No Privacy for Privates: How Military Communities Experience and Perceive the Privacy Risks of Military-Marketed Mobile Apps

Joshua Shinkle
Purdue University
jcshinkl@purdue.edu

Chandrika Mukherjee
Purdue University
cmukherj@purdue.edu

Abdullah Imran
Purdue University
imran8@purdue.edu

Arjun Arunasalam
Florida International University
aarunasa@fiu.edu

Donna Artusy*
Army Cyber Institute
dva3@georgetown.edu

Antonio Bianchi
Purdue University
antoniob@purdue.edu

Z. Berkay Celik
Purdue University
zcelik@purdue.edu

Alexander Master
United States Military Academy
alexander.master@westpoint.edu

Abstract

A subset of mobile applications is explicitly marketed to military-affiliated personnel. These Military-Marketed Mobile Apps (MMMApps) collect privacy-sensitive data using the same mechanisms as general-purpose apps. However, when such data belongs to military-affiliated personnel, it may be exploited by malicious actors in ways that threaten personal safety, unit operations, and national security. Despite these risks, the data practices and code provenance of MMMApps, as well as how this population perceives and attempts to mitigate these risks, remain poorly understood. In this paper, we address this gap by combining large-scale app analysis with a user study. We first curate a dataset of 242 MMMApps and leverage app analysis techniques to characterize their data practices and code provenance. Then, we conduct a user study with $n = 103$ military-affiliated participants in the United States to examine which data practices and code provenance characteristics they consider inappropriate, what threat scenarios they believe those practices enable, and which mitigations they view as most effective.

Our results show that MMMApps frequently exhibit data practices and code provenance characteristics that are misaligned with the privacy expectations of military-affiliated personnel. For instance, 40% of MMMApps collect more data than they disclose in their privacy labels or data safety sections. 83.5% of our study participants report using at least one MMMApp that engages in data practices they are uncomfortable with. Additionally, although military-affiliated personnel are generally concerned about third-party libraries accessing their data, 64% of MMMApps include third-party SDKs, some developed in countries perceived as adversarial by a majority of the participants. Overall, our findings reveal a substantial misalignment between the privacy expectations of military-affiliated personnel and the data practices and software supply chains of MMMApps. We propose recommendations at the federal, DoD, app store, and device levels to improve privacy risk mitigation for this at-risk population.

Keywords

data privacy, at-risk populations, mobile app analysis, data disclosure, mobile security, user study, perceptions, third-party SDKs

1 Introduction

When a fitness app leaks location data from a civilian jogger, it creates a privacy concern. When the same app leaks location data from a service member stationed at a military base, it can reveal military secrets, potentially costing people their lives [57]. This distinction highlights a critical gap in mobile privacy research: while data collection practices in consumer apps have been extensively studied [4, 6–8, 19, 22, 60, 63, 65, 77, 80, 82, 84, 97, 113, 119, 125, 128, 129, 138, 145, 150, 155, 159], the amplified risks these same practices pose to military-affiliated personnel remain poorly understood.

United States (U.S.) military-affiliated personnel (i.e., active-duty service members, reservists, Department of Defense (DoD)[1] civilians, veterans, and family members of these individuals) increasingly rely on commercial mobile apps for health services, financial management, professional development, and community connection [9, 53, 158]. The mobile app ecosystem's economic model, which depends heavily on the collection and sale of personal information [17, 47, 85, 123, 134, 160], creates significant data exposure for this population. Data brokers actively sell datasets targeting military personnel, including granular location traces, financial information, and behavioral profiles [47, 135]. When aggregated and sold, this data enables adversaries to conduct surveillance, social engineering, and targeted attacks against individuals involved in national security [5, 20, 26, 34, 46, 54, 67, 92, 93, 96, 116, 137, 156].

Despite these heightened stakes, existing protections are inadequate. Prior research shows that apps frequently collect and share more data than they disclose in their app store listings and privacy policies [3, 64, 73]. Compounding this, a subset of mobile apps specifically market themselves to military-affiliated personnel. We

Proceedings on Privacy Enhancing Technologies 4(1), 1–21

*The views and conclusions expressed in this paper are those of the authors and do not necessarily reflect the official views, policies, opinions, or positions of their employers, organizations, affiliations, or sponsors.

[1]"DoD" is widely used throughout U.S. Code and military doctrine, while some newer documents refer to the organization as the Department of War (DoW). We use DoD throughout for uniformity and clarity.

refer to these apps as MMMApps (Military-Marketed Mobile Apps).[2] Whether the data practices and code provenance characteristics of MMMApps are misaligned with what their target users find appropriate, and the degree to which a gap exists between what these apps do and what their users know or expect, remain open questions.

In this paper, we address these gaps through a two-pronged investigation. Combining mobile app analysis and a user study, we examine both practice (what data MMMApps actually collect, transmit, and disclose, along with their code provenance) and perception (how military-affiliated personnel understand and attempt to mitigate the risks these apps pose). More precisely, this paper investigates the following research questions:

RQ1: *What data practices and code provenance characteristics are present in MMMApps?*
RQ2: *How do the data practices and code provenance characteristics of MMMApps align with the perceptions of military-affiliated personnel?*

- **RQ2a**: *To what extent do MMMApps' data practices and code provenance characteristics align with what military-affiliated personnel consider appropriate?*
- **RQ2b**: *Based on the data practices and code provenance observed in RQ1, what inferences and threat scenarios do military-affiliated personnel believe are possible, and which security domains do they believe are at risk?*
- **RQ2c**: *What mitigations do military-affiliated personnel assess as most effective and which would they be most likely to adopt or support?*

We first curate a dataset of 242 MMMApps through systematic searches of app marketplaces and military-focused online forums. Then, using established static analysis, dynamic analysis, and network traffic analysis tools and techniques from prior work, we analyze MMMApps' data collection, transmission, and privacy disclosure practices. We focus on what types of data are being collected and transmitted, recognizing that certain data types are perceived as more sensitive than others. In parallel, we examine the code provenance responsible for such data practices (i.e., the origin of all code contained in the app, including code by the first-party developer, directly included third-party libraries, and transitively included dependencies of those libraries), as this dimension introduces potential software supply-chain risks and privacy concerns.

Lastly, we conduct a user study with $n = 103$ military-affiliated personnel, treating them as domain experts to surface what behaviors they find inappropriate (e.g., which data they don't want apps collecting), what threat scenarios they believe those behaviors enable, and which mitigations they believe would be most effective.

Our analyses reveal that MMMApps not only transmit data to third-party services, but also exhibit code provenance characteristics that military-affiliated personnel find inappropriate. For example, 40% of MMMApps show discrepancies between their stated privacy disclosures and their actual data practices. Additionally, 83.5% of our military-affiliated study participants use at least one MMMApp that engages in data practices they find inappropriate. Furthermore, over 13% of MMMApps contain foreign first-party or third-party code, and a non-trivial subset includes code from countries the U.S. government has formally listed as "adversaries", countries whose code participants were almost unanimously uncomfortable with. In one case, the foreign code was introduced through a third-party dependency, without the developer's awareness. After our responsible disclosure, the developer removed the dependency. Together, these findings reveal a significant mismatch between the privacy expectations of MMMApp users and the actual data collection and supply chain practices of these mobile apps.

In summary, this paper makes the following contributions:

- We present the first curated dataset of 242 MMMApps, establishing and documenting the existence of this distinct app ecosystem that explicitly markets itself to military-affiliated personnel.
- We conduct the first technical analysis of MMMApps' data collection, transmission, and privacy disclosure practices, as well as code provenance.
- Through a user study with $n = 103$ U.S. military-affiliated personnel, we uncover which data practices and code provenance they find inappropriate, the inferences and threat scenarios they attribute to their discomfort, and instances in which they are unknowingly using apps that exhibit those behaviors perceived as inappropriate.
- We propose recommendations at the federal, DoD, app store, and device levels that military-affiliated personnel rate as most effective and would be likely to adopt or support.

Our work produced the following artifacts, which are publicly available on our project GitHub page: the list of 55 military-related keywords, the MMMApp dataset, the user study questionnaire, and the per-question aggregated quantitative user study response data.[3]

2 Background and Related Work

2.1 Privacy Analysis of Mobile Data Collection

Mobile apps collect data through multiple mechanisms: direct user input, access to device sensors and resources via permissions, and background processes that monitor user behavior [86, 87]. A significant portion of data collection occurs through third-party libraries and software development kits (SDKs) embedded within apps. These components provide functionality such as analytics and advertising, but they also transmit user information to remote servers, often without explicit user awareness or developer oversight. In particular, advertising SDKs track users across multiple apps and devices, aggregating behavioral data to build detailed user profiles [83]. When combined with data from other sources such as web trackers and cookies [25, 41, 92, 157], this information enables highly personalized dossiers that can be sold to data brokers and other third parties [81, 126]. To increase transparency, both Google and Apple have introduced disclosure mechanisms (Google Play Store's Data Safety section [62] and Apple's App Privacy Labels [61]) that require developers to disclose what data is collected, how it is used, and whether it is shared with third parties. However, these disclosures rely entirely on developer self-reporting and are not verified through automated auditing [3, 95].

[2] For example, USAA Mobile, a financial app, advertises itself as "an organization founded by military members for military members." [115]

[3] https://github.com/purseclab/no_privacy_for_privates

Researchers have extensively studied mobile app privacy using static analysis, dynamic analysis, and network traffic analysis [4, 8, 12, 43, 69, 75–77, 79, 80, 94, 97, 113, 114, 119, 121, 136, 159]. Several studies have applied these techniques across the app ecosystem and in specific domains (e.g., health, finance, children's apps), employing tools such as MobSF [1], Frida [122], and mitmproxy [31]. Findings consistently reveal widespread privacy violations, including unauthorized data collection, undisclosed third-party sharing, and discrepancies between stated and actual practices [13, 19, 37, 60, 64, 66, 72–74, 78, 82, 88, 89, 98, 124, 128, 129, 150, 154, 155]. Domain-specific studies reveal heightened privacy risks due to the sensitivity of the data involved and the vulnerability of target populations [6, 7, 22, 59, 63, 65, 84, 125, 138, 145]. Despite this extensive body of technical measurement work, MMMApps remain unexplored.

Our work extends prior work by applying established technical analysis methods to MMMApps, using their results to reveal gaps between what MMMApps do and what their users find acceptable.

2.2 User Perceptions of Mobile Privacy

While technical analysis reveals how apps behave, understanding users' perception and response to privacy risks is equally important for developing mitigations. Prior research has investigated user understanding of mobile app permissions [35, 40, 120, 143], comfort with data collection [14, 16, 127, 153], and ability to interpret privacy policies [18, 33, 144], finding that users have limited awareness of data practices and struggle to make informed privacy decisions.

Although data leaks can carry dramatically different consequences for military-affiliated personnel, and their privacy expectations may differ accordingly, no prior work has systematically investigated how this at-rsik population perceives privacy risks in mobile apps. Our user study addresses this gap by examining which data practices and code provenance characteristics military-affiliated personnel find inappropriate, what threat scenarios they believe those practices enable, and which mitigations they believe would be most effective/likely for them to support.

2.3 Privacy for Vulnerable Populations

Certain populations face heightened privacy risks due to their circumstances, identities, or roles. Prior research has examined privacy among activists at risk from state-level actors [131, 142], survivors of intimate partner violence vulnerable to technology-enabled stalking [130], immigrants and refugees concerned about surveillance by authorities [141, 149, 152], and LGBTQ+ individuals facing outing and discrimination [11, 39, 50, 139]. Across these, privacy violations that might be merely inconvenient for general users can have severe or even life-threatening consequences.

Despite this growing body of work on at-risk populations, military-affiliated personnel have received relatively little attention in privacy research. This gap is striking given documented risks: data brokers actively sell datasets targeting military personnel, adversaries can exploit mobile app data for intelligence gathering and social engineering, and even unintentional data exposure can compromise OPSEC and national defense [5, 34, 46, 57, 93, 96, 135]. Military-affiliated individuals face unique threat actors (e.g., nation-state adversaries and violent extremists), unique threat scenarios (e.g., mortar attacks on military outposts), and unique consequences (e.g., national security implications beyond personal harm).

Our work addresses this gap by conducting the first systematic investigation of privacy risks in apps marketed to military-affiliated personnel, combining the first technical analysis of MMMApps' data practices and code provenance with a user study examining whether military-affiliated personnel find those practices acceptable and what threat scenarios they believe those practices enable.

3 Motivation and Problem Statement

A subset of mobile apps (MMMApps) explicitly market themselves to military-affiliated personnel. Like all consumer apps, MMMApps are part of an ecosystem that depends heavily on data collection. For military-affiliated personnel, the stakes of that collection are categorically higher and well documented [5, 21, 26, 32, 54, 93, 96, 133, 147]. Critically, privacy risks are not limited to malicious apps. Even benign apps introduce vulnerabilities, as collected data can be sold or misused long after collection [135].

Yet, this problem remains poorly understood. Whether MMMApps exhibit data practices or code provenance characteristics that put users at risk had never been examined. Furthermore, whether military-affiliated personnel find these practices acceptable, what threat scenarios they believe those practices enable, and what mitigations they believe would be effective, had not been studied. This paper addresses both dimensions: examining what data practices and code provenance characteristics MMMApps exhibit, and whether military-affiliated personnel perceive those behaviors as acceptable.

4 Curating and Analyzing MMMapps

To investigate RQ1, we curate a dataset of MMMApps and take a mixed-method approach to analyze them.

4.1 Dataset Curation

While many apps explicitly market themselves to military-affiliated personnel, there is no single category or keyword on the Google Play Store that enables users to easily identify and retrieve all such apps. Additionally, some of these apps are popular, but only within specific niche communities. Therefore, to create our dataset of 242 MMMApps, we had to use two complementary approaches, sourcing apps from the Google Play Store and online forums.

4.1.1 Google Play Store

We first focus on collecting apps from the Google Play Store, the most popular platform for Android apps [148].

Seed Dataset. We generated a list of 55 military-related keywords through a brainstorming session with U.S. Army researchers (who were active-duty service members and Army civilian employees themselves) and used it to query Google Play. For each keyword, we retrieved 100 candidate apps by leveraging a third-party API (SerpAPI [71]), retrieving, in total, 719 unique apps.

Here, we note that the apps retrieved are not necessarily relevant apps. For example, after manually inspecting 15% of the retrieved apps, we found only 20% (21 apps) to be relevant. Thus, we manually labeled each app. Two authors independently labeled all 719 retrieved apps. These authors leveraged a careful labeling guide (See Appendix A.1). After labeling, the authors demonstrated a high

level of agreement, with Cohen's Kappa > 0.8 [58]. After reconciling the differences, we obtained a seed dataset of 168 MMMApps.

Filtering and Curating the Final Dataset. To expand beyond the seed dataset, we leveraged the 168 manually labeled apps to develop a high-recall filtration classifier. After evaluating multiple approaches (See Appendix A.2.1), we adopted an LLM-as-a-Judge model [51], with a recall = 0.94 to identify candidate MMMApps based on app descriptions. We then conducted additional data collection in batches: in each iteration, we queried Google Play using 10 new keywords, passed retrieved apps through the classifier, and manually validated candidate apps. We repeated this process until saturation (no new unique MMMApps identified), which occurred after four iterations (See Figure 5 for saturation details). This yielded 32 additional apps, resulting in a final dataset of 200 MMMApps.

4.1.2 *Online Forums*

We note that keyword searches on the Google Play Store target popular/highly rated apps. To augment our dataset with relevant MMMApps that are not well-ranked in the Play Store, we sourced apps from military-related online forums[4].

Forum Thread Curation. After consulting with active service members, we identified seven core subreddits: `r/military`, `r/army`, `r/USMC`, `r/navy`, `r/airforce`, `r/spaceforce`, and `r/uscg`. We leveraged the PRAW API [36] and app-related keywords (e.g., "app", "android", "google play") to retrieve 1, 500 unique threads. We manually inspected a 10% random sample and identified 251 app mentions (including redundant references), of which 18% were military-related, yielding 12 unique MMMApps across the sampled 150 threads.

Semi-Automated App Extraction. Given this low yield and the scale of the remaining threads, we adopted a semi-automated extraction approach. Specifically, we used an LLM-as-a-Judge to identify app mentions within threads and validated its performance on the manually inspected sample, achieving 99% recall.

We applied this extraction method in intervals to the remaining threads. At each interval, the authors confirmed the validity of the extracted apps, independently reviewing and annotating them with our labeling guide, demonstrating high agreement ($\kappa > 0.8$). We observed saturation after 16 processing intervals, with later batches yielding no new unique apps. In total, we identified 70 unique MMMApps from Reddit, 42 of which were not present in our Google Play dataset, resulting in a cumulative dataset of 242 MMMApps. We provide details of our LLM-as-a-Judge approach, the prompt used, and information on the saturation of apps in Appendix A.3.

We found Hots&Cots, Air Force promotion apps such as AFI Explorer, ACE PDG, and PDG Promote 2025+, as well as Navy BMR and Bluejacketeer, to be among the most frequently mentioned apps within these Reddit threads (see Figure 1). In addition, we identified apps related to uniform management, banking, health and benefits, test preparation, career navigation, and other relevant categories. While some apps received many mentions, the majority of references pointed to a long tail of less-cited apps. This reflects the diverse range of mobile tools used across the military community.

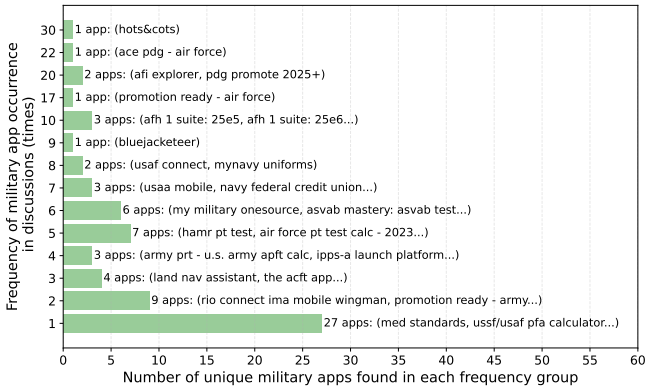

Figure 1: Popular apps mentioned in online forums.

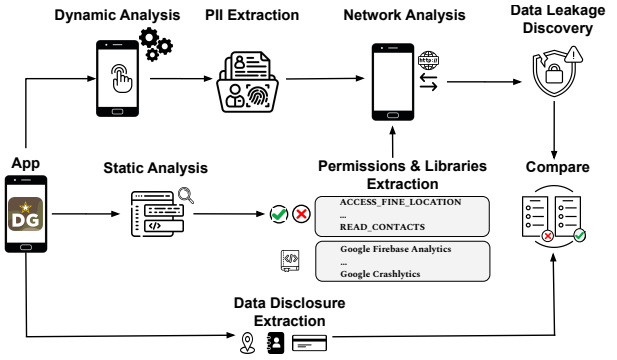

Figure 2: App analysis pipeline.

4.2 App Analysis Pipeline

Figure 2 overviews our systematic investigation of the data collection and transmission behaviors of MMMApps. We leverage static analysis, dynamic analysis, network traffic analysis and a comparison of data collection practices with developer disclosures.

Static Analysis. We leverage the Mobile Security Framework (MobSF v3.9.7) [1], which allows us to extract the permissions requested and the third-party dependencies embedded within the app. Permissions comprise access to sensitive system resources such as location data, contacts, storage, and unique device identifiers. Third-party dependencies include advertising networks, analytics platforms, and external SDKs that can collect and transmit user data independently. The information gathered from the static analysis serves as a basis for subsequent dynamic and network analysis.

Dynamic Analysis. The goal of our dynamic analysis was to extract what personally identifiable information (PII) is requested by the app, serving as a targeted filter to inform our subsequent network analysis. We leverage AndroidViewClient (v23.4.0) [42] to interact and capture UI elements displayed by an app during runtime. We ran each app for five minutes and systematically navigated through its core functionalities, and capture UI elements by searching for specific keywords and patterns corresponding to sensitive information such as "Name", "Email", and "Phone Number",

[4]We commit to sharing this paper's findings through these forums as well.

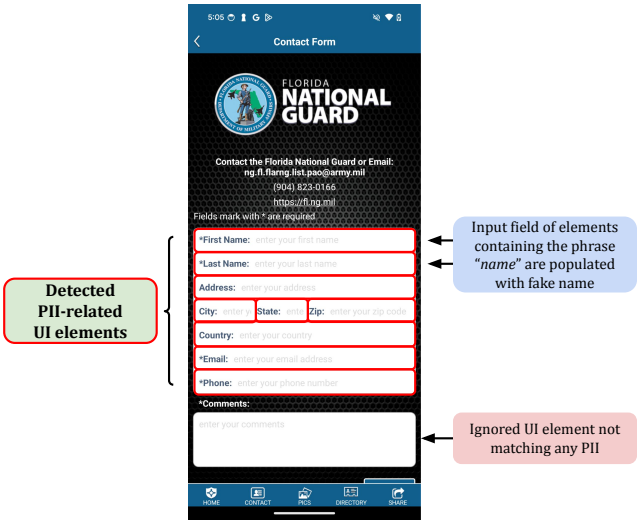

Figure 3: AndroidViewClient's detection of PII-related UI elements, achieved via keyword search.

as shown in Figure 3. UI elements considered include text fields, buttons, labels, and other input components that request personal information. We interact with each element and determine whether a new activity has been launched, doing so recursively until no additional activities are reachable. We note that the presence of a UI input field requesting PII does not itself confirm that the app collects that data. Rather, these findings guide our network analysis, which serves as the definitive means of identifying collected PII. Similarly, if a UI input field displays pre-filled personal information, we treat this as a signal that the app may have retrieved and stored that data, which we then verify through network traffic inspection.

Network Analysis. Whereas our dynamic analysis identifies what PII is requested by an app, our network analysis serves as the primary means of confirming what PII is actually collected and transmitted. We leverage MobSF with OWASP Zed Attack Proxy (ZAP v2.15.0) [112] to monitor network traffic while executing the app. ZAP operates as an interception proxy, and by installing ZAP's root certificate, we decrypt traffic from the app to external servers. To audit traffic to external servers, we take two approaches. First, we enter particular dummy personal information (such as a test email address, name, and phone number) into the app and monitor outgoing network traffic to see if these exact values appear in transmitted requests. If we detect a match, it serves as direct evidence that the app is transmitting user-provided PII over the network. To account for data transmitted in encoded/transformed formats, we check for common encoding schemes such as Base64, URL encoding, and simple hashing (e.g., MD5, SHA-1, SHA-256) of the known dummy inputs (e.g., names, emails, and phone numbers). Second, we search for indirect indicators of location-adjacent data, such as IP addresses, geolocation coordinates (latitude and longitude), and location-related keywords. This allows us to identify apps that may be circumventing explicit location permissions by deriving user location through IP-based geolocation techniques.

Code Provenance Analysis. To characterize the code provenance of MMMApps, we examined the geographic origin of all code contained in each app, distinguishing between first-party code written by the app developer and third-party code introduced through libraries identified in our analysis pipeline. For each app, we determined the country of origin of the first-party developer by scraping the Google Play Store for all developer-related data and analyzing the `developerLegalAddress` field. We found developer-related data for 205 apps in our dataset, while the remaining 37 apps were no longer available on the Google Play Store. Then, for each unique third-party library detected by our static analysis, we determined the library's country of origin by searching for the location of the developing company's headquarters in publicly available information. In both cases, we classified origins into three categories: U.S.-based, foreign, and originating from a country designated as "adversarial" in the 2023 DoD Cyber Strategy [101]. This classification allows us to assess the degree to which they contain code from entities that military-affiliated personnel are uncomfortable with.

Developer Disclosure Comparison. To assess the transparency and accuracy of app developers' disclosures, we compare data collection practices with information disclosed by developers. We scraped the Data Safety sections [62] for all Android apps in our dataset, gathering details of "data collected" and "data shared", as categorized by Google (e.g., location data, personal information, financial information) and cross-referenced them with observed data flows extracted from static, dynamic, and network analyses.

We choose MMMApps' Data Safety sections for comparison instead of their privacy policies because these sections are designed to (1) be readily accessible to users downloading the app and (2) draw user attention, whereas privacy policies are lengthy, filled with legal jargon, and often ignored [23].

Comparative Evaluation. To contextualize our findings, we establish a baseline of the iOS counterparts of MMMApps in our dataset. These comparisons enable us to evaluate cross-platform consistency in data collection and transmission behaviors.

We replicated our analysis pipeline on iOS. We took the sequence of actions performed during the automated Android dynamic analysis and manually reproduced them on the iOS version of the MMMapp, using WebProxyTool (v3.7.4) [44] to inspect the network traffic and verify whether the same data is transmitted by the iOS version of the MMMapp. While MobSF supports iOS analysis via the Corellium emulator, we found that many iOS apps use anti-emulation checks that disrupt execution. To avoid incomplete/misleading results, we didn't use MobSF for our iOS static analysis.

We extended our developer comparison to include Apple Privacy Labels [61] for each corresponding iOS version of the apps in our dataset. Apple's Privacy Labels disclose what types of data an app may collect, whether that data is linked to the user, and whether it is used for tracking purposes. To systematically gather this information at scale, we employed a scraper that queried publicly available metadata for iOS apps via Apple's App Store web interface.

4.3 RQ1: Data Practices and Code Provenance Characteristics of MMMapps

To evaluate the data practices and code provenance of MMMApps, we used the dataset collected as described in Section 4.1. From

Table 1: Data practices of MMMApps

Data Practices	Distribution	
(A) Third-Party Libraries	**% of Apps Using**	**# Third-party Libraries (% of Apps)**
	Google Firebase Analytics (59%)	0 (36%)
	Google Crashlytics (50%)	1–3 (41%)
	Google AdMob (20%)	4–6 (15%)
	Facebook Analytics (16%)	7–9 (6%)
	Google Tag Manager (13%)	10+ (2%)
(B) Requested Permissions	**% of Apps Requesting Permissions**	
	CAMERA (38%)	
	ACCESS_COARSE_LOCATION (34%)	
	READ_PHONE_STATE (28%)	
	ACCESS_FINE_LOCATION (27%)	
	RECORD_AUDIO (21%)	
	READ_CONTACTS (14%)	
	ACCESS_BACKGROUND_LOCATION (4%)	
(C) PII Requested	**% of Apps Containing**	**# PII Types Detected (% of Apps)**
	Email Address (18%)	
	Name (16%)	
	Phone Number (11%)	0 (70%)
	Military Base/Installation Branch (5%)	1–2 (15%)
	Address (5%)	3–4 (10%)
	DOB (3%)	5+ (4%)
	Gender (2%)	
	Age (2%)	
(D) PII Transmissions	**% of Apps Transmitting**	
	Email Address (17%)	
	Name (15%)	
	Phone Number (10%)	
	Military Base/Installation Branch (5%)	
	Address (5%)	
	DOB (3%)	
	Gender (2%)	
	Age (2%)	

this dataset of 242 apps, we were able to download and analyze 223 of them. The following sections report the findings from our static, dynamic, and network traffic analysis, along with our code provenance and privacy disclosure results.

4.3.1 *Data Practices Results*

Third-Party Library Usage. A key aspect of the static analysis was identifying the embedded third-party libraries. These libraries, often used for analytics, advertising, crash reporting, and cloud storage, can facilitate data sharing with external entities. Through our analysis, we found that 64% of MMMApps in our dataset incorporate one or more third-party SDKs. Certain third-party libraries appeared frequently throughout the dataset, particularly those related to analytics and advertising. The prevalence of these libraries suggests that many MMMApps are actively collecting usage statistics, behavioral data, and potentially PII, which could be used for advertising or monetization. Table 1(A) summarizes the most common third-party libraries and their distribution across MMMApps.

Permissions Requested. The permissions requested by MMMApps gave us insight into the types of data they accessed. The most frequently requested permissions are summarized in Table 1(B).

Detected PII Fields. To quantify the frequency with which different types of PII appeared in the analyzed MMMApps, our dynamic analysis extracted and classified the UI elements containing references to sensitive user information. We found 29% of MMMApps requesting or storing at least one form of PII, with email address as the most commonly detected PII field and 18% of MMMApps containing a user input field for it. Additionally, some MMMApps contained UI elements for military-specific identifiers, such as military base/installation and branch. Table 1(C) summarizes the number of different types of PII detected. Table 1(C) shows the percentage of MMMApps containing a UI element for each PII type, respectively.

Table 2: Provenance of first-party and third-party code

First-Party Code		Third-Party Code	
Origin	**% of Apps**	**Origin**	**% of Apps**
United States	86.3%	United States	57.4%
Foreign	13.7%	Foreign	15.3%
"Adversarial" Country	1.5%	"Adversarial" Country	7.4%

Transmitted PII. The network traffic analysis phase aimed to determine whether the PII detected in the dynamic analysis phase was being transmitted outside the device and to whom. We found that email address is the most commonly transmitted PII with 17% of MMMApps transmitting it. Table 1(D) summarizes the frequency with which each type of PII was observed in network transmissions. To understand who was receiving the transmitted PII, we categorized the destinations into two groups:

- App-Owned Servers: The app's own backend infrastructure, expected to receive user data for legitimate purposes (e.g., authentication, profile management).
- Integrated Third-Party Services: External services such as analytics platforms, advertising networks, or cloud storage providers that were integrated into the app as third-party libraries or SDKs.

We observed that 19% of MMMApps transmit PII to app-owned servers, while 3% of apps transmit PII-related information to known third-party services. Notably, 16% of apps that collected some form of PII were transmitting that data to third-party services often linked to advertising or analytics SDKs. While some of these transmissions were expected (e.g., app functionality requiring cloud storage), we also observed cases where PII was shared with third parties without an apparent functional necessity.

Although not all the Android apps we analyzed were available on iOS, we were able to download and examine 80 apps on iOS. For these 80 MMMApps, we found no discrepancies between our Android and iOS results. Whenever data transmission was observed in the Android version of an MMMApp, we also observed the same data being transmitted in the corresponding iOS version.

4.3.2 *Code Provenance: Results*

Table 2 overviews the code provenance of first-party and third-party code, organized by origin: United States, Foreign, or "Adversarial" Country (a subset of foreign countries, explicitly determined as "threats" in the 2023 DoD Cyber Strategy [101]; specifically, the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea). The full list of MMMApps that contain code originating in a foreign or "adversarial" country can be found in Appendix C. While the primary origin of code across both first-party and third-party is within the U.S., both categories have non-negligible foreign origin rates (which potentially may pose both privacy and operational risk for U.S. military-affiliated personnel). In particular, 86.3% of MMMApps originated within the United States, while 13.7% are foreign (1.5% of them are from the "adversarial" countries). Foreign countries include the United Kingdom, China, India, Canada, Turkey, Indonesia, Spain, Uzbekistan, Pakistan, Vietnam, Greece, Argentina, Colombia, Armenia, and Australia. Additionally, we found 76 unique third-party libraries being used in the analyzed apps. 57.4% of MMMApps

contained U.S. third-party code, while a surprising 7.4% contained code from an "adversarial" country (15.3% overall were foreign). The foreign third-party libraries originated from China, Israel, Russia, Germany, India, the United Kingdom, Canada, and Switzerland.

4.3.3 Code Provenance: Case Studies

Huawei SDK in MMMapps. Our analysis identified twelve MMMapps that integrate the Huawei Mobile Services (HMS) Core SDK. HMS Core[5] advertises its ability to map user locations, deliver advertisements for monetization, provide "app linking," and manage user images and video storage, among other capabilities [68].

These findings are significant given that in June 2020, the U.S. Federal Communications Commission (FCC) declared Huawei a national security threat to the U.S. [28], due to their close ties to the Communist Party of China and Chinese laws which require corporations to cooperate with intelligence services of the People's Republic of China [45]. Recent bipartisan efforts in the U.S. Congress have also been made to limit Huawei's activities [111]. Huawei's technology has been restricted in critical sectors to deter potential cyberspace espionage efforts that could be facilitated by Chinese hardware and software. Furthermore, despite the FCC's concerns, Huawei's SDK and the MMMapps that include it are widely available, and no regulatory guidance has been issued to discourage their use.

While we did not detect any data leaks to Huawei-owned servers during our analysis, it is important to consider that SDKs can be updated remotely at any time. A future update could silently enable the collection of sensitive user data, such as location or device identifiers, potentially compromising the privacy of thousands of military-affiliated personnel who have downloaded these apps.

We responsibly disclosed our discovery of HMS Core to all relevant MMMapp developers to inform them of our findings. In response, one developer acknowledged the concern, expressed interest in its implications, and decided to take mitigation actions to remove the Huawei code. The app in question was "Hots&Cots" version 1.43.0 in the Google Play Store. Hots&Cots is a "Yelp-like" app that enables service members to report on the quality of living and dining conditions at military installations. The app's developer is a former Army non-commissioned officer [99]. The app has been popularized in military social media spaces and was the most popular app in our dataset obtained from online forum discussions (See Figure 1). The developer was especially concerned about the privacy implications of the Huawei SDK's inclusion in their app, given that the user base of Hots&Cots is exclusively U.S. service members. Notably, they escalated the matter by contacting the maintainers of the third-party SDK responsible for including the Huawei code (OneSignal). When they did not respond to their inquiry, Hots&Cots re-engineered their notification stack with another provider to ensure removal of the Chinese code from their app. Hots&Cots notified their users about the removal of HMS Core based on the findings in our study [56].

Russian-Developed MMMapps with Russian Third-Party Services. In another case, we identified two MMMapps developed by Russian companies that integrate Russian third-party services, such as Yandex Ads, for monetization. The current geopolitical climate, particularly with the U.S. imposing economic and technological sanctions on the Russian Federation in response to their invasion of Ukraine [110], makes these findings significant. Similar to the Huawei SDK, although network analysis did not detect active data leaks to Russian servers, the integration of Russian SDKs means that the apps have the potential to update their behavior at any time. This could result in covert data collection on thousands of military-affiliated users without notice.

In line with responsible disclosure best practices, we notified the developers whose apps incorporated SDKs with ties to China and Russia (both described as "adversarial" nations in the 2023 DoD Cyber Strategy), sharing our findings to ensure they were informed of both the inclusion and its potential consequences. We received no response from the Russian developers by the time of publication.

[5] https://reports.exodus-privacy.eu.org/en/trackers/333/

Table 3: Comparison of self-reported disclosures and undisclosed observed data practices

App Store	Category	Data Collection (% of Apps)	Data Sharing (% of Apps)
Google	(i) Self-reported	Contacts (5%) Health and Fitness Data (6%) Messages (9%) Location Data (19%) Financial Information (25%) App Activity (40%) Personal Information (42%) Device Identifier (42%)	Contacts (2%) Health and Fitness Data (2%) Messages (0%) Location Data (8%) Financial Information (3%) App Activity (10%) Personal Information (10%) Device Identifier (12%)
	(ii) Undisclosed	Location Data (0%) Address (5%) Phone Number (5%) Other Personal Info (5%) Email Address (10%) Name (12%)	Location Data (3%) Address (0%) Phone Number (0%) Other Personal Info (0%) Email Address (15%) Name (7%)
Apple	(i) Self-reported	App Activity (77%) Personal Information (43%) Device Identifiers (27%) Location Data (23%) Health and Fitness Data (20%) Financial Information (9%) Contacts (6%) Messages (1%)	*Not applicable*
	(ii) Undisclosed	Email Address (25%) Name (21%) Other Personal Info (18%) Phone Number (10%) Address (10%) Sexual Orientation (3%) Location Data (0%)	*Not applicable*

4.3.4 Privacy Disclosures Results

Table 3 overviews the comparison of self-reported disclosures and undisclosed data collection and sharing. We found that 40% of MMMapps contained at least one discrepancy, indicating that they collected/shared more data than they acknowledged.

Comparing against Data Safety Section. We compared the self-reported data collection and sharing practices of MMMapps, as disclosed in the Google Play Store's Data Safety section, with the actual data flows observed in our static, dynamic, and network analyses. The Data Safety section requires developers to specify what types of user data are collected and shared. This provides an opportunity to evaluate the accuracy of these claims.

To assess the accuracy of the disclosures, we extracted the self-reported data collection practices from each MMMapps 's listing and calculated the percentage of MMMapps that report data collection in each category. Similarly, developers are required to indicate whether they share data with third parties. Table 3 - Google - (i) summarizes the self-reported data collection and data-sharing disclosures.

To evaluate the accuracy of these self-reported disclosures, we compared them against our empirical findings from the network analysis. Specifically, we checked: (1) Whether an MMMApp collected PII but did not report it; and (2) whether an MMMApp transmitted data to third parties despite not disclosing data sharing.

The results revealed discrepancies between the claimed and actual data handling practices. Table 3 - Google - (ii) shows the percentage of MMMApps that failed to disclose collected or shared data for each type of PII that we check for during our network analysis.

Comparing against Privacy Labels. Since we compared observed data leaks against developer declarations on the Google Play Store via the Data Safety section, we conducted a similar comparison for iOS by reviewing the privacy details listed on the Apple App Store for the same set of apps. Specifically, we examined if the types of data collected or shared, based on our manual testing and network traffic analysis, were accurately reflected in the privacy labels provided by developers. Table 3 - Apple - (i) presents a summary of self-reported data collection disclosures.

As with Android, we checked for discrepancies between what was actually transmitted and what was declared, revealing whether the disclosures aligned with observed behaviors. The iOS results also revealed significant discrepancies between the claimed and actual data handling practices. Table 3 - Apple - (ii) shows the percentage of MMMApps that failed to disclose collected data for each type of PII that we check during our network analysis.

Answer to RQ1: Regarding data practices, MMMApps incorporate third-party SDKs and collect and transmit PII to third-party services. They also exhibit discrepancies between what developers disclose and what our analysis observes on both Android and iOS. Regarding code provenance characteristics, a significant portion of MMMApps contain code from foreign developers or foreign third-party libraries, and a non-trivial subset contain code from developers in countries the U.S. government has formally listed as adversarial. In one case, code was introduced transitively through a dependency chain without the app developer's awareness, and the developer removed the code after we informed them.

5 User Study with Military-Affiliated Participants

5.1 Online Survey Methodology

We describe the setup, recruitment, and analysis methods of our user study to understand how military-affiliated personnel perceive and attempt to mitigate the risks posed by MMMApps (RQ2).

5.1.1 Study Design

We conducted an online survey study administered through Qualtrics [118], consisting of five blocks, each grounded in our technical findings from Section 4.3. Each block and its corresponding questions were designed to map directly to our RQs, ensuring the survey would yield data sufficient to address each RQ. Prior to full deployment, we conducted a pilot study ($n = 10$) to validate this alignment. Pilot responses were included in our final results. On average, the survey took 31 minutes to complete, and our study was approved by our university's Institutional Review Board (IRB).

In Block 1 (device and app usage), participants reported their usage frequency for 24 MMMApps, consisting of the 15 most frequently mentioned MMMApps on Reddit and the 15 most downloaded MMMapps on the Google Play Store, with duplicates removed. These 24 MMMApps are representative of the broader MMMApp dataset, as we observed no statistically significant differences in data practices or code provenance characteristics between these MMMApps and the rest of the analyzed MMMApps. In Block 2 (perception of data sensitivity), participants ranked and rated their comfort with the 22 data types and permissions we observed being collected in real MMMApps, as well as their comfort with apps containing code from the four countries identified as "adversarial" in the DoD Cyber Strategy Summary [101]. In Block 3 (inferences of sensitive information and threat scenarios), participants reasoned about what adversaries could infer from collected data and what threat scenarios those inferences could enable. In Block 4 (mitigation strategies), participants evaluated seven recommendations across the federal, DoD, app store, and device levels that we proposed based on the data practices and code provenance characteristics identified by our technical analysis. In Block 5 (demographics), participants reported demographic information and details on their military affiliation.

5.1.2 Recruitment

We recruited participants through two channels. First, we used Prolific [117], an online research recruitment platform, to reach military-affiliated adults. Prolific's built-in screening filters allowed us to pre-screen for participants who self-identified as active-duty or veterans. Second, we used open recruitment, in which active-duty U.S. service members distributed the survey link to colleagues via email and internal messaging platforms. To minimize coercion risk, service members distributed the link only to individuals outside their supervisory authority and had no access to survey responses.

Participants were required to be aged 18 or older and to self-identify as military-affiliated (defined as U.S. active-duty service members, U.S. Reserve or National Guard members, U.S. veterans, family members of the aforementioned affiliations, or DoD civilian employees). All participants were compensated with $10.

In total, $n = 103$ participants completed the survey. The largest group identified as U.S. military veterans (48.5%), followed by active-duty service members (35.9%), family members (15.5%), Reserve or National Guard members (6.8%), and DoD civilian employees (1.9%). Regarding device usage, 70.9% of participants primarily use a personal device in their everyday lives, 27.2% use a mix of personal and government-issued devices, and only 1.9% rely primarily on a government-issued device, underscoring the relevance of MMMApp usage on personal devices outside institutional oversight. Detailed participant demographics can be found in Table 6 in the Appendices.

5.1.3 Analysis of Responses

Quantitative Analysis. For quantitative survey items (including Likert-scale comfort ratings, data-sensitivity rankings, foreign-SDK comfort ratings, mitigation-effectiveness ratings, and multiple-choice impact-domain selections), we report descriptive statistics (e.g., percentages and average ratings). For within-participant comparisons on ordinal measures, we apply rank-based nonparametric significance tests where appropriate to avoid distributional assumptions. For paired comparisons between two conditions, we used the

Wilcoxon signed-rank test [132, 151]. For item-level follow-up, we identified within-category items that consistently deviated from participants' rankings using within-participant Wilcoxon signed-rank tests with Benjamini-Hochberg FDR control [15]. For outcomes where each participant provided ratings across three or more conditions, we used the Friedman test [48] (reporting Kendall's W [70] as an effect size) followed by paired Wilcoxon post-hoc [132, 151] comparisons with Holm correction [55] to control family-wise error. We report adjusted p-values alongside effect sizes to emphasize magnitude in addition to statistical significance.

Qualitative Analysis. To characterize recurring patterns in participants' open-text responses, we used inductive qualitative coding and randomly sampled 20% of responses for each open-text question analyzed. For each question, two authors jointly developed a codebook defining each code. We use "code" and "category" interchangeably to refer to these codes. Both authors independently applied the codes to the same sampled dataset. Each response could receive multiple codes. We assessed agreement at the code level by converting each code into a binary present/absent label for each response and computing Cohen's κ [27] for each code. As a supplementary response-level measure of coding overlap, we also computed Jaccard similarity [30] between the two coders' assigned code sets for each response. Agreement was high across both metrics (mean $\kappa > 0.8$, mean Jaccard > 0.8). Authors discussed disagreements, refined the codebook, and produced a consensus-coded version of the sampled data. Given that agreement was high, suggesting that the codebook and its application were stable, the remaining 80% of the responses were coded by a single author. We report the percentage distribution of responses across codes and summarize representative instances to illustrate each code.

5.2 User Study Results

We present the results of our user study and answers to **RQ2a-2c**.

5.2.1 *RQ2a: Discomfort with MMMapps' Behavior and Code Provenance*

We analyzed participants' perceptions of data sensitivity, comfort with data collection, comfort with data collection by MMMApps, unknown third-parties, and foreign parties, and comfort with code from countries that the U.S. has listed as "adversarial".

Ranking Most Sensitive Data Types. Participants ranked 22 data types and permissions from most to least uncomfortable when collected. These were the data types and permissions we observed being collected in our app analysis. Notably, permissions dominated the top of the discomfort rankings. A Wilcoxon signed-rank test on participant-level median ranks confirmed that permissions were ranked significantly more uncomfortable than PII items overall (W=1749.5, p-value<0.001, Cohen's d=0.3304). Using within-participant category baselines with Benjamini-Hochberg FDR control, we identified items that consistently deviated from others in their category across $n = 103$ respondents: Address, Financial Information, Phone Number, Date of Birth, and the permission "Access Camera" were rated significantly more uncomfortable than other items in their categories (negative median deviation), whereas Gender, Branch, Age, Sexual Orientation, and the permissions "Access Health and Fitness Data" and "Make/Manage Phone Calls" were rated significantly less uncomfortable (positive median deviation).

Comfort with Data Collection by Data Type. Comfort ratings on a 5-point scale (extremely uncomfortable to extremely comfortable) reinforced the ranking results. Financial information elicited the strongest discomfort, with 90.3% of participants reporting being extremely or somewhat uncomfortable with its collection. One participant offered an explanation for this discomfort, saying "Foreign governments target financially vulnerable individuals to collect information in exchange for money." This is of particular note since we saw that the most widely used MMMApps we showed to participants were financial in nature. Location permissions followed closely: 83.5% were extremely or somewhat uncomfortable with fine location access, 81.6% with SMS/iMessages access, 81.5% with background location access, 78.6% with audio recording, and 78.7% with access to contacts. By contrast, participants expressed considerably more comfort with the collection of demographic data: 61.1% were somewhat or extremely comfortable with gender collection, 50.5% with age, and 52.6% with email address. Military-specific identifiers showed mixed results. 46.6% were uncomfortable with base/installation collection, while 50.5% were comfortable with branch collection, suggesting participants do not uniformly treat military-specific data as more sensitive.

Discrepancies Between MMMapp Behavior and Reported Uncomfortability. To assess the degree to which participants are (potentially unknowingly) using MMMApps that engage in data practices they find inappropriate, we cross-referenced each participant's self-reported app usage with their comfort ratings for the data types and permissions those MMMApps collect or request. Participants were asked to indicate how frequently they or a family member use each of 24 MMMApps (selected as described in Section 5.1) on a five-point scale (Always, Often, Sometimes, Rarely, Never). For each participant, we identified the subset of MMMApps they reported using at any frequency (Rarely through Always) and retrieved the PII types and permissions our technical analysis observed each of those MMMApps collecting or requesting. We then cross-referenced this against each participant's comfort ratings for those specific data types and permissions, collected later in the survey, in which participants rated their comfort with each of the 22 data types and permissions we observed across our technical analysis. A participant was considered to be using an MMMApp in a manner misaligned with their stated preferences if they reported using that MMMApp at any frequency and rated at least one of its observed data practices as extremely uncomfortable or somewhat uncomfortable. Ten participants answered never for all 24 MMMApps, leaving 93 participants for whom cross-referencing was possible. We found that 83.5% of participants use at least one MMMApp that collects or requests data they find inappropriate, while only 17 participants reported using no such MMMApps. Among participants who used at least one MMMApp they were uncomfortable with, the average number of such MMMApps per participant was 3.31 (SD=3.43), with an average of 3.88 apps (SD=5.02) per participant that did nothing they found inappropriate. This indicates that for most participants, uncomfortable MMMApp usage is not an isolated case but a pervasive condition. We also note that, because this analysis was conducted on only 24 of the 242 MMMApps in our dataset, these estimates likely substantially

underestimate the true misalignment between MMMApps' behavior and their users' privacy expectations.

Code Provenance Discomfort: MMMapps, Third Parties, and Foreign Parties. Participants were asked whether their discomfort would increase, remain the same, or decrease if each data type were (a) collected by an MMMApp, (b) shared with a foreign party, or (c) shared with an unknown third party. For foreign sharing, participants expressed dramatically elevated discomfort across all 22 data types: between 50.5% and 78.6% reported being more uncomfortable with foreign sharing, with the highest discomfort for financial information (78.6%), address (75.3%), camera access (75.5%), approximate location (75.8%), and contacts (75.8%). For third-party sharing, discomfort was similarly elevated, with 42.0%–74.0% of participants reporting increased discomfort. However, for MMMApp collection, the pattern reversed: for most data types, participants reported being equally or less uncomfortable with MMMApp collection than with their baseline. For example, for military base/installation, 49.0% reported being less uncomfortable and only 15.0% more uncomfortable. For branch, 52.0% reported less discomfort. Wilcoxon signed-rank tests confirmed this pattern is statistically significant across all 22 data types for both MMMApps vs. third-party and MMMApps vs. foreign comparisons (p-value<0.001 for all), while no significant difference was found between third-party and foreign sharing. This finding reveals a critical perception gap: military-affiliated personnel are significantly more comfortable with MMMApps collecting their data than when it is shared with third- or foreign parties. One participant illustrated this perception gap, saying "I trust military-affiliated apps and don't trust who I don't know." Conversely, our analysis demonstrates that 16% of MMMApps that collected some form of PII were transmitting that data to third-party services and over 15% of MMMApps contain foreign SDKs that could do the same.

Foreign Countries of Concern. Participants expressed near-universal discomfort with apps containing code from countries described as "adversarial" in the 2023 DoD Cyber Strategy [101]: 83.3% were extremely uncomfortable with apps containing code originating in the Democratic People's Republic of Korea, 83.3% with code originating in the Islamic Republic of Iran,, 82.4% with code originating in the Russian Federation, and 76.5% with code originating in the People's Republic of China. Participants explained their discomfort with responses such as "They're our adversary" and "Enemies of the USA". Between 27.2% and 29.1% of participants reported they would feel even more uncomfortable if they were military-affiliated (as opposed to a civilian), while the majority (50.5%–59.2%) reported equal discomfort regardless of affiliation. When asked whether specific MMMApps in our dataset contained foreign code, participants were largely uncertain: for most MMMApps, the majority responded "maybe." Hots&Cots (which our technical analysis confirmed contained a Huawei SDK) was identified as maybe containing foreign code by 54.4% of participants, while only 7.8% answered "yes." Similarly, MGRS UTM GPS and Defense & Military News, which had the highest "yes" rates (12.6% each), still saw the majority of participants respond "maybe" or "no." This uncertainty underscores a significant awareness gap: despite near-universal discomfort with foreign code in principle, participants were largely unsure if MMMApps actually contain it.

Popularity-Segmented Analysis. To examine whether discomforting data practices are concentrated in more or less popular MMMApps, we segmented MMMApps by download count into three tiers: popular (>5,000 downloads), moderately popular (1,000–5,000 downloads), and less popular (<1,000 downloads). Discomforting permissions were the most prevalent concern across all tiers, appearing in 63.41% of popular, 48.81% of moderately popular, and 41.03% of less popular apps. This was followed by discomforting PII collection (9.76%, 3.57%, and 10.26%, respectively), foreign third-party code (4.88%, 7.14%, and 8.55%), and foreign first-party code (0%, 2.38%, and 0.85%). Omnibus tests with pairwise post hoc comparisons revealed no statistically significant differences across popularity tiers for any of the aforementioned categories, suggesting these data practice concerns are distributed broadly rather than concentrated in any particular popularity segment.

Answer to RQ2a: Military-affiliated personnel find that the data practices and code provenance characteristics of many MMMApps are largely inappropriate. Additionally, sharing data with third- and foreign parties was rated significantly more uncomfortable relative to MMMApp collection alone. Furthermore, participants expressed near-universal discomfort with apps containing code from countries the U.S. government listed as "adversarial". Despite this discomfort, most participants use at least one MMMApp that engages in practices they are uncomfortable with, with the average participant using over three such MMMApps.

5.2.2 *RQ2b: Security Domains and Threat Scenarios*

We analyzed the open-text responses to identify sensitive information inferences and plausible threat scenarios related to data collected by MMMApps, following our qualitative analysis method. Figure 4 presents the coded categories and the share of participants mentioning each, for sensitive information inferences and perceived threats at personal, operational/unit, and national security levels.

Inferring Sensitive Information. Participants were asked what additional information a threat actor could infer from the 22 data types and permissions detected in our app analysis. The most commonly identified inference category was *Personal Network* (e.g., personal relationships and military associates) with 39.8%. *Pattern of Life* inferences were identified by 31.1% of participants, and *Identity Profile* construction was cited by 31.1% of participants. An equal proportion (31.1%) identified *Personal Vulnerability* inferences, recognizing that collected data could expose weaknesses (e.g., financial stress) that adversaries could exploit for coercion. *OPSEC* related inferences (e.g., deployment schedules) were identified by 30.1% of participants, and 19.4% of participants identified *Important Location* inferences (e.g., home or military base).

Security Domains at Risk. Participants were asked which security domains they believed could be impacted by adversarial exploitation of data collected through MMMApps. Personal safety was the most widely selected domain (91.3%), followed by operational/unit security (76.7%), and national security (67.0%). That almost two-thirds of participants identified national security as a threatened domain, alongside strong majorities for operational/unit security, underscores that military-affiliated participants view MMMApp data collection as a serious threat that spans beyond individual harm.

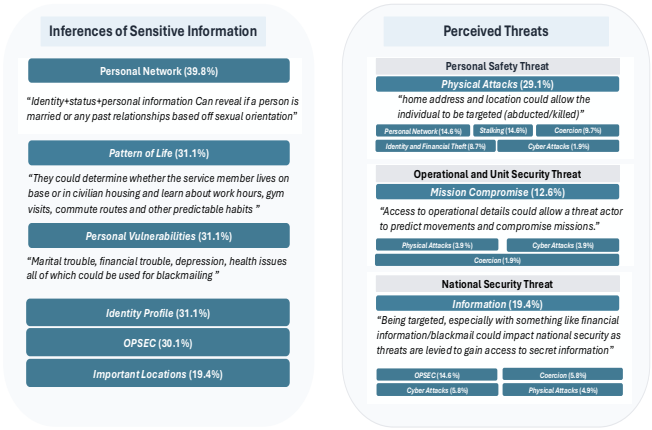

Figure 4: Participant-reported sensitive-information inferences (left) and perceived threat scenarios by impact level (right), showing category prevalence (percentage of participants) and representative exemplar quotes.

Perceived Threat Scenarios. For each security domain, participants were asked to infer what threat scenarios could occur if an adversary had access to any of the 22 data types and permissions detected in our app analysis. For personal safety, the most frequently described threat scenarios involved *Physical Attacks* (29.1%), whereas for operational and unit security, it involved *Mission Compromise* (12.6%). For example, adversaries could compromise a mission by setting up surprise attacks at a unit's rendezvous point. For national security, *Information* leaks (19.4%) were the most frequently described threat scenarios, with participants citing things like the exposure of large-scale classified military strategy. Together, these responses make clear that military-affiliated personnel do not perceive the data practices of MMMApps as abstract privacy concerns. They perceive them as actionable intelligence, whose exploitation carries consequences from the targeting of individual personnel to the destabilization of national security.

Answer to RQ2b: The majority of participants identified threat scenarios across all three security domains, demonstrating that military-affiliated participants believe the consequences of MMMApp data exposure extend beyond individual privacy, even reaching the highest levels of national defense. Participants identified a range of inferences adversaries could draw, from pattern-of-life analysis and personal network mapping to OPSEC violations and coercion scenarios, reflecting threat awareness consistent with the risks documented in our technical analysis. Participants also described perceived threat scenarios spanning the full spectrum of harm. For this population, the data practices of MMMApps are not an abstract privacy concern but a serious, multi-layered threat.

5.2.3 RQ2c: Mitigations

Based on the data practices and code provenance characteristics identified in our technical analysis, we developed seven recommendations across the federal, DoD, app store, and device levels and asked participants to evaluate each. The seven mitigations were: (1) a DoD-maintained approved app list for military-affiliated personnel; (2) DoD extension of privacy standards to MMMApps on personal devices; (3) app stores setting and enforcing rules for MMMApps; (4) a U.S. federal law restricting data brokers from buying or selling data about military-affiliated personnel; (5) a U.S. federal law requiring independent audits to verify the accuracy of privacy disclosures for MMMApps; (6) stricter bans on foreign code in MMMApps; and (7) in-phone warnings when foreign or unknown third-party code is present in an installed app. Therefore, to answer RQ2c, we analyzed participants' responses on the effectiveness and likelihood of adopting these mitigation strategies.

Perceived Effectiveness of Proposed Mitigations. Participants rated the effectiveness of seven mitigations on a 5-point scale. A Friedman test indicated that ratings differed across mitigations, p-value<0.001, $\chi^2(6, n = 103) = 53.937$, with a small effect size (Kendall's W = 0.0873). In-phone warnings when foreign or unknown third-party code is present were rated most effective (mean= 4.146) with 52.4% rating it extremely effective and 23.3% very effective. Wilcoxon signed-rank post-hoc test revealed that it was not significantly more effective than three other mitigations: U.S. federal law restricting data brokers from buying/selling military-affiliated data (mean=4.136), U.S. federal law requiring independent audits of privacy disclosures (mean=4.058), and stricter bans on foreign code in MMMApps (mean=4.039). These four mitigations were rated equally effective. A DoD-maintained approved app list, DoD extension of privacy standards to MMMApps, and app store enforcement rules were rated lower, though still rated as effective by the majority. Consistent with these modest between-mitigation shifts, the overall Friedman test effect size was small (Kendall's W = 0.0873).

Likelihood to Support Proposed Mitigations. Participants also rated the likelihood on a 5-point scale that they would adopt or support each mitigation. A Friedman test indicated that ratings differed across mitigations, p-value<0.001, $\chi^2(6, n = 103) = 22.225$, with a small effect size (Kendall's W = 0.036). In-phone warnings again ranked highest (mean=4.369), with 66.0% rating adoption/support as extremely likely and 16.5% somewhat likely. Wilcoxon signed-rank post-hoc test revealed the same pattern as effectiveness ratings: in-phone warnings were not significantly more likely to be adopted or supported than U.S. federal law restricting data brokers (mean=4.320), U.S. federal law requiring independent audits (mean=4.282), and stricter bans on foreign SDKs (mean=4.272). Participants rated all seven mitigations as more likely than unlikely for them to adopt or support. This pattern is consistent with the small effect size from the Friedman test (Kendall's W=0.036).

Answer to RQ2c: Participants expressed strong confidence in the recommendation for in-phone warnings, rating it as most effective and likely for them to adopt/support, with federal data broker restrictions, independent privacy audits, and foreign SDK bans rated equally highly.

6 Discussion

Risk Present in Observed Data Practices. Our analysis reveals that MMMApps represent a significant risk. Many MMMApps collect or transmit PII (e.g., 5% collected military base information). These risks are amplified by the sheer prevalence of third-party SDKs

(e.g., 59% of MMMApps use Google Firebase) which send data to external parties. Additionally, 19% of MMMApps transmit data to first-party/third-party servers. We also found cases of discrepancies in disclosed data collection/sharing. These findings corroborate existing literature [37, 82, 98, 124] in highlighting how the mobile app ecosystem allows sensitive information to flow outside the user's control. When applied to an at-risk demographic such as military-affiliated personnel, these systemic weaknesses have consequences well beyond consumer privacy. They create new attack surfaces that adversaries may exploit for strategic advantage.

User Expectations, Threat Perceptions, and Structural Gaps. Our user study reveals how military-affiliated personnel interpret and internalize data practices of MMMApps. Participants described potential threat scenarios made possible by data aggregation, including pattern-of-life inference and mission compromise.

Participants expressed strong discomfort with third-party data sharing, foreign code, and cross-border data flows, yet reported comparatively greater comfort when similar data collection occurred within apps explicitly branded for military use. This asymmetry suggests a form of contextual or institutional trust that may not align with the technical realities of SDK integration, transitive dependencies, and downstream data transmission. The greater comfort with MMMApps mirrors broader evidence that app labeling and descriptive framing often shape users' trust and privacy perceptions beyond the technical realities of the tool [2].

More broadly, the problem appears structural rather than informational. Consistent with prior findings that S&P guidelines for at-risk populations can sometimes be underdeveloped and inadequate [10, 146], 65.1% of our military-affiliated participants reported receiving little to no institutional guidance regarding personal app usage, and even those who had received guidance questioned its adequacy (72.2%). The most strongly supported mitigations were systemic in nature, including stronger app store oversight, independent audits, and federal regulatory safeguards, rather than individual behavioral adjustments. This aligns with prior work that shows technical mitigations alone are insufficient, and that non-technical mitigations are equally necessary to best protect vulnerable groups [49, 52, 140]. These findings indicate that the risks identified in our empirical analysis stem from ecosystem-level governance gaps and supply chain opacity more than user ignorance.

Implications for Governance. The risks associated with MMMApps' data practices in raise questions for governance at the federal, DoD, and app store levels. These implications are not derived solely from technical analysis. They are reinforced by participant perceptions that current protections are insufficient and that meaningful safeguards must operate at structural levels. See Table 9 for a summary of the mitigations and their rationale/benefits.

Our findings suggest several regulatory intervention avenues that merit further consideration. First, the DoD could explore whether and to what extent existing privacy and security standards should apply to personal apps that explicitly market themselves to military populations, particularly given the limited institutional guidance currently reported by personnel. Second, app store operators might consider whether additional review processes or design principles are warranted for developers building apps aimed at sensitive or at-risk communities (e.g., strengthened scrutiny of third-party SDK integrations, clearer disclosure requirements, or mechanisms to reveal transitive dependencies[6] that developers may be unaware of). Third, policymakers could expand the current governance landscape (See Appendix E) by examining whether current data broker regulations adequately protect sensitive populations, including military-affiliated personnel, especially in light of participant concerns about downstream data aggregation and inference risks.

Finally, given the inconsistencies observed between stated and actual data practices, future legislation regarding app privacy policies could consider mechanisms, such as independent audits, to improve the accuracy and accountability of mobile app disclosures. Privacy policies represent a complementary avenue for future inquiry in this regard. While they are less conspicuous, they are more legally binding than Data Safety sections, as deceptive privacy policies may trigger FTC investigation and penalties. These considerations involve complex tradeoffs and require careful evaluation by government and military stakeholders to assess feasibility, proportionality, and potential unintended consequences.

7 Limitations

U.S.-Centric Scope. Our study is intrinsically U.S.-centric, due to the apps analyzed and the population from which we recruited participants. As a result, our findings reflect legal, regulatory, operational, and cultural factors specific to the U.S. military ecosystem. Future work can extend this analysis to military personnel and other at-risk populations in different countries to identify cross-national similarities and differences in privacy expectations, threat perceptions, and exposure to supply chain risks.

App Dataset. While we identified apps from two sources (Google Play and online forums), some important MMMApps may be missing. Several factors contribute to this gap, such as search queries (i.e., keywords) not covering all possible variations, Google Play's search and ranking algorithms prioritizing popular but often irrelevant apps, and apps with lower engagement on online forums or fewer reviews on Google Play not surfacing in our data. Additionally, despite our filtration classifier's high recall rate, it may overlook relevant apps with vague descriptions. Nevertheless, we made a concerted effort to curate a diverse set of MMMApps that would allow us to identify concerning data practices.

Program Analysis. One potential limitation of our analysis is the presence of false negatives, where certain data leaks may have gone undetected. This can occur due to encryption or encoding of data in transit, making it difficult to extract and analyze network traffic effectively. While our network analysis attempts to bypass SSL pinning, this technique is not always effective, meaning that some encrypted transmissions may not have been intercepted. We also report that we were unable to analyze 30 MMMApps because they required login credentials. Additionally, another possible source of false negatives stems from the reliance on keyword matching for UI element detection. We may have missed particular instances where PII is displayed under different terminology.

False positives can arise in dynamic analysis when UI elements contain keywords resembling PII but are unrelated to actual data collection. For example, an app may have labels or placeholders

[6] This is illustrated by the Hots&Cots case study in Section 4.3.3.

containing words such as "Name" or "Email" without actually requesting user input. However, since our methodology confirms PII collection only when the corresponding data is observed in network traffic, these false positives do not affect our final findings. Dynamic analysis serves solely to guide which PII types to monitor during network analysis, while network analysis provides the ground truth for determining what data is actually collected and transmitted.

Another limitation arises from the static analysis of permissions, which relies on the Android manifest file. The manifest lists declared permissions, but those deemed "dangerous" by Android also require user approval at runtime. Some apps declare permissions they never use, leading to potential false positives in our analysis, while others prompt users to grant access to sensitive data such as location without any clear functional justification.

One gap in our pipeline is the inability to detect back-end data sharing. Many MMMApps collect data locally, but transmit it only to their own servers, where subsequent sharing with third-party entities may occur. Since our network traffic analysis is limited to on-device communications, we are unable to observe what happens once data reaches the MMMApp 's back-end, meaning true data sharing behaviors may be underrepresented in our findings.

Finally, our attribution of code origin relies on the self-reported developer addresses listed in the Google Play Store, which do not always reflect the true geographic origin of an app's code or its developers due to the potential for falsification. Importantly, this suggests our findings on the prevalence of foreign and "adversary-originating" code likely represent a *lower bound* of reality.

User Study. Our user study has several limitations. First, our recruited participants were obtained through online recruitment platforms and snowball sampling, which may introduce self-selection bias and limit generalizability. Second, participants' responses reflect stated perceptions and hypothetical reasoning rather than observed real-world behavior under operational constraints. Third, participants evaluated data practices in a survey context rather than through direct interaction with apps. Despite these limitations, we argue that our results retain ecological validity because the survey instruments were grounded in empirically observed app behaviors, incorporated real-world MMMApps examples, and reflected threat scenarios articulated by participants themselves. Additionally, we made a best effort to ensure a diverse set of military-affiliated participants. Future work should incorporate longitudinal or behavioral studies, expand recruitment across additional service branches and roles, and examine how perceptions evolve in response to changes across federal legislation, DoD regulations, and app store policies.

8 Conclusion

This paper presents the first systematic investigation of the privacy risks posed by MMMApps to military-affiliated personnel, combining large-scale app analysis with a user study. Our analyses reveal that MMMApps' data practices and code provenance are misaligned with what military-affiliated personnel find appropriate. For example, we found that 83.5% of our user study participants use MMMApps that engage in the very practices they find unacceptable. These findings underscore a critical, previously undocumented mismatch between the privacy expectations of MMMApps' target users and the actual practices of these apps, motivating protective action from policymakers, developers, and the military community alike.

Ethical Considerations

The data we handle in our app analysis encompasses online communications, Android apps, and iOS apps. We collected only non-identifiable information from the online forum threads. We did not collect any account-related metrics of users. Whenever necessary, we created demo alias user accounts for our analysis pipeline and did not rely on existing authentic personas.

For the user study, we obtained IRB approval from our institution prior to conducting any data collection. The study was deemed exempt because participant identities could not be ascertained from the survey responses. Participants were presented with an online informed consent form before beginning the survey, which explained the study's purpose, procedures, and their rights, including the right to withdraw at any time without penalty. We did not collect any personally identifiable information within the survey itself. Compensation-related contact information was collected in a separate, unlinked form and deleted immediately after compensation was issued. All survey responses are stored in encrypted, access-controlled storage.

Acknowledgments

We would like to express our gratitude to the anonymous reviewers whose feedback improved the quality of this manuscript. We would also like to thank Jessica Dawson for valuable discussions about this work and for helping bring it to fruition.

This research was sponsored by the United States Military Academy through the Army Cyber Institute and was accomplished under a Cooperative Agreement, grant number W911NF-24-2-0213. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the United States Army or the United States Government.

Disclosure. The authors used generative AI tools to revise the text and correct typos, grammatical errors, and awkward phrasing.

References

[1] Ajin Abraham. 2015. MobSF. https://github.com/MobSF/Mobile-Security-Framework-MobSF

[2] Omer Akgul, Ruba Abu-Salma, Wei Bai, Elissa M Redmiles, Michelle L Mazurek, and Blase Ur. 2021. From secure to military-grade: Exploring the effect of app descriptions on user perceptions of secure messaging. In *Workshop on Privacy in the Electronic Society*.

[3] Mir Masood Ali, David G Balash, Monica Kodwani, Chris Kanich, and Adam J Aviv. 2023. Honesty is the Best Policy: On the Accuracy of Apple Privacy Labels Compared to Apps' Privacy Policies. https://doi.org/10.48550/arXiv.2306.17063

[4] Benjamin Andow, Samin Yaseer Mahmud, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Serge Egelman. 2020. Actions speak louder than words: Entity-Sensitive privacy policy and data flow analysis with PoliCheck. In *USENIX Security Symposium*.

[5] Steven J. Arango. 2022. Data Brokers Are a Threat to National Security. https://www.usni.org/magazines/proceedings/2022/december/data-brokers-are-threat-national-security

[6] Alireza Ardalani, Joseph Antonucci, and Iulian Neamtiu. 2024. A Study of Personal Information Leaks in Mobile Medical, Health, and Fitness Apps. In *IADIS International Journal on WWW/Internet*.

[7] Alireza Ardalani, Joseph Antonucci, and Iulian Neamtiu. 2024. Towards Precise Detection of Personal Information Leaks in Mobile Health Apps. https://doi.org/10.48550/arXiv.2410.00277

[8] Ioannis Arkalakis, Michalis Diamantaris, Serafeim Moustakas, Sotiris Ioannidis, Jason Polakis, and Panagiotis Ilia. 2024. Abandon All Hope Ye Who Enter Here: A Dynamic, Longitudinal Investigation of Android's Data Safety Section. In *USENIX Security Symposium*.

[9] U.S. Army. 2021. Two new Army apps you will want. https://www.army.mil/article/245156/two_new_army_apps_you_will_want

[10] Arjun Arunasalam, Habiba Farrukh, Eliz Tekcan, and Z Berkay Celik. 2024. Understanding the security and privacy implications of online toxic content on refugees. In *USENIX Security Symposium*.

[11] Noah Ashman. 2020. Outed by Advertisements: How LGBTQ Internet Users Present a Case for Federal Data Privacy Legislation. https://scholarsbank.uoregon.edu/items/6c4ec607-3c0b-40d1-92fa-84776545fab7

[12] Michael Backes, Sven Bugiel, and Erik Derr. 2016. Reliable third-party library detection in android and its security applications. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[13] David G Balash, Mir Masood Ali, Xiaoyuan Wu, Chris Kanich, and Adam J Aviv. 2022. Longitudinal analysis of privacy labels in the apple app store. https://doi.org/10.48550/arXiv.2206.02658

[14] Felix Beierle, Vinh Thuy Tran, Mathias Allemand, Patrick Neff, Winfried Schlee, Thomas Probst, Johannes Zimmermann, and Rüdiger Pryss. 2020. What data are smartphone users willing to share with researchers? Designing and evaluating a privacy model for mobile data collection apps. In *Journal of Ambient Intelligence and Humanized Computing*.

[15] Yoav Benjamini and Yosef Hochberg. 1995. Controlling the false discovery rate: a practical and powerful approach to multiple testing. In *Journal of the Royal Statistical Society: Series B (Methodological)*.

[16] Kitti Bessenyei, Banuchitra Suruliraj, Alexa Bagnell, Patrick McGrath, Lori Wozney, Anna Huguet, Bernice Simone Elger, Sandra Meier, and Rita Orji. 2021. Comfortability with the passive collection of smartphone data for monitoring of mental health: an online survey. In *Computers in Human Behavior Reports*.

[17] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt. 2018. Third Party Tracking in the Mobile Ecosystem. In *ACM Conference on Web Science*.

[18] Wasja Brunotte, Larissa Chazette, Lukas Kohler, Jil Klunder, and Kurt Schneider. 2022. What about my privacy? Helping users understand online privacy policies. In *International Conference on Software and System Processes and International Conference on Global Software Engineering*.

[19] Duc Bui, Yuan Yao, Kang G Shin, Jong-Min Choi, and Junbum Shin. 2021. Consistency analysis of data-usage purposes in mobile apps. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[20] Dell Cameron. 2026. The Pentagon Knew Enemies Could Track Troops' Phones for Years. Now They Are. https://www.wired.com/story/the-pentagon-knew-enemies-could-track-troops-phones-for-years-now-they-are/

[21] Dell Cameron and Dhruv Mehrotra. 2025. Google Ad-Tech Users Can Target National Security 'Decision Makers' and People With Chronic Diseases. https://www.wired.com/story/google-dv360-banned-audience-segments-national-security/

[22] Jiaxun Cao, Hiba Laabadli, Chase H Mathis, Rebecca D Stern, and Pardis Emami-Naeini. 2024. "I Deleted It After the Overturn of Roe v. Wade": Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era. In *CHI Conference on Human Factors in Computing Systems*.

[23] Fred Cate. 2010. The Limits of Notice and Choice. In *IEEE Symposium on Security and Privacy (S&P)*.

[24] National Cyber Security Centre. 2022. Threat report on application stores. https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf

[25] Quan Chen, Panagiotis Ilia, Michalis Polychronakis, and Alexandros Kapravelos. 2021. Cookie Swap Party: Abusing First-Party Cookies for Web Tracking. In *Web Conference*.

[26] Bruce Chojnacki, Zachary Daher, and Alexander Master. 2025. Poster: Unseen Threats: The Privacy Risks of Data Collection in Government Fleet Vehicles. In *USENIX Symposium on Vehicle Security and Privacy*.

[27] Jacob Cohen. 1960. A coefficient of agreement for nominal scales. In *Educational and Psychological Measurement*.

[28] Federal Communications Commission. 2020. FCC Designates Huawei and ZTE as National Security Threats. https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats

[29] U.S. Congress. 2023. 10 U.S. Code 2224: Defense Information Assurance Program. https://uscode.house.gov/view.xhtml?req=(title:10%20section:2224%20edition:prelim

[30] Wikipedia contributors. 2026. Jaccard index. https://en.wikipedia.org/wiki/Jaccard_index

[31] Aldo Cortesi, Maximilian Hils, and Thomas Kriechbaumer. 2010. mitmproxy. https://mitmproxy.org/

[32] Joseph Cox and Dhruv Mehrotra. 2025. The Murky Ad-Tech World Powering Surveillance of US Military Personnel. https://www.wired.com/story/rtb-location-data-us-military/

[33] Gitanjali Das, Cynthia Cheung, Camille Nebeker, Matthew Bietz, and Cinnamon Bloss. 2018. Privacy policies for apps targeted toward youth: descriptive analysis of readability. In *JMIR mHealth and uHealth*.

[34] Jessica Dawson. 2021. Microtargeting as Information Warfare. In *The Cyber Defense Review*.

[35] Manila Devaraja and Sameer Patil. 2025. Understanding User Prioritization and Comprehension of Smartphone Permissions. In *Proceedings of the ACM on Human-Computer Interaction*.

[36] PRAW Developers. 2025. PRAW: The Python Reddit API Wrapper Documentation. https://praw.readthedocs.io/en/stable/index.html

[37] Michalis Diamantaris, Serafeim Moustakas, Lichao Sun, Sotiris Ioannidis, and Jason Polakis. 2021. This sneaky piggy went to the android ad market: Misusing mobile sensors for stealthy data exfiltration. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[38] Defense Information Systems Agency DoD Cyber Exchange. 2023. DoD Cyber Hygiene: Information Security Helps Protect from Cybersecurity Threats. https://www.aetc.af.mil/News/Article-Display/Article/3431998/dod-cyber-hygiene-information-security-helps-protect-from-cybersecurity-threats/

[39] Alexander Dolphin. 2023. Putting Pride In Privacy. https://www.openrightsgroup.org/blog/putting-pride-in-privacy/

[40] Bharathi Donku, Shahriar Rahman Khan, Tariqul Islam, and Raiful Hasan. 2025. Discrepancies in Mobile App Permissions: Exploring Transparency and User Awareness in the Android Ecosystem. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*.

[41] DPC. 2020. Guidance Note: Cookies and Other Tracking Technologies. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

[42] Dtmilano. v23.4.0. AndroidViewClient. https://github.com/dtmilano/AndroidViewClient

[43] Xiaolin Du, Zhemin Yang, Jiapeng Lin, Yinzhi Cao, and Min Yang. 2024. Withdrawing is believing? detecting inconsistencies between withdrawal choices and third-party data collections in mobile apps. In *IEEE Symposium on Security and Privacy (S&P)*.

[44] FJEDI. 2025. WebProxyTool. https://apps.apple.com/us/app/webproxytool-inspect-network/id1578538118

[45] Center for Naval Analyses. 2023. China's National Security Laws and Their Implications Beyond China's Borders. https://www.cna.org/quick-looks/2023/China-national-security-laws-implications-beyond-borders.pdf

[46] Jaclyn Fox. 2024. The New Insider Threat: How Commercially Available Data can be used to Target and Persuade. In *The Managing Insider Risk & Organizational Resilience (MIROR) Journal*.

[47] Jaclyn Fox, Alexander Master, Nicolas Starck, and Jessica Dawson. 2023. Death by a Thousand Cuts: Commercial Data Risks to the Army. Army Cyber Institute. https://doi.org/10.55682/EGQK7666

[48] Milton Friedman. 1937. The use of ranks to avoid the assumption of normality implicit in the analysis of variance. In *Journal of the American Statistical Association*.

[49] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *USENIX Security Symposium*.

[50] Christine Geeng and Alexis Hiniker. 2021. LGBTQ privacy concerns on social media. https://arxiv.org/pdf/2112.00107

[51] Jiawei Gu, Xuhui Jiang, Zhichao Shi, Hexiang Tan, Xuehao Zhai, Chengjin Xu, Wei Li, Yinghan Shen, Shengjie Ma, Honghao Liu, et al. 2024. A Survey on LLM-as-a-Judge. https://doi.org/10.48550/arXiv.2411.15594

[52] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *CHI Conference on Human Factors in Computing Systems*.

[53] Robert Hammer. 2024. Military Health System Using Mobile Apps for Warfighter Readiness. https://www.health.mil/News/Articles/2024/10/24/Military-Health-System-Using-Mobile-Apps-for-Warfighter-Readiness

[54] Nicholas Harrell, Alexander Master, Nicolas Starck, and Daniel Eerhart. 2025. Tactics and Techniques of Information Operations: Gaps in US Response to Counter Malign Influence. In *International Conference on Cyber Warfare and Security*.

[55] Sture Holm. 1979. A simple sequentially rejective multiple test procedure. In *Scandinavian Journal of Statistics*.

[56] Hots&Cots. 2025. Hots&Cots Notification System Changes. https://www.hotscots.app/transparency

[57] Jeremy Hsu. 2018. The Strava Heat Map and the End of Secrets. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

[58] Louis M Hsu and Ronald Field. 2003. Interrater agreement measures: Comments on Kappan, Cohen's Kappa, Scott's π, and Aickin's α. https://psycnet.apa.org/doi/10.1207/S15328031US0203_03

[59] Kit Huckvale, John Torous, and Mark E. Larsen. 2019. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. In *JAMA Network Open*.

[60] Hiroki Inayoshi, Shohei Kakei, and Shoichi Saito. 2024. Detection of Inconsistencies between Guidance Pages and Actual Data Collection of Third-party

SDKs in Android Apps. In *IEEE/ACM International Conference on Mobile Software Engineering and Systems*.
[61] Apple Inc. 2025. App Privacy Details on the App Store. https://support.apple.com/en-us/102399
[62] Google Inc. 2025. Provide information for Google Play's Data safety section. https://support.google.com/googleplay/android-developer/answer/10787469
[63] Leonardo Horn Iwaya, M Ali Babar, Awais Rashid, and Chamila Wijayarathna. 2023. On the privacy of mental health apps: An empirical investigation and its implications for app development. In *Empirical Software Engineering*.
[64] Akshath Jain, David Rodriguez, Jose M Del Alamo, and Norman Sadeh. 2023. Atlas: Automatically detecting discrepancies between privacy policies and privacy labels. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*.
[65] Shanzay Javaid, Yusra Kayani, and Ezequiel Donovan. 2025. COPPA VIOLATION CRISIS: Verifiable Parental Consent Failures In Mobile Apps. In *Pixalate*.
[66] Haojian Jin, Minyi Liu, Kevan Dodhia, Yuanchun Li, Gaurav Srivastava, Matthew Fredrikson, Yuvraj Agarwal, and Jason I Hong. 2018. Why are they collecting my data? inferring the purposes of network traffic in mobile apps. https://doi.org/10.1145/3287051
[67] Karen Jowers. 2026. 'Scary and silencing': Troops, families receive threats from foreign bad actors. https://www.militarytimes.com/news/pentagon-congress/2026/05/29/scary-and-silencing-troops-families-receive-threats-from-foreign-bad-actors/
[68] John H Junior. 2021. Huawei Mobile Services Core (HMS Core): Replacement of Google's developer libraries, here's everything you need to know. https://www.huaweicentral.com/hms-core/
[69] Daniel Jurafsky and James H Martin. 2019. Speech and language processing 3rd edition. https://web.stanford.edu/~jurafsky/slp3/
[70] Maurice G Kendall and B Babington Smith. 1939. The problem of m rankings. In *The Annals of Mathematical Statistics*.
[71] Julien Khaleghy. 2015. SerpAPI. https://serpapi.com/google-play-api
[72] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2023. Comparing privacy labels of applications in android and iOS. In *Workshop on Privacy in the Electronic Society*.
[73] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2023. The overview of privacy labels and their compatibility with privacy policies. https://arxiv.org/abs/2303.08213
[74] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2024. Unpacking privacy labels: A measurement and developer perspective on google's data safety section. In *USENIX Security Symposium*.
[75] Mugdha Khedkar, Ambuj Kumar Mondal, and Eric Bodden. 2024. Do Android App Developers Accurately Report Collection of Privacy-Related Data?. In *ACM International Conference on Automated Software Engineering Workshops*.
[76] Mugdha Khedkar, Michael Schlichtig, and Eric Bodden. 2024. Advancing Android Privacy Assessments with Automation. In *IEEE/ACM International Conference on Automated Software Engineering Workshops*.
[77] Simon Koch, Benjamin Altpeter, and Martin Johns. 2023. The OK is not enough: A large scale study of consent dialogs in smartphone applications. In *USENIX Security Symposium*.
[78] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. 2022. Keeping privacy labels honest. In *Privacy Enhancing Technologies Symposium (PETS)*.
[79] Konrad Kollnig and Nigel Shadbolt. 2022. TrackerControl: Transparency and Choice around App Tracking. https://doi.org/10.21105/joss.04270
[80] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2021. Are iphones really better for privacy? comparative study of ios and android apps. https://doi.org/10.2478/popets-2022-0033
[81] Brian Krebs. 2024. The Global Surveillance Free-for-All in Mobile Ad Data. https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data/
[82] Beau Kujath, Jeffrey Knockel, Paul Aguilar, Diego Morabito, Masashi Crete-Nishihata, and Jedidiah R Crandall. 2024. Analyzing Prominent Mobile Apps in Latin America. In *Free and Open Communications on the Internet*.
[83] Ravie Lakshmanan. 2020. Security Researchers Uncover iOS SDK Involved in Ad Fraud and Data Collection. https://thehackernews.com/2020/08/ios-sdk-ad-fraud.html
[84] Paloma Secunda Laretto, Anne Zimmerman, and Olivia Bowers. 2025. Blog - the dark side of wearables: A potential fertility surveillance network. https://bioethicstoday.org/blog/the-dark-side-of-wearables-a-potential-fertility-surveillance-network/#
[85] Mary Lee, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, and Bryce Downing. 2020. The Internet of Bodies: Opportunities, Risks, and Governance. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3200/RR3226/RAND_RR3226.pdf
[86] Douglas J Leith. 2021. Mobile handset privacy: Measuring the data ios and android send to apple and google. In *Security and Privacy in Communication Networks (SecureComm)*.
[87] Douglas J Leith. 2022. What Data Do The Google Dialer and Messages Apps On Android Send to Google?. In *Security and Privacy in Communication Systems*.
[88] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I Hong. 2022. Understanding challenges for developers to create accurate privacy nutrition labels. In *CHI Conference on Human Factors in Computing Systems*.
[89] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Faith Cranor. 2023. Data safety vs. app privacy: Comparing the usability of android and ios privacy labels. https://doi.org/10.56553/popets-2024-0047
[90] Google LLC. 2026. Google Fit: Activity Tracking. https://play.google.com/store/apps/details?id=com.google.android.apps.fitness
[91] C. Todd Lopez. 2025. 'Zero Trust' Architecture Could Prevent Adversary Data Theft, Protect Warfighters. https://www.defense.gov/News/News-Stories/Article/Article/4078717/zero-trust-architecture-could-prevent-adversary-data-theft-protect-warfighters/
[92] Alexander Master, Jaclyn Fox, Nicolas Starck, Maxwell Love, and Benjamin Allison. 2025. Tracking The Trackers: Commercial Surveillance Occurring on U.S. Army Networks. Army Cyber Institute. https://doi.org/10.48550/arXiv.2602.12388
[93] Dhruv Mehrotra and Dell Cameron. 2024. Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany. https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/
[94] Mark Meng, Chuan Yan, Yun Hao, Qing Zhang, Zeyu Wang, Kailong Wang, Sin Gee Teo, Guangdong Bai, and Jin Dong. 2024. A large-scale privacy assessment of android third-party SDKs. https://doi.org/10.48550/arXiv.2409.10411
[95] Lily Newman. 2023. You Can't Trust App Developers' Privacy Claims on Google Play. https://www.wired.com/story/google-play-data-safety-forms-mozilla-research/
[96] Military.com News. 2025. Data Breach Prompts Coast Guard to Take Personnel and Pay System Offline. https://www.military.com/daily-news/2025/02/17/data-breach-prompts-coast-guard-take-personnel-and-pay-system-offline.html
[97] Trung Tin Nguyen, Michael Backes, Ninja Marnau, and Ben Stock. 2021. Share first, ask later (or never?) studying violations of GDPR's explicit consent in android apps. In *USENIX Security Symposium*.
[98] Trung Tin Nguyen, Michael Backes, and Ben Stock. 2022. Freely given consent? studying consent notice of third-party tracking and its violations of GDPR in android apps. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*.
[99] Patty Nieberg. 2023. Army Veteran Launches 'Hots & Cots,' a Yelp for Enlisted Life. https://taskandpurpose.com/military-life/former-soldier-created-app-review-facilities/
[100] Department of Defense. 2005. 32 CFR § 631.11 - Off-limits establishments and areas. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-V/subchapter-I/part-631/subpart-B/section-631.11
[101] The Department of Defense. 2023. 2023 DOD Cyber Strategy Summary. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF
[102] U.S. Department of Defense. 2014. DoD Instruction 8100.02: Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/810002p.pdf
[103] U.S. Department of Defense. 2014. DoD Instruction 8500.01: Cybersecurity. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf
[104] U.S. Department of Justice. 2025. Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons. https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern
[105] National Institute of Standards and Technology. 2019. NIST SP 800-163 Rev. 1: Vetting the Security of Mobile Applications. https://doi.org/10.6028/NIST.SP.800-163r1
[106] National Institute of Standards and Technology. 2020. NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5
[107] National Institute of Standards and Technology. 2023. NIST SP 800-124 Rev. 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise. https://doi.org/10.6028/NIST.SP.800-124r2
[108] Office of the Law Revision Counsel. 2022. 50 USC 3334d: Cyber Protection Support for the personnel of the intelligence community in positions highly vulnerable to cyber attack. http://uscode.house.gov/view.xhtml?req=%28title%3A50+section%3A3334d+edition%3Aprelim%29
[109] Office of the Law Revision Counsel. 2025. 15 USC 45: Unfair methods of competition unlawful; prevention by Commissions. https://uscode.house.gov/view.xhtml?req=(title:15%20section:45%20edition:prelim)
[110] U.S. Department of the Treasury. 2025. Ukraine-/Russia-related Sanctions. https://ofac.treasury.gov/sanctions-programs-and-country-information/ukraine-russia-related-sanctions

[111] Kate O'Keeffe and Maggie Eastland. 2026. Lawmakers Urge US Agencies to Rein In Huawei's American Unit. https://news.bloomberglaw.com/tech-and-telecom-law/lawmakers-urge-us-agencies-to-rein-in-huaweis-american-unit
[112] OWASP. v2.15.0. Zed Attack Proxy (ZAP). https://www.zaproxy.org/
[113] Federica Paci, Jacopo Pizzoli, and Nicola Zannone. 2023. A comprehensive study on third-party user tracking in mobile applications. In *International Conference on Availability, Reliability and Security*.
[114] Xiang Pan, Yinzhi Cao, Xuechao Du, Boyuan He, Gan Fang, Rui Shao, and Yan Chen. 2018. FlowCog: Context-aware semantics extraction and analysis of information flow leaks in android apps. In *USENIX Security Symposium*.
[115] Google Play. 2026. USAA Mobile. https://play.google.com/store/apps/details?id=com.usaa.mobile.android.usaa
[116] Christian Preti, Nicholas Harrell, and Alexander Master. 2026. Privacy Under Pressure: Assessing Online Commercial Surveillance Countermeasures and Gaps. In *European Conference on Cyber Warfare and Security*.
[117] Prolific.com. 2026. Prolific. https://www.prolific.com/
[118] qualtrics.com. 2026. Qualtrics. https://qualtrics.com/
[119] Abdelrahman Ragab, Mohammad Mannan, and Amr Youssef. 2024. "Trust Me Over My Privacy Policy": Privacy Discrepancies in Romantic AI Chatbot Apps. In *European Symposium on Security and Privacy Workshops (EuroS&PW)*.
[120] Selvakumar Ramachandran, Andrea Dimitri, Maulahikmah Galinium, Muhammad Tahir, Indirajith Viji Ananth, Christian H Schunck, and Maurizio Talamo. 2017. Understanding and granting android permissions: A user survey. In *International Carnahan Conference on Security Technology (ICCST)*.
[121] Ramakrishnan Raman, Khyati R Nirmal, Anita Gehlot, Snehal Trivedi, Dimple Sain, and R Ponnusamy. 2022. Detecting Android Malware and Sensitive Data Flows Using Machine Learning Techniques. In *Conference on Contemporary Computing and Informatics (IC3I)*.
[122] Ole André Vadla Ravnås. 2014. Frida. https://frida.re/
[123] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, Phillipa Gill, et al. 2018. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In *NDSS Symposium*.
[124] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *USENIX Security Symposium*.
[125] Brian Reed. 2021. Many finance mobile apps fail to protect data. https://www.paymentsjournal.com/many-finance-mobile-apps-fail-to-protect-data/
[126] The Register. 2025. Amazon Sued for Snarfing Sensitive Data from Third-Party Apps. https://www.theregister.com/2025/01/30/amazon_sued_for_snarfing_sensitive/
[127] Caroline Roberts, Jessica ME Herzing, Jimena Sobrino Piazza, Philip Abbet, and Daniel Gatica-Perez. 2022. Data privacy concerns as a source of resistance to complete mobile data collection tasks via a smartphone app. In *Journal of Survey Statistics and Methodology*.
[128] David Rodriguez, Joseph A Calandrino, Jose M Del Alamo, and Norman Sadeh. 2025. Privacy Settings of Third-Party Libraries in Android Apps: A Study of Facebook SDKs. https://usableprivacy.org/static/files/rodriguez_pets_2025.pdf
[129] David Rodriguez, Jose M Del Alamo, Celia Fernández-Aller, and Norman Sadeh. 2024. Sharing is not always caring: Delving into personal data transfer compliance in Android apps. https://ieeexplore.ieee.org/document/10379677
[130] Michaela Rogers, Colleen Fisher, Parveen Ali, Peter Allmark, and Lisa Fontes. 2023. Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. In *Trauma, Violence & Abuse*.
[131] Leah Namisa Rosenbloom. 2022. Activists want better, safer technology. https://doi.org/10.48550/arXiv.2209.01273
[132] SciPy. 2026. wilcoxon. https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.wilcoxon.html
[133] Tim Sh. 2025. Everyone knows your location: tracking myself down through in-app ads. https://timsh.org/tracking-myself-down-through-in-app-ads/
[134] Justin Sherman. 2021. Data Brokers and Sensitive Data on U.S. Individuals. https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-individuals/
[135] Justin Sherman, Hayley Barton, Aden Klein, Brady Kruse, and Anushka Srinivasan. 2023. Data Brokers and the Sale of Data on US Military Personnel. https://techpolicy.sanford.duke.edu/wp-content/uploads/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf
[136] Peng Shi and Jimmy Lin. 2019. Simple bert models for relation extraction and semantic role labeling. https://doi.org/10.48550/arXiv.1904.05255
[137] Jac W Shipp. 2026. Digital Force Protection for Expeditionary Land Forces: An Early-Warning Framework for Mission Command Resilience. In *The Cyber Defense Review*.
[138] Harman Singh. 2025. From Swipe to Scare: Data Privacy and Cyber Security Concerns in Dating Apps. https://thecyphere.com/blog/privacy-security-concerns-in-dating-apps/
[139] SINTEF-9012. 2018. Sintef-9012/grindr-privacy-leaks: Report and raw data about privacy leaks in Grindr. https://github.com/SINTEF-9012/grindr-privacy-leaks
[140] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers. In *USENIX Security Symposium*.
[141] Enno Steinbrink, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. Digital privacy perceptions of asylum seekers in Germany: An empirical study about smartphone usage during the flight. In *Proceedings of the ACM on Human-Computer Interaction*.
[142] Borislav Tadic, Markus Rohde, Dave Randall, and Volker Wulf. 2023. Design evolution of a tool for privacy and security protection for activists online: cyberactivist. In *International Journal of Human–Computer Interaction*.
[143] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *CHI Conference on Human Factors in Computing Systems*.
[144] Jenny Tang, Hannah Shoemaker, Ada Lerner, and Eleanor Birrell. 2021. Defining privacy: How users interpret technical terms in privacy policies. In *Proceedings on Privacy Enhancing Technologies*.
[145] Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky. 2021. Mobile health and privacy: cross sectional study. In *British Medical Journal Publishing Group*.
[146] Kurt Thomas, Patrick Gage Kelley, Sunny Consolvo, Patrawat Samermit, and Elie Bursztein. 2022. "It's common and a part of being a content creator": Understanding How Creators Experience and Cope with Hate and Harassment Online. In *CHI Conference on Human Factors in Computing Systems*.
[147] Army Times. 2025. Official Army app had Russian code, might have harvested user data. https://www.armytimes.com/news/your-army/2022/11/15/official-army-app-had-russian-code-might-have-harvested-user-data/
[148] Lionel Sujay Vailshery. 2025. Google Play Store - statistics & facts. https://www.statista.com/topics/9929/google-play-store/
[149] Sara Vannini, Ricardo Gomez, and Bryce Clayton Newell. 2020. "Mind the five": Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations. In *Journal of the Association for Information Science and Technology*.
[150] Yin Wang, Ming Fan, Junfeng Liu, Junjie Tao, Wuxia Jin, Haijun Wang, Qi Xiong, and Ting Liu. 2024. Do as you say: Consistency detection of data practice in program code and privacy policy in mini-app. https://doi.org/10.1109/TSE.2024.3479288
[151] Frank Wilcoxon. 1992. Individual comparisons by ranking methods. In *Breakthroughs in statistics: Methodology and distribution*.
[152] Saskia Witteborn. 2021. Data privacy and displacement: A cultural approach. In *Journal of Refugee Studies*.
[153] Yuxi Wu, Jacob Logas, Devansh Ponda, Julia Haines, Jiaming Li, Jeffrey Nichols, W Keith Edwards, and Sauvik Das. 2025. Modeling End-User Affective Discomfort With Mobile App Permissions Across Physical Contexts. In *Symposium on Usable Security and Privacy (USEC)*.
[154] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. 2022. Lalaine: Measuring and characterizing non-compliance of apple privacy labels at scale. https://www.usenix.org/conference/usenixsecurity23/presentation/xiao-yue
[155] Yue Xiao, Adwait Nadkarni, and Xiaojing Liao. 2023. Enhancing Transparency and Accountability of TPLs with PBOM: A Privacy Bill of Materials. In *Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*.
[156] Jesse A. Yarbrough. 2025. Caveat Oculus: Data Brokers, Surveillance Capitalism, and the Threat to Homeland Security. http://doi.org/10.2139/ssrn.6442825
[157] Zhonghao Yu, Sam Macbeth, Konark Modi, and Josep M Pujol. 2016. Tracking the trackers. In *International Conference on World Wide Web (WWW)*.
[158] Jared Zabaldo. 2022. 10 Military Apps Worth Checking Out. https://www.usamm.com/blogs/news/10-military-apps-worth-checking-out
[159] Yifan Zhang, Zhaojie Hu, Xueqiang Wang, Yuhui Hong, Yuhong Nan, XiaoFeng Wang, Jiatao Cheng, and Luyi Xing. 2024. Navigating the Privacy Compliance Maze: Understanding Risks with Privacy-Configurable Mobile SDKs. In *USENIX Security Symposium*.
[160] Shoshana Zuboff. 2020. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

A App Dataset Curation Details

Below, we present additional details of our app dataset curation.

A.1 Labeling Guide

In this section, we present the labeling guide we used to determine if an app is marketed to military-affiliated users.

(1) Read the app description. Does the app explicitly mention that its services cater to U.S. military members (e.g., "Best app for soldiers"). If yes, label it a MMMApp and proceed to the next app. If not, proceed to Step 2.
(2) Does the app explicitly mention that its services cater to U.S. military veterans (e.g., "Voted best choice for military veterans"). If yes, label it a MMMApp and proceed to the next app. If not, proceed to Step 3.
(3) Does the app description explicitly discuss content that is related to U.S. military (e.g., military news, military uniform guide). If yes, label it a MMMApp and proceed to the next app. If not, proceed to Step 4.
(4) Label it as not a MMMApp.

We provide a concrete example of each of these criteria using our full MMMApp dataset. For example, "Army Leader Smart Cards" provides soldiers and Army leaders with quick, mobile access to basic Army smart-card reference material for training, readiness, and professional knowledge refreshment, directly falling under Criterion (1). Similarly, the "Official Navy PFA" app provides sailors with Navy physical fitness assessment guidance and tools, directly falling under Criterion (1). The "MyVetBENEFITS" app helps veterans identify benefits and services they may be eligible for based on their service background, directly falling under Criterion (2). Similarly, the "VA: Health and Benefits" app provides veterans with access to VA health care, benefits, claims, and payment information, directly falling under Criterion (2). The "Defense & Military News" app provides news and updates related to defense and military affairs, directly falling under Criterion (3). Similarly, the "US Military Rank & Reference" app provides reference material on U.S. military ranks, insignia, and related military information, directly falling under Criterion (3). Finally, an app like "Google Fit" [90] does not explicitly mention services for U.S. military members or veterans, nor does its description discuss U.S. military-related content. Therefore, after failing Criteria (1)–(3), it falls under Criterion (4) and is not considered a MMMApp.

A.2 Google Play Store App Collection

We present here additional details of our Play Store app collection.

Table 4: Comparison of different classifiers. We prioritize the recall metric, because we use this classifier to filter before further manual analysis.

Classifier	Accuracy	Precision	Recall	F1-Score
LLM-as-a-Judge, Binary {0,1}	0.91	0.87	**0.79**	0.82
LLM-as-a-Judge, Range [0,1]				
Threshold = 0.5	0.9352	0.8721	**0.8614**	0.8673
Threshold = 0.8	0.9390	0.8812	**0.8557**	0.8698
Threshold = 0.1	0.8250	0.5802	**0.9182**	0.7071
Keyword Classifier (v1)	0.7205	0.4321	**0.5230**	0.4728
Keyword Classifier (v2)	0.7842	0.5289	**0.8572**	0.6525
BERT Classifier	0.91	0.88	**0.94**	0.89

A.2.1 Filtering MMMapps via Classifier

To ensure comprehensive coverage in collecting MMMApps, we conducted additional data collection by querying Google Play using an expanded set of keywords. Here, we opted for a classifier that retrieves candidate apps (serving as a filter) before further manual inspection. This binary text-based classifier classifies the app description as a potential MMMApp or irrelevant. We made this design choice for two reasons. First, when authors labeled the initial dataset, we discovered a large diversity of MMMApps (e.g., apps helping for military exam prep, military dating apps, military uniform guides). Thus, we hypothesized that developing a highly accurate classifier solely based on app descriptions would be challenging, as it could also lead to missing important MMMApps. Second, given the substantial imbalance in apps retrieved via keyword searches on Google Play, where only one fifth of the retrieved apps are truly military-focused, introducing an automated filtering mechanism to identify candidate apps would significantly reduce the required manual effort. Thus, we opted for a machine learning classifier that prioritized recall. This reduces false negatives and minimizes the likelihood of missing relevant MMMApps to serve as a filtration step before further manual review.

We experimented with several classifiers to identify MMMApps. First, we implemented two keyword-based classifiers: one that searched for any of our 55 curated keywords in app descriptions (v1), and another that restricted matches to military branch names (v2). Second, we evaluated an LLM-as-a-Judge approach [51], using a static prompt (Appendix A.2.2) and testing both binary and continuous outputs with thresholding. Finally, we fine-tuned a BERT-based classifier on our manually labeled seed dataset using an 80/20 stratified train–test split.

Table 4 summarizes the performance of these classifiers. The fine-tuned BERT model achieved the best recall (0.94), which is our primary evaluation metric, and best F1-Score. For this reason, we adopt the BERT classifier in our study.

A.2.2 Prompts Used in LLM-as-a-Judge

The static prompt used for the "binary LLM-as-a-Judge":

> You are a classifier - you will be given an instruction how to classify an app description. Does it represent an app that someone in the USA military (any branch e.g., Army, Marine Corps, Navy, Air Force, Space Force, and Coast Guard) or veteran can use? If so, please return 1. If not please return 0. If the app is for military of another country (e.g., canada) please return 0. If the app is about any military fitness, please return 0. If an app has use cases for military but is most commonly used by the general population (e.g., a recruiting app that is not targeted towards military) return 0. If the app description is about a game that relates to the military please return 0. Your output should only be the integers 0 or 1, nothing else

The static prompt used for the "range LLM-as-a-Judge":

> You are a classifier - you will be given an instruction on how to classify an app description. Does it represent an app that someone in the USA military (any branch e.g., Army, Marine Corps, Navy, Air Force, Space Force and Coast Guard) or veteran can use? Please return a decimal score between 0 to 1, with 1 representing a stronger likelihood of the app being related to USA Military. If the app is for the military of another country (e.g., Canada) the likelihood should be closer to 0. If the app is about any military

fitness, the likelihood should be closer to 0. If an app has use cases for the military but is most commonly used by the general population (e.g., a recruiting app that is not targeted towards only the military, like Indeed, LinkedIn, etc.), the likelihood should be closer to 0. If the app description is about a game that relates to the military, the likelihood should be closer to 0. If the description mentions military ranks, military dating, connecting military units and associations, assisting military personnel with language learning, personal use for service members, military transition support, veterans, National Guard, or if the app is an official U.S. military app developed by e.g., the Department of Veterans Affairs (VA), it should be rated closer to 1. Your output should only be a decimal number between 0 or 1 (up to two decimal points), nothing else.

A.2.3 Saturation After Automated Approach

After four iterations, we found no new MMMApps, as seen in Table 5.

Table 5: Batch Data Collection from Play Store

Batch	New Unique Apps	Candidates	True MMMApps
Batch 1	267	21	20
Batch 2	245	18	6
Batch 3	202	12	6
Batch 4	196	5	0

A.3 Online Forum App Collection

We identified seven military-focused subreddits based on consultation with active service members: `r/military`, `r/army`, `r/USMC`, `r/navy`, `r/airforce`, `r/spaceforce`, and `r/uscg`. Using the PRAW Python library [36], we queried each subreddit with app-related keywords (e.g., "app", "android", "app store", "google playstore", "playstore"), retrieving up to 1,000 results per keyword and collecting associated metadata (e.g., comments, upvotes).

A.3.1 LLM-as-a-Judge to Extract Apps

Across all queries, we retrieved 1,500 unique threads. Of these, 29% were non-functional or could not be processed via the API (e.g., image-only threads or invalid links), leaving 71% functional threads for analysis. We used GPT-4-Turbo in an LLM-as-a-Judge configuration to extract app mentions from each thread, including nested comments. To validate extraction performance, we compared LLM-identified apps against manually identified apps from the 10% sampled threads, observing 99% recall.

Threads were processed in 16 intervals of approximately 96–97 threads each. After each interval, two authors reconciled app annotations. Cohen's Kappa exceeded 0.8 across intervals.

A.3.2 Saturation of Apps

Figure 5 illustrates the decreasing number of newly identified unique apps across batches, with batches 14–16 yielding zero new apps, indicating saturation.

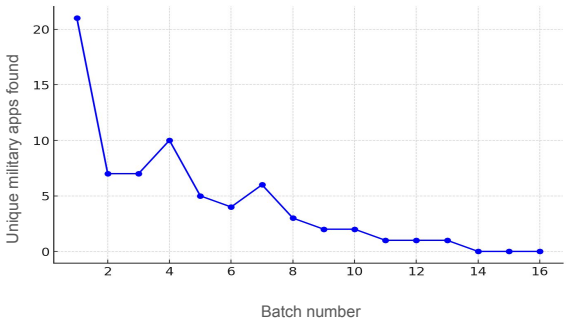

Figure 5: Saturation reached when processing online forum threads in batches.

A.3.3 Prompt for Reddit Data Collection

You are given a reddit post's title, text and comments concatenated. Please find if the given texts are talking about some apps. If the posts/comments talk about some particular app/apps, please return the name of those apps separated by comma, otherwise, return 0.

B Additional User Study Detail

Table 6 shows detailed demographics of our participants.

Table 6: Survey participant demographics (n = 103)

Demographic Data	n	%
*Military Status**		
U.S. Military Veteran	50	48.5%
U.S. Active Duty	37	35.9%
Family Member of U.S. Service Member/Veteran	16	15.5%
U.S. Reserve or National Guard Member	7	6.8%
U.S. DoD Civilian Employee	2	1.9%
Branch		
Army	51	49.5%
Air Force	22	21.4%
Navy	20	19.4%
Marine Corps	5	4.9%
Prefer not to say	4	3.9%
Coast Guard	1	1.0%
Gender		
Male	64	62.1%
Female	36	35.0%
Prefer not to say	3	2.9%
Age Group		
18–24	14	13.6%
25–34	28	27.2%
35–44	27	26.2%
45–54	17	16.5%
55–64	10	9.7%
65+	5	4.9%
Prefer not to say	2	1.9%
Race/Ethnicity		
White	66	64.1%
Black or African American	18	17.5%
Asian	10	9.7%
Prefer not to say	4	3.9%
Other	3	2.9%
American Indian or Alaska Native	1	1.0%
Native Hawaiian or Pacific Islander	1	1.0%
Primary Device Usage		
Personal device	73	70.9%
Mix of personal and government-issued devices	28	27.2%
Government-issued device	2	1.9%

*Military status was a multi-select item; therefore, percentages in that category exceed 100%.

C MMMapps Containing Code Originating in Foreign Countries

We share the 56 MMMapps that contain first-party and/or third-party code originating in a country other than the United States in Tables 7 and 8. Some of these countries are "adversarial" countries: a subset of foreign countries explicitly determined as a "threat" in the 2023 U.S. DoD Cyber Strategy [101]. We mark these 21 MMMapps with †. Additionally, some MMMapps both originate in a foreign country and use a third-party library that originates in a foreign country. We mark these six MMMapps in Table 8 with a ‡.

D Mitigations' Rationale and Benefit

Below, in Table 9, we present the rationale and benefit behind each of the mitigations we proposed.

E Data Policies on Device Use, Location Sharing, and Online Activity

Below, we present a summary of various laws, regulations, and policy directives that relate to data collection and privacy in mobile apps. We examine U.S. federal laws and Department of Defense directives about mobile device use and data security (Table 10), sector-specific privacy laws such as HIPAA, GLBA, and ECPA and their relevance to military populations (Table 11), and the growing body of state-level consumer privacy statutes that regulate mobile apps, data brokers, and third-party sharing (Table 12).

Table 7: MMMapps Originating in a Foreign Country

App Name	APK	Country
Marine Corps Ringtones	com.coolapps.marinecorpsringtones	Argentina
Military GPS Survival Kit	com.ekik.tacticalnavigation	Armenia
MilitaryCupid: Military Dating	com.cupidmedia.wrapper.militarycupid	Australia
ASVAB Test Prep 2025	co.spurry.asvab	Canada
FUNKER530 - Military Videos	com.funker530.funker530app	Canada
Veterans Yoga Project	veterans.yoga.project	Canada
Military Ringtones	com.yesringtonesapps.militaryringtonesfree	Colombia
Army Dictionary	com.lifenet.army	Greece
Army Cadet College (ACC) App	com.edurev.armycadetcollege	India
Best Marine : Online Shopping	co.shopney.bestmarine	India
eMarinersApp - Marine Uniform	com.emarinersapp	India
MGRS UTM GPS	info.yogantara.yytestgps	Indonesia
Military Sounds	com.akadtech.militarysounds	Indonesia
West Point AOG Gift Shop	com.celerant.ios.westpointtest	Pakistan
Military Training Exercises	com.watervideosoftware.militarytraining	Spain
Mgrs & Utm Map	com.zahidcataltas.mgrsharita	Turkey
Military Dating App - AGA	com.agadating.military	Turkey
Military Science Master	com.outmaster.militarymaster	Turkey
AFV Recognition	com.watchandshoot.afvrecognition	UK
AirForces Monthly Magazine	com.triactivemedia.airforcesmonthly	UK
MBR - Military Broadcast Radio	com.kevtucker.mbr	UK
Military Ethics	com.corvita.cme	UK
U.S. Military Ranks	com.jonis.militaryrank	UK
Military Dictionary	com.sultonuzdev.militarydic	Uzbekistan
ASVAB Practice Test 2025	com.sima.asvab	Vietnam
ASVAB Practice Test Prep 2025	pp.asvab	China †
ASVAB Test 2025 prep	asvab.test.prep.us	China †
ASVAB® Practice Test 2025	asvab.exam	China †

We followed a responsible disclosure procedure for any app with ties to an "adversarial" country.
† Indicates an "adversarial" country, per the 2023 DoD Cyber Strategy.

Table 8: MMMapps Using a Third-Party Library that Originates in a Foreign Country

App Name	APK	Country	Third-Party Lib.
Air Force Falcons	com.cbs.sportsapp.android.afa	Canada	Tapstream
ASVAB Practice Test 2024 Prep	com.bestfungames.asvab	Germany	Adjust
ASWB Exam Prep LCSW Test 2025	com.bestfungames.aswb	Germany	Adjust
Best Marine : Online Shopping‡	co.shopney.bestmarine	Germany	Adjust
Military Bible Challenge	net.militarybiblechallenge.app	India	CleverTap
Defense & Military News	com.briox.riversip.android.tech.defense	India	InMobi
The ACFT App	com.acftapp.acftlite	India	InMobi
ASVAB Marines Mastery	com.hltcorp.marines	Israel	AppsFlyer
ASVAB Mastery: ASVAB Test	com.hltcorp.asvab	Israel	AppsFlyer
ASVAB Navy Mastery	com.hltcorp.navy	Israel	AppsFlyer
ASVAB Practice for Dummies	com.gwhizmobile.dummiesasvab	Israel	AppsFlyer
Best Marine : Online Shopping‡	co.shopney.bestmarine	Israel	AppsFlyer
MilitaryCupid: Military Dating‡	com.cupidmedia.wrapper.militarycupid	Israel	AppsFlyer
VET Tv	com.vettv	Israel	AppsFlyer
Defense & Military News	com.briox.riversip.android.tech.defense	Israel	ironSource
The ACFT App	com.acftapp.acftlite	Israel	ironSource
Military Training Exercises‡	com.watervideosoftware.militarytraining	Switzerland	AppBrain
GI Jobs	com.gijobs.publication	UK	Countly
Best Marine : Online Shopping‡	co.shopney.bestmarine	UK	UXCam
Alabama National Guard	bfac.android.aiguard	China †	HMS** Core
Alaska National Guard	bfac.android.alaskanationalguard	China †	HMS Core
FUNKER530 - Military Videos‡	com.funker530.funker530app	China †	HMS Core
Hots&Cots***	com.rob.hotscots	China †	HMS Core
MBR - Military Broadcast Radio‡	com.kevtucker.mbr	China †	HMS Core
MCM Organization	me.rtrt.app.mcma	China †	HMS Core
MS National Guard Outreach	bfac.android.msoutreach	China †	HMS Core
Michigan National Guard	bfac.android.michigannationalguard	China †	HMS Core
Military Sounds‡	com.akadtech.militarysounds	China †	HMS Core
Military Training Exercises‡	com.watervideosoftware.militarytraining	China †	HMS Core
NY National Guard	bfac.android.nynationalguard	China †	HMS Core
Naval Library Navy Army ASVAB	com.navallibrary.navallibrary	China †	HMS Core
Defense & Military News	com.briox.riversip.android.tech.defense	China †	Mintegral
Army PRT - U.S. Army APFT Calc	com.vandersw.armypft	China †	RjFun
Corps PT Calculator CFT & PFT	com.vandersw.marinepft	China †	RjFun
Air Force Falcons	com.cbs.sportsapp.android.afa	Russia †	Pushwoosh
US Forces awards	ru.asmkery.awardsusa	Russia †	Yandex Ad
US military ranks	ru.asmkeri.ranksusa	Russia †	Yandex Ad

We followed a responsible disclosure procedure for any app with ties to an "adversarial" country.
† Indicates an "adversarial" country, per the 2023 DoD Cyber Strategy.
‡ Indicates the MMMapps that also originate in a foreign country and therefore also appear in Table 7.
** Huawei Mobile Services
***At the time of publication, this app no longer contains signatures for this third-party SDK.

Table 9: Mitigations' Rationale and Benefit

Mitigation	Rationale	Benefit
In-phone warnings when third-party code is present in an installed app	After passing the initial app store review process, developers can update their app with new SDKs, causing one-time checks and audits to miss them [24]. An in-phone warning reflects the app's current state, catching code introduced in later updates.	Gives users a live signal to act on (e.g., revoke permissions, delete data, or uninstall) when a previously trusted app introduces new data disclosure risk after an update.
U.S. federal law restricting data brokers from buying or selling data about military-affiliated personnel	Few data broker rules already exist, and do not provide at-risk populations like service members with protections [135]. Legal restrictions could close this gap.	Limits demand; even if an app leaks data, brokers cannot legally buy, sell, or share the data, shrinking the market and limiting the damage a malicious app disclosure can do.
U.S. federal law requiring independent audits to verify the accuracy of privacy disclosures for MMMApps	Developer disclosures are self-reported and frequently inaccurate [3, 95]. Independent audits enable enforcement mechanisms and provide external pressure to improve.	Forces disclosures to match actual behavior, making it harder for apps to hide what they collect or share and improve user trust.
Stricter regulation on foreign code in MMMApps	A notable share of MMMApps include foreign or "adversarial"-nation code, which military-affiliated personnel are uncomfortable with (see Section 4.3.2). Foreign SDKs can also be updated remotely to begin collecting data at any time.	Removes a direct supply chain path for adversaries to acquire military-personnel data, reducing OPSEC and force protection exposure.
DoD-maintained approved app list for military-affiliated personnel	The DoD has the time, resources, and expertise to vet code origin, dependencies, and data practices which individual users do not, and can evaluate apps that are unsafe for use. Military services already do this in other domains, such as designating "off-limits establishments" around military installations [100].	Allows personnel to rely on vetted governmental guidance rather than an app's marketing, and shifts the burden away from the individual.
DoD extension of privacy standards to MMMApps on personal devices	The DoD already maintains privacy and security standards for mobile devices (see Table 10). Extending them specifically to MMMApps would make these standards more robust.	Extends existing protections to where the risk exists and moves the data safety burden from individuals onto established standards.
App stores setting and enforcing rules for MMMApps	App store enforcement stops dangerous apps at the source, before they reach users, rather than relying on users to avoid them.	Reduces how many risky apps ever reach an app store, reducing how much users need to police their own choices.

Table 10: Summary of relevant U.S. federal law, regulations, and guidance on data sharing/collection/processing and device security for the military

Policy Category	Policy Summary	Source
FTC Oversight of Consumer Data Practices	Entities collecting or processing consumer data must not engage in deceptive or unfair practices. These entities must accurately disclose how user data is collected, used, and shared.	Title 15 USC 45 [109]
Defense Information Assurance Implementation	Mandates the establishment of a Department of Defense information assurance program to protect and defend critical defense information, systems, and networks during all operations.	Title 10 USC 2224, Section (a) [29]
System Security Objectives	Sets continuous information security requirements by ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of essential Defense data and systems.	Title 10 USC 2224, Section (b) [29]
Training and Preparedness Exercises	Requires the conduct of cyber defense exercises to train DoD personnel to recognize and respond to information warfare threats.	Title 10 USC 2224, Section (c) [29]
Cyber Protection for Military Personnel	Cyber protection support must be provided to military personnel in vulnerable positions to protect their personal devices and accounts.	Title 50 USC 3334d, Section (b)(1) [108]
Limitations on Cyber Protection	Cyber protection support does not permit the use of personal devices for official business, nor does it extend to senior personnel using personal devices for government work.	Title 50 USC 3334d, Section (d) [108]
Scope of Cyber Protection Support	Cyber protection services include training, guidance, and assistance against cyber attacks.	Title 50 USC 3334d, Section (c) [108]
Department of Justice (DOJ) Rules on Personal Data	The DOJ restricts or prohibits certain data transactions that could allow countries of concern or covered persons to access sensitive U.S. personal or government-related data and threaten national security. These include limits on collection or transfer of geolocation data near federal buildings or military installations.	EO 14117, ref Title 5 USC 804(2) [104]
DoD Commercial Mobile Device Restrictions	Prohibits unauthorized use of commercial wireless devices and services within DoD networks.	DoDI 8100.02, Enclosure 3 [102]
DoD Cybersecurity Requirements for Mobile Use	Requires that all DoD systems—including mobile applications—undergo cybersecurity review and risk-based controls.	DoDI 8500.01 Enclosure 3 [103]
DoD Data Privacy Expectations for Military Personnel	The DoD Cyber Hygiene Initiative emphasizes cybersecurity training for military personnel to protect classified, controlled unclassified information (CUI), and personally identifiable information (PII) from cyber threats. The Cyber Awareness Challenge educates personnel on recognizing cyber threats, implementing best practices such as multi-factor authentication (MFA), encryption, and secure device usage, and maintaining operational security (OPSEC) by limiting the exposure of sensitive data online. The policy stresses social media caution, disabling geolocation features, and avoiding public WiFi for military communications. By enforcing these measures, the DoD aims to enhance overall cyber resilience.	DoD Cyber Exchange, Defense Information Systems Agency (DISA) [38]
DoD Zero Trust Architecture Implementation	Zero Trust Architecture (ZTA) is a DoD effort that implements microsegmentation and enforces constant authentication — to prevent adversary data exploitation and misuse, protect warfighters, and secure DoD information systems.	U.S. Department of Defense [91]
NIST Guidelines for Secure Mobile App Development	The National Institute of Standards and Technology (NIST) provides guidelines for building secure *mobile applications*, especially those targeting enterprise, government, or sensitive sectors. *NIST SP 800-163* outlines app vetting and testing protocols, while *SP 800-124* provides device-level management expectations, and *SP 800-53* offers a comprehensive control framework for *data protection* and *privacy*.	NIST SP 800-163 [105], SP 800-124 [107], SP 800-53 [106]

Table 11: Sector-specific federal privacy laws and their potential applicability to military members

Policy Category	Policy Summary	Source	Potential Applicability to Military Members
HIPAA and Business Associate Rules	Protects the security and privacy of protected health information (PHI). Applies to covered entities and their third-party business associates (e.g., cloud services for supporting patient apps).	45 C.F.R. Parts 160–164	Applies to veterans or active-duty service members using TRICARE apps, VA health portals, or telehealth tools.
GLBA – Financial Privacy and Safeguards	Requires financial institutions to protect customer financial data and notify users of information sharing with non-affiliates. Opt-outs and safeguards are required.	15 U.S.C. §§ 6801–6809	Applies to military members using mobile banking, loan, or financial planning apps linked to military banks.
COPPA – Children's Online Privacy	Requires child-directed online services to obtain verifiable parental consent before collecting personal information (e.g., names, device IDs, location) from children under 13.	15 U.S.C. §§ 6501–6506	Applies to dependents of military families using games or educational apps on base-issued devices.
ECPA – Electronic Communications Privacy Act	Prohibits unauthorized interception, disclosure, or access to communications (in transit or stored). Applies to many service providers and app developers.	18 U.S.C. §§ 2510–2712	Applies to military members using dating, messaging, or social media apps where communication privacy is important.

Table 12: High-Level Summaries of U.S. State Consumer Privacy Laws

State*	Scope and Key Provisions for Mobile Applications
California CCPA/CPRA	Grants rights to access, delete, correct, and opt out of sale/sharing of personal information. *Mobile apps* must disclose data practices, honor GPC, and obtain consent for processing sensitive personal information. *Data brokers* register annually and comply with reporting and deletion request requirements, and *data sharing* must be transparent.
Colorado CPA	Provides opt-outs for the sale of personal data, profiling, sales, and targeted ads. *Mobile apps* need clear notices, in-app opt-outs, and user rights. *Data brokers*, or similar, may fall under controller rules; *data sharing* must be limited by contracts.
Connecticut CTDPA	Adds child protections and opt-outs for sales and targeted ads. *Mobile apps* and other platforms should respect browser signals and user rights. *Data brokers*, or similar maybe controllers; *data sharing* requires purpose alignment and contracts.
Delaware DPDPA	Expands protections for minors. *Mobile apps* must obtain parental consent for those under 13 and for some under 17 years of age, limit tracking, and honor GPC. *Data brokers* or similar follow controller rules; *data sharing* must allow opt-outs.
Indiana IDPA	Mirrors Colorado/Virginia. Controllers, which may include *mobile apps*, must allow access, correction, deletion, and opt-outs. *Data brokers* act as controllers; *data sharing* needs transparency and contracts.
Iowa ICDPA	Grants limited rights (access and deletion). Controllers, which may include *mobile apps*, must support these rights. *Data brokers* not addressed; *data sharing* rules are less regulated.
Kentucky KCDPA	Provides access, deletion, portability, and opt-outs for sale and targeted ads (without profiling opt-out). *Data brokers* covered as controllers; data sharing lightly regulated, no universal opt-out.
Maryland MODPA	Grants core rights and opt-outs. Controllers (which may include *mobile apps*) must disclose practices, honor global signals, and obtain sensitive data consent. *Data brokers* or similar and *processors* face strict disclosure and contractual duties.
Minnesota MCDPA	Adds rights to contest profiling and core consumer rights. *Mobile apps* must disclose practices, honor signals, and obtain consent for sensitive data. *Data brokers*, or similar as controllers and *processors* must follow controller-processor contracts.
Montana MTCDPA	Emphasizes purpose limits and transparency. Controllers, which may include *mobile apps*, must allow opt-outs and easy user requests. *Data brokers* may be covered; *data sharing* rules are more now.
Nebraska NDPA	Grants standard rights plus strict processing safeguards. Controllers, which may include *mobile apps*, must provide notices, honor signals, and restrict collection. *Data brokers* or similar are controllers; *data sharing* and *processors* need contracts.
New Hampshire Privacy Act	Provides core rights with low applicability thresholds. Requires clear, platform-agnostic privacy notices, honors universal opt-out signals, and mandates opt-in for sensitive data. Controllers and processors face disclosure and contractual duties.
New Jersey NJDPA	Covers nonprofits and grants access, correction, deletion, and opt-outs. Controllers, which may include *mobile apps*, must support privacy settings and honor signals. *Data brokers* or similar as controllers; *data sharing* must meet notice and opt-out rules.
Oregon OCPA	Provides robust rights with strict data collection limits. *Mobile apps* must disclose third-party sharing and support opt-outs. *Data brokers* register; *data sharing* categories must be disclosed.
Rhode Island RIDTPPA	Covers broad rights and unique notice duties for all online services. Controllers, which may include *mobile apps*, must disclose all recipients and support opt-outs. *Data brokers* register annually; *processors* and *controllers* must meet audit and transparency rules.
Tennessee TIPA	Offers strong rights with NIST safe harbor. Controllers, which may include *mobile apps*, must use privacy-by-design and user control. *Data brokers* or similar covered; *data sharing* must be secure.
Texas TDPSA	Broad protections with opt-outs and sensitive data consent. Controllers, which may include *mobile apps*, must provide notices and support opt-outs. *Data brokers* register; *data sharing* must be disclosed.
Utah UCPA	Grants basic rights (no correction). Controllers, which may include *mobile apps*, must allow deletion and opt-outs. *Data brokers* are not required to register; *data sharing* rules are narrow.
Virginia VCDPA	Requires opt-outs and data minimization. Controllers, which may include *mobile apps*, must enable user rights for sensitive data. *Data brokers* are not separately regulated; *data sharing* must be tied to disclosed purposes.

*Notably, several states with large military installations and military populations, such as North Carolina (Fort Bragg), Washington state (Joint Base Lewis-McChord and Seymour Johnson Air Force Base), Georgia (Fort Benning, Fort Gordon, and Robins Air Force Base), and Missouri (Fort Leonard Wood and Whiteman Air Force Base), do not have comprehensive consumer privacy protections codified into law.