Stop Abandoning Me: Exploring the Landscape of Unmaintained IPA Support Applications

Ivy Turk
Ruhr-Universität Bochum

Jasmin Wyss
Ruhr-Universität Bochum

Rebekah Overdorf
Ruhr-Universität Bochum
Research Center Trustworthy Data Science and Security in University Alliance Ruhr

1 Introduction

Those experiencing intimate partner abuse (IPA) by an abuser with physical access to them as well as their devices are hard to reach and difficult to protect. This challenge does not stop well-meaning people from developing creative and beneficial support tools for those who need them most [9]. Although the creation of these tools is often strongly motivated and well intentioned, there is significantly less consideration and support for these tools long term. This leads to a loss of support over time, broken functionality and outdated information, and an overall lack of maintenance [2]. In essence, the created tools become *abandoned*, to the severe detriment of vulnerable users who rely on their continued existence.

There are a multitude of reasons why an application may lose support over time. An app may simply be a prototype, never intended for widespread use, e.g. [5,6,8]. A tool may be tied to fixed funding, and running costs cannot be paid after the funding period ends. The technical leads on a project may provide the tool to support organisations to use, but become busy with other projects and leave the organisation to manage the tool by themselves, which is not always possible [10]. In many cases, the loss of technical support for a tool is no-one's fault. But this matters little for the users who lose access to beneficial systems.

App abandonment has a severe impact on users. Survivors of abuse often use support tools for emergency contacts, support networks, and evidence collection. Establishing a stable connection to emergency support is incredibly difficult in partner abuse scenarios due to surveillance [3, 11, 12] and shared access to devices [4], and losing an emergency support app isolates survivors. Similarly, gathering evidence of long-term abuse takes extensive effort [7], which is undone in an instant if the evidence storage app goes down or the application is no longer compatible with a newer OS version. These harms need to be mitigated, and while these applications can help users, their abandonment leaves survivors back where they started, if not worse off [10].

In this ongoing research, we investigate the landscape of abandoned applications through a measurement study of publicly available and discussed support tools online. Our research question is:

- What proportion of domestic abuse support apps have lost support or are no longer available?

2 Methods

We explored the landscape of support applications for people who experience abuse and whose abuser is presumed to have access to their devices through a four stage process. First, we define search terms for app stores, search engines, and publication databases to identify support applications. We then construct a dataset of these that are either available, publicly discussed in academic or journalistic outlets, or otherwise have left discoverable traces of their existence on the web. We annotate metadata and descriptive data about these tools which are then analysed for correlations between application characteristics and liveness.

Data Collection We perform a series of searches the following platforms hosting our target application types: Google Play (Android apps), Apple App Store (iOS apps), Google Scholar (academic outputs), GitHub (code repositories), and Google Search (web applications and tools fitting other categories). We used snowball sampling to identify further tools matching our criteria by looking at academic citations, suggested apps on the mobile app stores, and lists of tools found

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

via web searches. The full list of search terms are provided in Appendix A.

Annotation We annotate our dataset with two types of information: system metadata, and descriptive labels. Our metadata includes publicly available information on the tools' publication dates, platforms distributing the tool, most recent updates and review dates, and mean review scores. Our descriptive labels categorise applications by target audience, type of support provided (described in detail in Appendix B.1), and the liveness status of the tool. All annotations are objective, and therefore do not require multiple annotators to label. Our dataset was compiled by the lead author, and checked by other authors.

We classify applications as one of "live", "No updates in {1,2,3+} years", "On request only", "Paid access only", "Not publicly distributed", and "Down". We later group these labels for simplicity into "Live", "Restricted Access" (on request only / paid access only), "Abandoned" (no updates in 1+ years), and "Unavailable" (down / not distributed). According to application analytics company 42matters [1], 96% of the top 1 000 Google Play apps and 97% of the top 1 000 iOS apps were updated in the last year. Therefore, we chose to use one year since the latest update as a threshold for "abandoned" applications, as we can expect live apps to be updated at least yearly.

Analysis Our annotated dataset consists solely of measurable data about the applications, and therefore we use different statistical measures to explore it. In future work, we plan on using a logistic regression model to look for correlations between types of application and their current liveness status. In our current research, this model is limited as many categories have too few matching applications, and therefore we instead leave this for future analysis once we have grown our dataset to a sufficient size.

Ethics Our dataset consists of no human data, and only publicly available information about applications which are intended to be public. Therefore, we determined that an ethical review was not necessary, as long as sensible precautions were implemented. To avoid undue strain on distribution servers and networks, we performed data collection manually, which limited the number of queries performed. Regarding the well-being of team members, we made sure to keep an open communication channel between co-authors to alleviate undue psychological strain.

3 Preliminary Results

Our results so far focus on statistics of the applications in our preliminary database. We describe the application dataset as of May 2026, the types of apps found according to our classifications, and the "liveness" of apps in the dataset.

Application Dataset Our dataset contains 117 support tools, including 80 Android apps, 65 iOS apps, and 7 applications available by other means. Notably, 34 tools were exclusively available on one mobile operating system, and 10 were not distributed via official app stores.

Types of Support Provided The majority of applications identified are *information* apps (78 / 117, 66.7%) which assist the user in understanding abusive behaviours, the support available, and connecting with a support network. We identify fewer evidence collection/distribution (30 / 117, 25.6%) and emergency support (36 / 117, 30.8%) applications that were at least partially targeted to people living through IPA. The detailed classifications of applications are provided in Appendix B.2.

Liveness Of the applications in our dataset, 46 (39.3%) were currently available and up to date, with a further 9 (7.7%) available on request or with a paid subscription. Another 37 (31.6%) were classified as abandoned, and 25 (21.4%) are not available. Overall, **62 / 117 (53.0%)** of applications in our dataset have lost support over time. This is a disconcertingly large figure, implying that half of all applications that someone uses for support will stop working over time.

4 Follow-up Research

We will continue with this research through extended data collection, aiming to include applications in languages other than English. We will repeat our collection process with queries translated into Spanish, French, German, and the spoken languages of additional recruited researchers. Assuming this provides sufficient data to enable statistical validity, we will use logistic regressions to identify the types of applications which are more likely to be abandoned. We currently hypothesise that this will mostly focus on academic outputs, where prototypes are designed in papers and released as prototypes with no intentions of being maintained. We will also explore regional differences in application availability, distribution methods, and organisation affiliation as possible indicators of (an absence of) long-term support for these tools.

Our research has created a large dataset of IPA support apps, which we will provide and explore further in our future work. This includes exploration of the hiding mechanisms employed by IPA apps, where the abuser adversary is assumed to have access to the same device and can identify the support tools a survivor is using.

Acknowledgments

The authors would like to thank Nimra Ahmed and Sophie Stephenson for inspiring this project through discussions at CHI 2026 in addition to their own research highlighting this issue. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

[1] 42matters. App update frequency statistics 2026: Google play store aso. https://42matters.com/google-play-aso-with-app-update-frequency-statistics, 2026. Accessed on 25 May 2026.

[2] Nimra Ahmed, Angelika Strohmayer, and Elaine M. Huang. Scattered searches, broken apps, quiet repairs: A feminist autoethnographic critique of technology and research on gender-based violence. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, CHI '26, New York, NY, USA, 2026. Association for Computing Machinery.

[3] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky spy devices and defective detectors: The ecosystem of intimate partner surveillance with covert devices. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 123–140, Anaheim, CA, August 2023. USENIX Association.

[4] Periwinkle Doerfler, Kieron Ivy Turk, Chris Geeng, Damon McCoy, Jeffrey Ackerman, and Molly Dragiewicz. Privacy or Transparency? Negotiated smartphone access as a signifier of trust in romantic relationships, 2024.

[5] Nitesh Goyal, Leslie Park, and Lucy Vasserman. "you have to prove the threat is real": Understanding the needs of female journalists and activists to document and report online harassment. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[6] Philippe Mangeard, Bhaskar Tejaswi, Mohammad Mannan, and Amr Youssef. Warne: A stalkerware evidence collection tool. *Forensic Science International: Digital Investigation*, 48:301677, 2024. DFRWS EU 2024 - Selected Papers from the 11th Annual Digital Forensics Research Conference Europe.

[7] Sophie Stephenson, Naman Gupta, Kyle Huang, David Youssef, Kayleigh Cowan, and Rahul Chatterjee. Trauma-informed digital evidence collection: A design inquiry into evidence practices for technology-facilitated abuse in intimate partner violence. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, CHI '26, New York, NY, USA, 2026. Association for Computing Machinery.

[8] Sharifa Sultana, Mitrasree Deb, Ananya Bhattacharjee, Shaid Hasan, S.M.Raihanul Alam, Trishna Chakraborty, Prianka Roy, Samira Fairuz Ahmed, Aparna Moitra, M Ashraful Amin, A.K.M. Najmul Islam, and Syed Ishtiaque Ahmed. 'unmochon': A tool to combat online sexual harassment over facebook messenger. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[9] Mehreen Sumra, Sohail Asghar, Khalid S. Khan, Juan M. Fernández-Luna, Juan F. Huete, and Aurora Bueno-Cavanillas. Smartphone apps for domestic violence prevention: A systematic review. *International Journal of Environmental Research and Public Health*, 20(7), 2023.

[10] Nick Taylor, Keith Cheverst, Peter Wright, and Patrick Olivier. Leaving the wild: lessons from community technology handovers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, page 1549–1558, New York, NY, USA, 2013. Association for Computing Machinery.

[11] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1893–1909. USENIX Association, August 2020.

[12] Kieron Ivy Turk and Alice Hutchings. Spy-oT: Understanding how users learn to use internet of things devices for abusive purposes. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2025)*, Seattle, WA, August 2025. USENIX Association.

A Application Search Terms

All searches were performed both with and without "app" as a suffix, for example "Harassment support app" and "Harassment support".

- Partner Abuse Terms
  - Intimate partner abuse
  - Intimate partner violence
  - Domestic abuse

  - Domestic violence
  - Abuse support
  - Violence support
  - Abuse help
- Forms of Abuse Terms
  - Harassment support
  - Surveillance support
  - Spying support
  - Spyware detection
  - Spyware removal
- Types of Support Terms
  - Abuse information
  - Abuse evidence
  - Evidence Collection
  - Abuse recording
  - Abuse emergency
  - Emergency support
  - Safety
  - Personal safety

B Application Support Types

B.1 Derivation of Categories

We classify applications according to the form of support they provide. We build on the classifications defined by Sumra et al. [9]: legal information, self-assessment, informative, avoidance, and emergency assistance apps. The first four of these categories can be grouped under "information", while emergency assistance can be divided into Police / emergency services, contacting friends, and sharing information (such as current location) with contacts in both categories. We add an additional sub-category for information describing applications that aid in building a support network. There are also a wealth of evidence applications [7], which we divide into collection and sharing.

B.2 Application Classifications

Category	Sub-Category	Count
Information	Education	46
	Services	28
	Legal Advice	5
	Networking	14
	Planning	19
	Any	78
Evidence	Collection	29
	Sharing	11
	Any	30
Emergency	Police	26
	Friends	16
	Sharing	5
	Any	36

Table 1: Categories of Applications. The "any" subcategory totals the unique applications with at least one subcategory within the overarching category.