Quality Assessment of Online Automated Privacy Policy Generators: An Empirical Study

Ruoxi Sun
The University of Adelaide, Australia
ruoxi.sun@adelaide.edu.au

Minhui Xue
The University of Adelaide, Australia
jason.xue@adelaide.edu.au

ABSTRACT

Online Automated Privacy Policy Generators (APPGs) are tools used by app developers to quickly create app privacy policies which are required by privacy regulations to be incorporated to each mobile app. The creation of these tools brings convenience to app developers; however, the quality of these tools puts developers and stakeholders at legal risk. In this paper, we conduct an empirical study to assess the quality of online APPGs. We analyze the completeness of privacy policies, determine what categories and items should be covered in a complete privacy policy, and conduct APPG assessment with boilerplate apps. The results of assessment show that due to the lack of static or dynamic analysis of app's behavior, developers may encounter two types of issues caused by APPGs. First, the generated policies could be incomplete because they do not cover all the essential items required by a privacy policy. Second, some generated privacy policies contain unnecessary personal information collection or arbitrary commitments inconsistent with user input. Ultimately, the defects of APPGs may potentially lead to serious legal issues. We hope that the results and insights developed in this paper can motivate the healthy and ethical development of APPGs towards generating a more complete, accurate, and robust privacy policy.

CCS CONCEPTS

• **Security and privacy → Software and application security**.

KEYWORDS

Automated privacy policy generator, Privacy policy completeness analysis, Quality assessment

1 INTRODUCTION

Mobile phones have become increasingly important to our daily lives. Information privacy issues are of growing concern to developers as well as to mobile app users. Nowadays, it is very common that

a mobile app accesses, requires, or transmits users' sensitive personal information when requesting services. Privacy policy is one of the key legal statements that is used to protect users' personal information. Many countries have adopted privacy regulations, such as the Children's Online Privacy Protection Act (COPPA) [1], Health Insurance Portability and Accountability Act (HIPPA) [17], the European General Data Protection Regulation (GDPR) [8], and the California Online Privacy Protection Act (CalOPPA) [2]. These regulations restrict the behavior of apps and define the obligations of app developers. One of the main requirements of these privacy regulations is that a privacy policy is mandatory for an app. For example, the Article 13.1(c) of GDPR requires that the use of a data subject's personal data should have a legal basis. The Federal Trade Commission (FTC) also recommended that app developers should ensure easy access to the privacy policy through app stores. However, not every app developer is a legal professional and writing privacy policies could be a time-consuming and tedious task [4]. The emergence of APPGs greatly eases such dilemma. For companies small in size or individual developers who cannot afford the expense of legal fees, an APPG online could be a good option, which can quickly create a customized privacy policy with basic or perhaps reliable terms.

The ease of APPGs comes at a cost of legal risk. FTC severely penalizes companies for breach of commitments in their privacy policies [19]. Failing to provide a correct privacy policy may cause serious legal issues. For example, InMobi, a Singapore-based mobile advertising company, was fined $950,000 by FTC as it collected user's location information without declaring the behaviors in the privacy policy [6]. In 2014, a company of a popular flashlight app and its owner were complained by FTC as they did not reflect the app's use of personal data in app privacy policies. Users of the APPG may encounter the same legal issue with the APPG *per se.*

In this paper, we make several key contributions listed below.

- To assess privacy practices of online APPGs, we analyzed the completeness of privacy policies and determined what categories and items should be covered in a complete privacy policy.
- We investigated 10 popular online APPGs and then studied the complexity of use and payment methods used by them. We designed three boilerplate apps to generate privacy policies and used them for APPG quality assessment. Our method assesses the quality of APPGs by combining the aspects of completeness of privacy policy and the consistency with user input.
- Combined with the results of the quality assessment, we believe that the quality of free APPGs not significantly outperforms that of a well-designed template. We found that

the quality of the paid APPGs largely outperforms the free APPGs, despite many functional issues arisen.

1.1 Related Work

Privacy policy generation techniques. Recent work has been proposed to generate privacy policies for apps. For instance, the AutoPPG [18] conducts static code analysis to extract app behaviors about user personal information. Based on the extracted behaviors, AutoPPG applies natural language processing (NLP) techniques to generate privacy policies.

Mobile app privacy policy. Several works have studied the consistency between privacy policies and app behaviors [11, 15]. Andow *et al.* [3] present a state-of-the-art privacy policy analysis tool, termed PolicyLint. Utilizing sentence-level NLP techniques, PolicyLint is able to detect the positive and negative statements in a privacy policy, which enables the automated analysis of the contradictions in a privacy policy. Chen *et al.* [5] analyzed the security risk of banking apps with NLP and static analysis. Zimmeck *et al.* [20] designed a scaling privacy compliance analysis tool through code analysis and machine learning techniques.

Our work. Because the existing online APPGs rely heavily on user input and templates, if the quality of APPGs cannot be guaranteed, the privacy policy they generate may deviate from the terms expected by users, and inconsistencies with app behaviors may cause serious legal consequences. This paper differentiates from previous works by looking into the quality assessment of APPGs *per se* in terms of their completeness and consistency.

2 METHODOLOGY

2.1 Collecting Online APPGs

In order to investigate the current status of APPGs, we identified a set of popular app privacy policy generators. We first used Google search queries, including but not limited to "privacy terms template", "GDPR compliant privacy policy generator", and "mobile app privacy policy generator". For each result, we selected the first ten entries, including advertising links provided by Google. We also collected recommendation of APPGs across forums, blogs [7, 9], or in the post of the legal consultant website [12]. We remove the APPGs that cannot generate privacy policies for mobile apps and select the most popular ones in terms of their stated marketing scale and user recommendations.

After removing duplicates and highly similar sites, we obtained top 10 popular APPGs listed in Table 1. Although most of them collect user Privacy Identifiable Information (PII), such as mailing address and email address, or even require financial information for service purchasing, only six of them have privacy policies to protect their customers' privacy. While APPGs having advertised their services are being widely used, 40% of them also have disclaimers, stating that their services are only pieces of legal advice, instead of a formal legal service. For example, the APPG #7 listed in Table 1 claims that they provide "Trusted legal agreement". However, they also have a disclaimer stating that, "TermsFeed.com is not a law firm and is not providing legal advice. All information (including agreements, forms and documents) available on our site, www.termsfeed.com, are provided without any warranty, express or implied". Furthermore, for other APPGs, there is no company
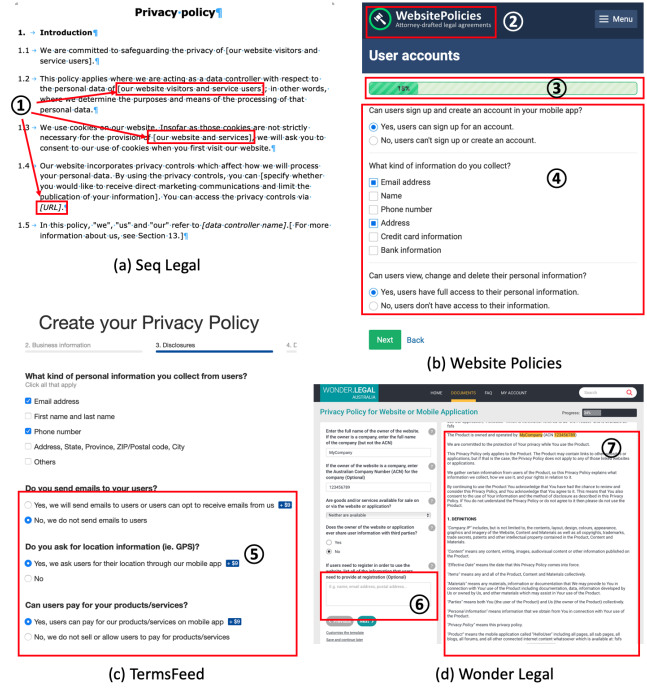

Figure 1: The UIs of APPGs. (1) Fill-in spaces in template. (2) Logo. (3) Progress bar. (4) Multiple choice questions. (5) Paid features. (6) Text area for user input. (7) Preview of policy.

information provided, neither on their websites nor in payment receipts.

Figure 1 shows the user interfaces of typical APPGs. APPGs in a template form, *i.e.*, #1 and #2, always have fill-in space for users to input detailed information. The user interface of survey questionnaire APPGs usually includes a logo, multiple choice questions with yes or no answers, and a progress bar. Some APPGs require payments to use advanced features. APPG # 9 improves the flexibility of user input through an editable text area and provides a preview of the generated privacy policy.

More than half of the APPGs listed in Table 1 are free of charge, or have a free version with limited functionalities, *e.g.*, no GDPR compliant or can only generate one privacy policy. For the three paid APPGs, the user will be charged from $20 to $40 per privacy policy generated, or paid per item added into policy, *e.g.*, $14 for business using, $9 for terms related to location information collection, $14 for involving Google Analytics, which can make one privacy policy costs exceed $180.

2.2 Completeness Analysis of Privacy Policies

As required in GDPR and other privacy regulations, apps must have a privacy policy to explicitly inform what kind of data is collected from users and how data is handled. Related works [10, 16] also argue that a complete app privacy policy should include the following categories:

- ***The basic information,*** which includes the identity of data collector, *e.g.*, the name of the company, email address, and

Table 1: Overview of online APPGs

#	APPG	Company	Location	Payment	Has Privacy Policy?	Has Disclaimer?
1	seqlegal.com	SEQ Legal LLP	Oxfordshire, UK	Free	No	No
2	volusion.com	Volusion	Austin, USA	Free	Yes	No
3	app-privacy-policy-generator.firebaseapp.com	Individual	N/A	Free	No	No
4	getterms.io	Humaan	Perth, Australia	Free	Yes	Yes
5	privacypolicygenerator.info	N/A	N/A	Free	No	Yes
6	legenova.com	Legal Nova Ltd	Sofia, Bulgaria	Free	Yes	No
7	termsfeed.com	N/A	N/A	Paid	Yes	No
8	websitepolicies.com	WebsitePolicies Inc.	Toronto, Canada	Paid	Yes	Yes
9	wonder.legal	Miracle	Paris, France	Paid	No	No
10	termly.io	Termly LTD	London, UK	Free/Period	Yes	Yes

location of the company, the name of the app, and the date of version.

- **The personal information to be collected,** which includes PII and non-PII. As per the guide of PII protection by Mc-Callister [13], the PII includes the name of a user, email address, IP address, location information, *etc.* However, due to the constant evolution of technologies, PII and non-PII may change and overlap. Thus, we also consider non-PII information collected by apps, *e.g.*, the content created by users in apps, device information, and information collected from any third parties.

- **Why and how the data are to be used,** which includes the purpose of data access, the identity of third parties, and whether the data will be disclosed as a response to legal requests.

- **Information management,** which includes the description of user rights, data transfers, the practice of data protection, the retention of data, the notification of change to privacy policies, whether the data will be shared in the case of business merges and acquisitions, and asset sales, and the protection of children's data.

Several most popular apps, *e.g.*, Facebook, Google Calendar, Pokémon Go, Clash of Clans, Tik-tok, EBay, and Runtastic, were analyzed in this paper. Based on the data from Google Play Store, the downloads of these apps have all exceeded 50 million. Considering the spread scale and number of users of these apps, we can infer that their privacy policies are of high quality and minor defects. Through the completeness analysis on their privacy policies, we further investigated the categories that should be covered in privacy policies and determined essential items in each category as shown in Table 2.

In our investigation, two APPGs (#1 and #2) are in form of templates. All the remaining APPGs have a survey questionnaire, querying questions from users, and generate privacy policies based on the user input. Table 3 shows the result of APPG questionnaires. The symbol ● indicates that the item is covered by the questionnaire. As we can see, most APPGs are covered no more than half of the essential items, indicating two potential defects: 1) for some essential items, users cannot input any information to the generator; 2) even if the generated privacy policies cover more items than its questionnaire does, the descriptions of items are not able to closely follow user input. For example, APPG #4 does not even request which privacy information will be collected, but directly writes, "we only ask for personal information when we truly need it to

Table 2: Essential categories and items in privacy policies

Categories	Items
Basic information	Name of company, Address of company, Name of app, Contact info, and Date of last version.
Privacy Information Collected	Name of user, Email address, Phone number, Username/Account ID, IP address, Location information, Purchasing information, Content created by user, Information from third-parties, Device information, User activity, and Cookies.
Use of Information	For detecting abuse and illegal activity, For safety and security, For services improving, For service providing, Personalised advertising, Business analysis, Communication with users, Sharing with other users, Sharing with third-party, and Respond to legal requests.
Information Management	User rights, Data transfers, Protection of data, Data retention, Changes notifying, Business Transactions, Age. and Limits/Children's privacy

provide a service to you. We collect it by fair and lawful means, with your knowledge and consent," in the generated privacy policy.

We also counted how many questions in each survey questionnaire of APPGs. Two template-typed APPGs have few questions; however, the most complex APPG has 45 questions for users to answer, and it may take roughly an hour to generate one privacy policy.

2.3 Designing Boilerplate Apps

To further assess the quality of APPGs, we designed boilerplate apps to simulate the privacy policy generation process. For each APPG, we generated privacy policies based on the wording of the three same boilerplate apps to evaluate whether the generated privacy policy is covered by essential items and whether the generated terms are aligned with user input.

- **App 1:** The first app only collects the full name of the user which is visible on the screen. This app will only disclose user information in the case of legal request.

- **App 2:** A game app utilizing augmented reality technology collects user's location information. Users need to register an account to login the game app, which collects user's name and email address. Users are able to login with a third-party account, such as a Google account or a Facebook account. Users can purchase virtual items in-app through a third-party payment processor. The design of this app comes from the popular game Pokémon Go.

- **App 3:** The third app is an social app which enables users interaction and communication with each other. Users can create contents and share them publicly in-app. Users need

Table 3: Categories and items covered in APPG questionnaires (# APPG is referred to the first column of Table 1)

# APPG	1	2	3	4	5	6	7	8	9	10
Basic information										
Name of company		●	●	●	●		●	●	●	●
Address of company				●	●		●	●		●
Name of App				●	●	●	●	●	●	●
Contact info		●			●	●	●	●		●
Date of last version					●				●	●
Privacy Information Collected										
Name of user							●	●		
Email Address						●	●	●		
Phone							●	●		
Username/Account ID										
IP address										
Location information						●	●			●
Purchase information								●		
In-App sharing										
Content created by user										
Information from third-parties										
Device information										
User activity										
Cookie data			●							
Others					●	●	●		●	●
Use of Information										
Detect abuse and illegal activity							●			
Safety and security										
Improve products/services										
For service providing										
Personalised advertising			●				●	●	●	●
Business analysis						●	●	●	●	●
Communication with users							●	●	●	●
Sharing of information										
Sharing with other users						●	●	●	●	●
Sharing with third-party								●	●	
Respond to legal requests							●	●		
Information Management										
User rights								●		
Data transfers										
Protection of data									●	●
Data retention										●
Changes notifying								●		
Business Transactions							●	●	●	
Age limits/Children's privacy								●	●	●
Number of Questions	0	2	4	4	6	13	20	30	45	45

Table 4: Design of dummy apps

Identity of Data Collector	App 1	App 2	App 3
Name of company	◐	◐	◐
Address of company	◐	◐	◐
Name of App	◐	◐	◐
Contact info	◐	◐	◐
Date of last version	◐	◐	◐
Information Collection	**App 1**	**App 2**	**App 3**
Name of user	●	●	●
Email Address	◐	●	●
Phone	◐	◐	●
Username/Account ID	◐	●	●
IP address	◐	●	●
Location information	◐	●	●
Purchase information	◐	●	●
In-App sharing	◐	◐	●
Content created by user	◐	◐	●
Information from third-parties	◐	●	●
Device information	◐	◐	●
User activity	◐	◐	●
Cookie data	◐	◐	●
Others	◐	◐	●
Use of Information	**App 1**	**App 2**	**App 3**
Detect abuse and illegal activity	○	●	●
Safety and security	○	○	●
Improve products/services	○	●	●
For service providing	●	●	●
Personalised advertising	◐	◐	●
Business analysis	◐	◐	●
Communication with users	◐	●	●
Information Disclosure	**App 1**	**App 2**	**App 3**
Sharing with other users	●	●	●
Sharing with third-party	●	●	●
Respond to legal requests	●	●	●
Information Management	**App 1**	**App 2**	**App 3**
User rights	◐	◐	◐
Data transfers	◐	◐	◐
Protection of data	◐	◐	◐
Data retention	◐	◐	◐
Changes notifying	◐	◐	◐
Business Transactions	◐	◐	◐
Age limits/Children's privacy	◐	◐	◐

○: Not related ◐: Recommended ●: Essential

to register an account to login the social app. The registration process collects user's personal information, such as name, email address, phone number. The app also utilizes cookies data for updating services.

Table 4 lists all the categories and items that could be incorporated in the generated privacy policies. We defined a three-level criticality of items in an app: *Not related, Recommended, and Essential*. *Not related* means that the item is unnecessary to be explicitly mentioned in the privacy policy. For example, App 1 does not exploit user information for safety and security purpose, regardless of the reference, we give the corresponding item 0 score; *Recommended* means that the item is not critical; however, an incorrect description may cause potential inconsistency and legal issues; *Essential* items should be exactly described in the privacy policy as per user input and inconsistent description may cause serious legal issues. For example, App 3 collects email address from users, and this must be described consistently in the generated privacy policy.

2.4 Quality Assessment of APPGs

Based on the criticality level of items for each boilerplate app, we evaluate the quality of generated privacy policies. The rules of evaluation are described in Table 5. If the description exactly matches the user input, we will give a high score to the item; otherwise, a negative penalty score will be given. Considering there are many descriptions generated based on templates, which may be still correct but not exactly be consistent with the user input, we will assign a positive but a lower score. For example, whatever the user input is for a policy generated by APPG #2, it always has the sentence "we value your trust in providing us your Personal Information, thus we are striving to use commercially acceptable means of protecting it." We will only give score 1 for such blur description as this may lead to potential inconsistency and increase risks to developers and app users.

Using this method, we cannot only evaluate the completeness of a generated privacy policy, but also assess the APPG quality based on whether the terms match the user input. A higher score indicates

Table 5: The rules of APPG performance evaluation

Criticality of Items	Consistency with User Input	Score
Not related	N/A	0
Essential	Exactly consistent	5
	Not exactly consistent	3
	Inconsistent	-5
Recommended	Exactly consistent	3
	Not exactly consistent	1
	Inconsistent	-3

better performance of an APPG and a lower score indicates that there are more inconsistencies with user inputs or more terms generated by templates.

We also measure the similarity between generated privacy policies and the original privacy policies of boilerplate apps, *i.e.*, privacy policies from Facebook and Niantic.[1] We first store privacy policies into text files, then convert all uppercase characters into lowercase and remove all punctuation marks. We compute the TF-IDF [14] values for each word in privacy policies, where the word weighting is encoded by Equation (1) as follows.

$$w_{i,j} = tf_{i,j} \cdot \log\left(\frac{N}{df_i}\right), \tag{1}$$

where $w_{i,j}$ is the weight for word i in policy j, $tf_{i,j}$ is the frequency of word i in policy j, N is the number of documents in the collection, and df_i is the document frequency of word i in the collection. After applying TF-IDF analysis, we obtained a weight vector for each word in the privacy policy, where a high value indicates a high weight of this word in that policy.
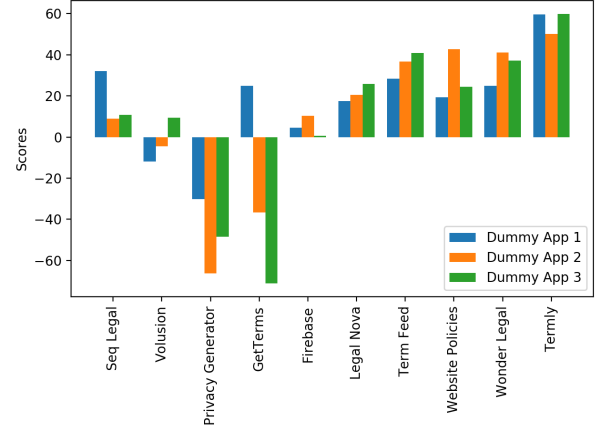
Cosine similarity is often used as an indicator of similarity between two documents. We applied this method according to Equation (2) to measure the similarity between the generated privacy policy and its original policy.

$$\text{cosine similarity} = \frac{V_g \cdot V_o}{\|V_g\| \cdot \|V_o\|}, \tag{2}$$

where V_g is the TF-IDF weight vector of generated privacy policy, V_o is the weight vector of original privacy policy. Because we design the functionalities of the boilerplate apps based on the original apps, a highly weighted word in the original privacy policy should also be weighted highly in the generated privacy policy. Hence, a high similarity rate indicates a high-quality APPG.

3 RESULTS AND ANALYSIS

To analyze the quality of APPGs, we generated 30 privacy policies with 3 boilerplate apps and 10 APPGs. Figure 2 shows the quality assessment results of these privacy policies. The scores are scaled into $[-100, 100]$ for comparison. The t-test applied on free and paid app scores indicates that there is significant difference in the performance of free and paid APPGs (see findings in detail below).
Finding 1. *The versatility of template is limited.* We can see that, for APPGs #1–#4, the assessment results of the three boilerplate apps are different, because they are in the form of templates or rely heavily on templates to generate privacy policies. The functions of apps are different from each other, so their scores change drastically. One template may generate a good quality privacy policy for a

---
[1]Niantic (https://nianticlabs.com) is a world's leading augmented reality game company, the developer of Pokémon Go.

Figure 2: The performance scores of APPGs evaluated by dummy apps.

specific app, but it may perform poorly when being applied to another app. For example, APPG #1 always generates a term that the app will not collect personal information from third parties. This is good enough for App 1, but it fails to match App 2 and App 3. The result shows that it is not a good solution to apply one template to all apps.
Finding 2. *Some APPGs generate over-scoped terms.* For APPGs #6, #7, and #9, the scores generally increase with the complexity of the boilerplate apps. This is mainly because the APPGs generate some personal information terms which are over-scoped of the ground truth that user inputs. For example, whatever the user input is, APPG #6 will, by default, generate terms to collect personal information, *e.g.*, email address, IP address, location information, which is heavily penalized for App 1 in our quality assessment.

As shown in Figure 3, we calculated the average quality score of each APPG and measure the similarity between generated privacy policies and the original ones. The scores of templates, free, and paid APPGs are marked as yellow, green, and blue, respectively. The red line represents the complexity of questionnaires encoded by the number of questions. The dashed line represents the similarity results.
Finding 3. *Keeping generated terms consistent with user input and ensuring the coverage rate of essential items is critical to high-quality policy generation.* The performance of APPGs mostly increases with the complexity of the questionnaire. However, for APPGs #8 and #9, despite more complex questionnaires, their performance is lower than APPG #7, which indicates that more complex survey questionnaires do not necessarily perform better. To achieve high quality, APPGs should consider more essential items in the design of questionnaires so as to ensure that a complete privacy policy is generated. In addition, users should be allowed to answer questions in a more flexible way, as some questions require users to provide more specific information rather than simply answering multiple choice questions; otherwise, the terms generated may not be consistent with the actual behavior of the app. For example, although APPG #8 has 30 questions in the survey, it never covers the item of cookies access and there is no text area for users to input which
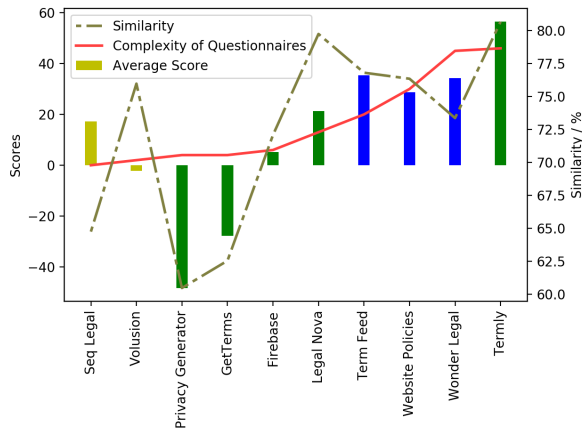
Figure 3: The performance of APPGs vs. complexity of questionnaire and similarity to original policies.

personal information will be collected. It will always claim the collection of device's IP address, location, and device name, lowering its quality score.

Finding 4. *The similarity score fluctuates with the quality assessment outcome.* The dashed line of Figure 3 reflects the similarity result of APPGs. For several APPGs, such as #1, #2, and #6, there are some gaps between similarity trend and scoring due to the fact that more penalties are pushed towards the low-quality terms which do not fit into actual user input.

Finding 5. *APPG quality is positively correlated to payment.* Considering the payment mode of APPGs shown in Table 1, free APPGs, such as #3–#6, perform less commendably than a well-designed template, evidenced by the fact that their quality scores are no greater than the template APPG #1. APPG #10 is an exception as it needs to be paid periodically for retrieving advanced features. Meanwhile, paid APPGs, such as #7–#9, normally have a more complex questionnaire and better perform than free APPGs.

4 CONCLUSION

We analyzed the privacy policies of popular apps and specified what categories and items a complete privacy policy should cover. Based on the essential items of privacy policy, we provide a method to assess the quality of online APPGs. The assessment results show that the performance of APPGs largely increases with the complexity of the survey questionnaires. Although there are still many template-generated terms which are potentially inconsistent with user's input, paid APPGs normally outperform free APPGs as a whole.

Most existing APPGs are in form of survey questionnaires. Even some APPGs claim that they do not make any templates, the method they applied is to collect user's answers and to fit them into a "smart" template. They only generate privacy policies relied on user's inputs (*e.g.*, answer questions). As lack of static or dynamic code analysis of apps, while using APPGs, developers and app users may encounter two types of serious issues. First, the generated policies could be incomplete because they did not cover all the essential items required by a privacy policy, *e.g.*, did not include all personal information collected by the app. Second, some generated policies

may be over-scoped, *e.g.*, they claim to collect personal information which is not in fact accessed by the app, and this may lead to potential inconsistency and legal issues. We strongly recommend that developers should systematically consult a professional legal team before releasing a privacy policy generated by APPGs. In future work, besides extending assessment to more APPGs, we will further optimize the APPG quality assessment through semantic analysis, and will conduct a more in-depth assessment as per the requirements of a specific regulation, *e.g.*, HIPAA or GDPR.

REFERENCES

[1] 1998. Children's Online Privacy Protection Act (COPPA). http://www.ftc.gov/ogc/coppa1.htm
[2] 2003. California Online Privacy Protection Act (CalOPPA). https://leginfo.legislature.ca.gov/
[3] Benjamin Andow, Samin Yaseer Mahmud, Wenyu Wang, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Tao Xie. 2019. Policylint: investigating internal privacy policy contradictions on Google play. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 585–602.
[4] Rebecca Balebako and Lorrie Cranor. 2014. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58.
[5] Sen Chen, Guozhu Meng, Ting Su, Lingling Fan, Minhui Xue, Yinxing Xue, Yang Liu, and Lihua Xu. 2020. An Empirical Assessment of Security Risks of Global Android Banking Apps. In *IEEE International Conference on Software Engineering (ICSE)*.
[6] Federal Trade Commission. 2016. Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission. https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked
[7] Marko Csokasi. 2019. 12 privacy policy generators to get GDPR compliant ASAP. https://digital.com/blog/best-privacy-policy-generators/
[8] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* 119 (2016), 1–88.
[9] Amanda Gaid. 2019. The 10 best privacy policy generators. https://au.oberlo.com/blog/privacy-policy-generator/
[10] Niharika Guntamukkala, Rozita Dara, and Gary Grewal. 2015. A machine-learning based approach for measuring the completeness of online privacy policies. In *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 289–294.
[11] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer. 2018. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 531–548.
[12] The legality. 2019. Best privacy policy generators for 2019. https://thelegality.com/reviews/best-privacy-policy-generators/
[13] Erika McCallister. 2010. *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing.
[14] Anand Rajaraman and Jeffrey David Ullman. 2011. *Mining of massive datasets*. Cambridge University Press.
[15] Rocky Slavin, Xiaoyin Wang, Mitra Bokaei Hosseini, James Hester, Ram Krishnan, Jaspreet Bhatia, Travis D Breaux, and Jianwei Niu. 2016. Toward a framework for detecting privacy policy violations in android application code. In *Proceedings of the 38th International Conference on Software Engineering*. ACM, 25–36.
[16] Welderufael B Tesfay, Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. 2018. PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*. ACM, 15–21.
[17] U.S. Dept. of Health and Human Services. 2000. Standards for Privacy and Individually identifiable health information; final rule. *Federal Register* 65, 250 (2000), 82462–82829.
[18] Le Yu, Tao Zhang, Xiapu Luo, Lei Xue, and Henry Chang. 2016. Toward automatically generating privacy policy for android apps. *IEEE Transactions on Information Forensics and Security* 12, 4 (2016), 865–880.
[19] Sebastian Zimmeck and Steven M Bellovin. 2014. Privee: An architecture for automatically analyzing web privacy policies. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. 1–16.
[20] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N Cameron Russell, and Norman Sadeh. 2019. MAPS: Scaling privacy compliance analysis to a million apps. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019), 66–86.