technology, application, and geography - forecast and analysis 2023-2027. `https://www.insiderintelligence.com/content/how-5g-will-change-retail`, Oct 2022.
25. R. Trimananda, H. Le, H. Cui, J. T. Ho, A. Shuba, and Markopoul. OVRseen: Auditing network traffic and privacy policies in Oculus VR. In *31st USENIX*, 2022.
26. T. Zhang, W. Y. C. Wang, L. Cao, and Y. Wang. The role of virtual try-on technology in online purchase decision from consumers' aspect. *Internet Research*, 2019.