Empirical Analysis of Sri Lankan Mobile Health Ecosystem: A Precursor to an Effective Stakeholder Engagement

Kenneth Thilakarathna,[1,2] Sachintha Pitigala,[2] Jayantha Fernando,[3] Primal Wijesekera,[4,5]
[1]University of Colombo School of Computing, [2]University of Kelaniya, [3]Heritage Partners, [4]ICSI, [5]UC Berkeley

ABSTRACT

Sri Lanka recently passed its first privacy legislation covering a wide range of sectors, including health. As a precursor for effective stakeholder engagement in the health domain to understand the most effective way to implement legislation in healthcare, we have analyzed 41 popular mobile apps and web portals. We found that 78% of the tested systems have third-party domains receiving sensitive health data with minimal visibility to the consumers. We discuss how this will create potential issues in preparing for the new privacy legislation.

KEYWORDS

privacy, health surveillance, compliance

1 INTRODUCTION

Sri Lanka's mature and effective public health ecosystem has proven equally efficient compared to major economies. Given the open and unrestricted nature of the health ecosystem, patients can consult any medical practitioner at will without worrying about insurance or the cost. Inadvertently, this has also created a vibrant digital ecosystem where consumers in Sri Lanka have long enjoyed the comfort of scheduling appointments over the phone digitally.

As the first in the region, Sri Lanka recently passed its first nationwide privacy legislation [3]. Europe and the US, despite having regulations in place for some time, are facing continuous threats of breaching consumer privacy expectations and regulatory violations. Research at the intersection of Tech, Policy, and Legal has shown various reasons, such as lack of awareness, miscomprehension of the regulatory requirements, miscommunication, the lack of transparency in the third-party code and systems used by developers, and finally, lack of a strong institutional framework due to budgetary and bureaucratic constraints. This long list of reasons has produced the notion of law in the books vs. law in the code.

Sri Lanka is uniquely placed in this journey since the country is at an early phase of setting up the institutional framework for the implementation of privacy legislation enacted recently. The core objective of the work is to utilize the golden period and ensure that relevant authorities and stakeholders in the health domain are properly informed by empirical evidence and aware of their responsibilities towards a privacy-conscious ecosystem.

2024(X), 1–5

https://doi.org/XXXXXXX.XXXXXXX

2 RELATED WORK

Prior studies have investigated potential regulatory violations in mobile apps in the US [17, 22, 31, 35, 35, 37] while another line of work examines the compliance of mobile health apps in the context of GDPR [10, 16, 29, 33]. The focus of privacy studies has delve into the healthcare ecosystem through multiple subsystems such as analyzing privacy of femtech health [14, 36, 40], mobile-based COVID-19 tracing applications for their privacy implications [11, 41], operation of mobile therapy apps, a subset of the telehealth app ecosystem [23, 26] to name a few. Another research trajectory assesses the availability, scope, and transparency of mobile health app privacy policies [9, 32, 39, 42] where there are studies focused on understanding the developers' role in health privacy and challenges faced in producing complied software solutions [5, 6, 8, 21, 28, 30, 43]. In the US, legal authorities such as the FTC and HHS scrutinize mobile health apps for compliance [15, 18–20]. FTC has used the HBNR [12] and FTC Act [2] to pursue these actions as these apps traditionally fall outside the scope of HIPAA [1].

3 BACKGROUND

3.1 What is a health app?

Definitions of "health app," "medical app," or "wellness app" can overlap, and there is no universally accepted definition for these terms. For the context of this work, we define a health app as an Android-based mobile app or a mobile-ready website that lets consumers (patients) communicate with a healthcare provider and schedule an appointment or give specific information or guidance on a specific health condition such as diabetes, or online pharmacy.

3.2 Applicable Privacy Legislation

In 2022, the government of Sri Lanka passed its Personal Data Protection Act, No. 9 of 2022 (PDPA), which is a commendable starting point for a privacy ecosystem [3]. PDPA is a comprehensive privacy legislation such as CCPA or GDPR; however, Health data is defined under a special category with extra protection.

4 METHODOLOGY

4.1 Mobile Analysis Tool

We focused our analysis on the Android ecosystem, given it is the most prevalent mobile operating system [13] and our in-house tools on Android. In our custom Android platform (based on v9.0-_r39), we modified the platform to enable the real-time monitoring of apps' access to protected resources (e.g., location data, address book contacts, etc.) and sharing over the network. We have also implemented stringent guards to hide our instrumentation from the latest array of anti analysis techniques [25, 27, 34, 44, 46].

Our network interception occurs at two different points: one at the default Android network stack at *conscrypt* library level just

before the SSL_read and SSL_write, and one at the webview library level intercepting XHR requests. Our instrumentation does not have any false positives, but there is a probability of false negatives due to the coverage in app execution – the data should be treated as the absolute lower bound of what is happening in the real world.

4.2 App Corpus

We looked for Android apps and websites that let a patient make an appointment with a physician, provide information or guidance on specific conditions, online pharmacy systems, rehabilitation apps, or sites for leading hospitals in the Sri Lanka Google Play Store from 01 June 2024 until 07 June 2024 and in the Google website. We ended up testing 41 Android-based apps and websites. The dataset includes 5 Android apps and 37 websites accessed through Android: 11 hospitals, 14 medical clinics, four information sites targeting specific conditions, seven online pharmacies, and five physician scheduling portals. The data set also has different types of health apps focusing on fertility, diabetes, cancer, mental health, etc. From here onward, we refer to both apps and websites as health systems.

4.3 Testing Procedure

We tested the apps and websites using Pixel 3a phones running our instrumented Android. We explored the apps/websites as much as possible go over as many options and links as possible. Whenever possible, we also searched for specific conditions or a specific physician to see whether such information is shared with third-parties.

Android offers more sensitive resources and functionalities than the desktop environment. Hence, understanding how these websites behave in the mobile ecosystem is important. During the app testing, the researcher recorded all the sensitive data used, such as synthetic names, all the synthetic health data used to fill the questions, sensitive pages visited, such as "help on anxiety." Once the network traces are decoded, we use a script to look for any transaction with specific strings used in the testing.

4.4 Health Data

The definition of health data under PDPA [3] is ”personal data related to the physical or psychological health of a natural person, which includes any information that indicates his health situation or status;;” and HHS recently issued a guidance [24], identifying that even sharing the app name along with a unique ID of the consumer would fall within the definition of Personal Health Information (PHI), as it identifies the individual’s past, present or future health or health care or payment. Keeping this new legal principles in mind, we labeled the following items as health data as any of the following can be used to infer their health conditions or health interests: conventional health data, app usage (apps targeting specific medical conditions), search queries within health apps (searching for a medical condition, a medication, etc.), navigation with the app (viewing pages focusing on a specific medical condition).

4.5 Ethical Considerations

Based on our number of prior conversations with our Institutional Review Board on large-scale mobile app analysis for compliance, we determined we do not require an IRB review for this study. We are not examining any human subject but only the app execution.

Third-Party Recepient	Type	Number of Apps	Health Data Status
Google Analytics	Tracking/ Event Reporting	10	Non-compliant
Google Search	Search	8	Likely non-compliant
Facebook	Tracking/ Event Reporting	6	Non-compliant
Doubleclick	Advertising	5	Non-compliant

Table 1: Third-party recipients of physician information.

Third-Party Recepient	Type	Number of Apps	Health Data Status
Google Analytics	Tracking/ Event Reporting	24	Non-compliant
Google Search	Search	11	Likely non-compliant
Facebook	Tracking/ Event Reporting	5	Non-compliant
Zoho	CDN	5	Unknown
Doubleclick	Advertising	4	Non-compliant
GStatic	CDN	3	Unknown
Google Tag Manager	Tracking	2	Non-compliant
Cloudfare	CDN	2	Unknown
Private Site	Personal	1	Likely non-compliant

Table 2: Recipients of sensitive usage information.

Ecological Validity

Android apps are likely to detect the geolocation based on the IP and might change their behavior accordingly. All Sri Lankan based apps were executed in Sri Lanka to preserve the ecological validity of the test environment. We only have one app that stopped its execution after detecting the underlying custom Android OS.

5 DATA SHARING PRACTICES

Physician Information. : Since the pandemic, systems allowing scheduling appointments online have soared, and most of them went unchecked until recently. Online physician scheduling is quite popular in Sri Lanka. In the health compliance ecosystem, they play a crucial role. Our dataset has seventeen systems that allow patients to search for physicians, get scheduling information, or make an appointment directly. We have observed that ten health systems (58.82% out of 17 health systems with the scheduling feature) have shared sensitive physician information with third parties. Physician information can divulge a patient’s condition as a highly sensitive data point. Table 1 lists all the third-party recipients of such sensitive information. The last column denotes whether the respective recipient will treat the health data without violating any regulatory or consumer privacy expectations.

Usage Information. : Event reporting in online systems is usually harmless for the consumers. But, in a health system, it can diffuse sensitive information such as potential interest or a condition a patient has. For example, a repeated visit to infertility pages can likely expose consumer’s highly sensitive condition. Hence, sharing usage information should be done carefully with masking. This

concern is confirmed by HSS (in the US) as per their latest guidance on regulatory expectations [24].

In our dataset, we have 27 (65.85% of our test-pool) apps sharing highly sensitive usage information with third parties who are likely to use such information for user tracking and profiling. This usage information includes visits to infertility treatment pages, mental illness tests, physician pages specializing in specific conditions. In an ideal setup, patients are highly unlikely to share their interests and why they visit such pages. Table 3 lists all the third-party recipients of such sensitive information. The last column denotes whether the recipient will treat the health data without violating regulatory or consumer privacy expectations – this is determined based on their public documents.

We observed that nine health systems shared the search queries we used during the testing with third-party recipients—Google Analytics (8 apps) and Facebook (2 apps) are the most common recipients. Similar to app usage, search queries are sensitive, such as physicians, symptoms, and a particular medicine, all of which could expose sensitive conditions associated with the patient.

We also observed one health system sending sensitive health information over the Internet unencrypted, jeopardizing the confidentiality and integrity of the patients' health data.

Out of the 33 health systems sharing data with third parties, only nine health systems (27.27%) have acknowledged third-party data sharing in their privacy policies, and, overall, 27 (65% of our test-pool) health systems did not have a privacy policy.

Except for two Android apps (which shared AAID with Facebook and Google Analytics), none of the other systems shared soft or persistent IDs with third parties. From a developer perspective, no sensitive health data shared had an ID linking to the patient. The biggest caveat, however, is the patient's IP address. Even HIPAA labels the IP address as one of the eighteen HIPAA identifiers that can be used to link to a specific person. The extent of the linkage depends on the nature of the mobile phone's connection. If it is a home WIFI, it is easy to link each data transfer to a specific person along with the IP address and many other meta information.

6 REGULATORY PREPARATION

The main objective of this work is to understand the current status of the mobile health ecosystem as a precursor to understanding the cost, responsibilities, and challenges faced by developers and health organizations in complying with the new Privacy legislation.

The preparation has to be done in two ways: by managing consent and by providing data subject rights. We recently conducted a focus group to understand stakeholder perspectives on the new privacy legislation [4]. Participants raised both of these tasks as sources of cost in the process of complying with new legislation.

None of the health systems we analyzed have any sort of consent management (except for one website that had cookie consent). This will be one of the first major changes for health systems to properly manage consumers' consent. There are several challenges to effectively obtaining an *informed* consent from patients.

PDPA requires the controller to properly convey one or more predefined purposes to the data subject before obtaining consent unless exempted under PDPA guidelines such as legal obligations. Given the widespread use of third parties receiving sensitive health data, it will be a challenge for health systems to set a predefined purpose properly. Especially once a data controller shares data with the likes of Facebook and Google Analytics, it is hard to dictate how they are going to use the health data.

Another major change would be to obtain consent for cross-border data transfer. All third-party data recipients are not based in Sri Lanka; hence, as per PDPA clauses, health systems need to obtain consent from the users of the health systems properly.

The heavy use of third-party trackers such as Google Analytics, Facebook, and DoubleClick further complicates since controllers need to properly expose how the data recipients are going to profile customers based on health data. Apart from the knowledge that most of such data is used in Advertising, it is a black box for outsiders to understand how the whole mobile ad ecosystem behaves, leaving the data controllers in Sri Lanka in the dark. PDPA has a separate clause for profiling, especially when using special category data such as health.

PDPA (similar to the clauses in GDPR and CCPA) emphasizes providing data subjects (patients in this context) with an array of rights: access, erase, and withdraw consent. Our prior work on implementation of data subject requests (DSR) in CCPA [37, 38] showed controllers have a hard time accurately responding to DSR because controllers are not fully aware of how third parties collected data from data subjects while executing within the controller's app. Given the widespread use of third-party trackers, Sri Lankan health systems will face the same issue.

PDPA sets clear guidelines on what information should be available for the consumer for transparency. Privacy policy is one of the key techniques to properly convey data practices, purposes, and other relevant information. Most health systems in Sri Lanka do not have any privacy policy. We believe this will be an easy first step for many organizations to publish an accurate privacy policy. Still, this step will also be affected by third-party data collection's opaque nature and their purposes.

Literature has looked into how developers understand their regulatory responsibilities and the gaps in their comprehension of the regulations [7]. Further work is needed to understand why developers share health data with third parties that have publicly asked not to share heath data with them [1] [2]. Literature has proposed solutions such as the use of SBOM to communicate compliance restrictions [45]. This is one of the overarching objectives of this work, i.e., to work with stakeholders to understand how to effectively implement privacy legislation while helping the likes of developers of health systems providing proper guidance and tools.

The Data Protection Authority of Sri Lanka is keen to work with stakeholders to understand their perspectives and figure out the best way to roll out the implementation with the help of relevant parties such as health organizations, patients, developers of health systems, and legal practitioners. We have already conducted one stakeholder engagement to understand the cost, challenges, and opportunities that lie ahead in the compliance process. We hope this work will set an effective precursor for engaging with professionals in the healthcare domain to figure out their costs and challenges in preparing for the new legislation. The objective of this is not to blame anyone but to figure out where the help is most needed.

[1] https://support.google.com/analytics/answer/13297105?hl=en
[2] https://web.facebook.com/business/help/361948878201809?id=188852726110565&_rdc=1&_rdr

ACKNOWLEDGMENTS

This work was supported by the U.S. National Science Foundation (under grant CNS-2055772 & CNS-2217771).

REFERENCES

[1] Coppa support. https://github.com/prebid/prebid.github.io/pull/3476. Accessed: 2022-01-28.
[2] Federal Trade Commission (FTC) Act. 15 U.S.C. §45(a)(1).
[3] Personal data protection act. https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf.
[4] Round table discussion on pdpa. https://www.linkedin.com/pulse/roundtable-discussion-privacy-regulation-beyond-primal-wijesekera-lor3c/.
[5] B Aljedaani and MA Babar. Challenges with developing secure mobile health applications: Systematic review. jmir mhealth uhealth 9, e15654, 2021.
[6] Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, and M Ali Babar. An empirical study on developing secure mobile health apps: The developers' perspective. In *2020 27th Asia-Pacific Software Engineering Conference (APSEC)*, pages 208–217. IEEE, 2020.
[7] Noura Alomar and Serge Egelman. Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Proceedings on Privacy Enhancing Technologies*, 4(2022):24, 2022.
[8] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. Engineering privacy by design: Are engineers ready to live up to the challenge? *The Information Society*, 35(3):122–142, 2019.
[9] J Benjumea, J Ropero, O Rivera-Romero, E Dorronzoro-Zubiete, and A Carrasco. Assessment of the fairness of privacy policies of mobile health apps: Scale development and evaluation in cancer apps. *JMIR Mhealth Uhealth*, 8(7):e17134, 2020.
[10] Jaime Benjumea, Enrique Dorronzoro, Jorge Ropero, Octavio Rivera-Romero, and Alejandro Carrasco. Privacy in mobile health applications for breast cancer patients. In *2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS)*, pages 634–639, 2019.
[11] Swathikan Chidambaram, Simon Erridge, James Kinross, and Sanjay Purkayastha. Observational study of uk mobile health apps for covid-19. *The Lancet Digital Health*, 2(8):e388–e390, 2020.
[12] Federal Trade Commission. Health breach notification rule. https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule/. Accessed: 2023-10-15.
[13] Stat Counter. Mobile operating system market share worldwide. https://gs.statcounter.com/os-market-share/mobile/worldwide, 2023. Accessed: 2023-10-15.
[14] Daniel A Epstein, Nicole B Lee, Jennifer H Kang, Elena Agapie, Jessica Schroeder, Laura R Pina, James Fogarty, Julie A Kientz, and Sean Munson. Examining menstrual tracking to inform the design of personal informatics tools. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6876–6888, 2017.
[15] Leselye Fair. First ftc health breach notification rule case addresses goodrx's not-so-good privacy practices. https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices, 2023. Accessed: 2023-10-15.
[16] Ming Fan, Le Yu, Sen Chen, Hao Zhou, Xiapu Luo, Shuyue Li, Yang Liu, Jun Liu, and Ting Liu. An empirical evaluation of gdpr compliance violations in android mhealth apps. In *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*, pages 253–264, 2020.
[17] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, Alessandra Gorla, et al. Angel or devil? a privacy study of mobile parental control apps. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020(2):314–335, 2020.
[18] FTC. Betterhelp, inc., in the matter of. https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter, 2023. Accessed: 2023-10-15.
[19] FTC. Ovulation tracking app premom will be barred from sharing health data for advertising under proposed ftc order. https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc, 2023. Accessed: 2023-10-15.
[20] HHS & FTC. Use of Online Tracking Technologies. https://www.hhs.gov/sites/default/files/ocr-ftc-letters-re-use-online-tracking-technologies.pdf, July 20 2023.
[21] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*, 23:259–289, 2018.
[22] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazar, Kenneth A Bamberger, and Serge Egelman. The price is (not) right: Comparing privacy in free and paid apps. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020(3):222–242, 2020.
[23] Muhammad Hassan and Masooda Bashir. Unveiling privacy measures in mental health applications. In *Adjunct Proceedings of the 2023 ACM International Joint Conference on Pervasive and Ubiquitous Computing & the 2023 ACM International Symposium on Wearable Computing*, pages 648–654, 2023.
[24] Health and Human Services. Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, December 01 2022.
[25] INKA Entworks Inc. Appsealing. https://www.appsealing.com/, September 30 2021.
[26] Leonardo Horn Iwaya, M Ali Babar, Awais Rashid, and Chamila Wijayarathna. On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering*, 28(1):2, 2023.
[27] Jongsu Lim, Yonggu Shin, Sunjun Lee, Kyuho Kim, and Jeong Hyun Yi. Survey of dynamic anti-analysis schemes for mobile malware. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 9(3):39–49, 2018.
[28] Joana Muchagata and Ana Ferreira. Translating gdpr into the mhealth practice. In *2018 International Carnahan Conference on Security Technology (ICCST)*, pages 1–5, 2018.
[29] Trix Mulder. Health apps, their privacy policies and the gdpr. *European Journal of Law and Technology*, Jun 2019. University of Groningen Faculty of Law Research Paper No. 15/2020.
[30] Uzma Mustafa, Eckhard Pflugel, and Nada Philip. A novel privacy framework for secure m-health applications: The case of the gdpr. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pages 1–9, 2019.
[31] Trung Tin Nguyen, Michael Backes, Ninja Marnau, and Ben Stock. Share first, ask later (or never?) studying violations of GDPR's explicit consent in android apps. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3667–3684, Berkeley, CA, USA, 2021. USENIX.
[32] Kristen O'Loughlin, Martha Neary, Elizabeth C. Adkins, and Stephen M. Schueller. Reviewing the data security and privacy policies of mobile apps for depression. *Internet Interventions*, 15:110–115, 2019.
[33] Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, 6:9390–9403, 2018.
[34] Promon. Shield: In-App Protection and Security for Mobile Apps. https://promon.co/products/mobile-app-protection/, September 30 2021.
[35] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, Serge Egelman, et al. "won't somebody think of the children?" examining coppa compliance at scale. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2018(3):63–83, 2018.
[36] Celia Rosas. The future is femtech: Privacy and data security issues surrounding femtech applications. *Hastings Bus. LJ*, 15:319, 2019.
[37] Nikita Samarin, Shayna Kothari, Zaina Siyed, Oscar Bjorkman, Reena Yuan, Primal Wijesekera, Noura Alomar, Jordan Fischer, Chris Hoofnagle, and Serge Egelman. Lessons in vcr repair: Compliance of android app developers with the california consumer privacy act (ccpa). *arXiv preprint arXiv:2304.00944*, 2023.
[38] Nikita Samarin and Primal Wijesekera. Understanding how third-party libraries in mobile apps affect responses to subject access requests. 2023.
[39] Brinda Hansraj Sampat and Bala Prabhakar. Privacy risks and security threats in mhealth apps. *Journal of International Technology and Information Management*, 26(4), 2017.
[40] Laura Shipp and Jorge Blasco. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proc. Priv. Enhancing Technol.*, 2020(4):491–510, 2020.
[41] Yogesh Simmhan, Tarun Rambha, Aakash Khochare, Shriram Ramesh, Animesh Baranawal, John Varghese George, Rahul Atul Bhope, Amrita Namtirtha, Amritha Sundararajan, Sharath Suresh Bhargav, et al. Gocoronago: privacy respecting contact tracing for covid-19 management. *Journal of the Indian Institute of Science*, 100:623–646, 2020.
[42] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 22(e1):e28–e33, 08 2014.
[43] Mohammad Tahaei, Julia Bernd, and Awais Rashid. Privacy, permissions, and the health app ecosystem: A stack overflow exploration. In *Proceedings of the 2022 European Symposium on Usable Security*, pages 117–130, 2022.
[44] Talsec. Talsec freeRASP. https://www.talsec.app/freerasp-in-app-protection-security-talsec, September 30 2021.
[45] Primal Wijesekera. Health compliance through a transparent supply chain. 2024.
[46] Hang Zhang, Dongdong She, and Zhiyun Qian. Android root and its providers: A double-edged sword. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 1093–1104, New York, NY, USA, 2015. Association for Computing Machinery.

ID / URL	App Name	App Type	Service Category	Owner Category
com.inova.velocity	Doc990	Android App	Physician Appointment	Third-Party/Telecom
doc.lk	Doc990	Website	Physician Appointment	Third-Party/Telecom
com.developer.odoc	oDoc - Video Consultations	Android App	Video Consultation	First-party/technical
asirihealth.com	Asiri Health	Website	Appointment/generic	Hospital
www.durdans.com/appointments/	Durdans	Website	Appointment/generic	Hospital
www.nawaloka.com/channeling/	Nawaloka	Website	Generic	Hospital
www.lankahospitals.com/en/doctor-channeling/	Lanka Hospital	Website	Generic	Hospital
www.delmonhospital.com/en/find-a-doctor	Delmon Hospital	Website	Generic	Hospital
www.ninewellshospital.lk/appointment-booking/	Nine Wells	Website	Appointment/generic	Hospital
https://medihelphealth.com/ https://www.medihelp.lk/	Medihelp	Website	Appointment/generic	Hospital
www.wishfertility.lk/	Wish Fertility	Website	Generic	Medical Services
hemashospitals.com/	Hemas Hospitals	Website	Generic	Hospital
ivflanka.com/	IVF Lanka	Website	Generic	Medical Services
www.suvika.lk/	Suvika	Website	Generic	Medical Services
www.pfrcivf.lk/	PCR IVF	Website	Generic	Medical Services
jeewakaprivatehospital.lifegroup.lk/ channel-your-doctor/	Jeewaka Hospital	Website	Generic	Hospital
www.goldenkeyhospitals.com/ ask-online-from-a-consultant	Golden EENT	Website	Generic	Medical Services
www.inspirationscare.lk/#	Inspiration	Website	Generic	Medical Services
santadorahospital.com/	Santa Dora	Website	Generic	Medical Services
arogyahospitals.lk/	Arogya	Website	Generic	Medical Services
www.diabetessrilanka.org/	National Diabetes Centre	Website	Generic	Medical Info Services
www.csth.health.gov.lk/	CSTH	Website	Generic	Medical Info Services
www.jaffnadiabeticcentre.org/	Jaffna Diabetic Centre	Website	Generic	Medical Info Services
www.nawinna.com/	Nawinna	Website	Generic	Medical Services
www.queensburyhospitals.lk	Queensbury	Website	Generic	Hospital
diabeteshormonecenter.com/	DHC	Website	Generic	Hospital
ceylincocancercentre.lk/	Ceylinco	Website	Generic	Medical Services
cdem.lk/	CDEM	Website	Generic	Medical Services
com.health_assist	Nawaloka	Android App	Generic	Hospital
com.durdans.patientcare	Durdans	Android App	Generic	Hospital
www.healthguard.lk/	Health Guard	Website	Generic	Pharmacy
unionchemistspharmacy.lk/	Union Chemist	Website	Generic	Pharmacy
www.mycare.lk/	mycare	Website	Generic	Pharmacy
www.uniquepharmacy.lk/	Unique Pharmacy	Website	Generic	Pharmacy
www.carelink.lk/	Carelink	Website	Generic	Pharmacy
www.ceymed.lk/	Ceymed	Website	Generic	Medical Service
buymedicine.lk/	Buy Medicine	Website	Generic	Pharmacy
onlinepharmacy.lk/	Online Pharmacy	Website	Generic	Pharmacy
echannelling.com/	eChanneling	Website	Physician Appointment	Third-Party
vida.lk	Vida	Website	Generic	Medical Services
www.odoc.life/	oDoc - Video Consultations	Website	Generic	Medical Services

Table 3: List of applications tested