Apps, Code, Culture, and Market Reform: Examining Influences on Android Permissions

JONATHAN SCHUBAUER, JAYTI DEV, DAVID ARGAST, L. JEAN CAMP, and SAMEER PATIL, School of Informatics, Computing, and Engineering Indiana University Bloomington, USA

ABSTRACT

Consumers in the mobile application market can putatively protect their privacy with the use of permissions. This requires that mobile device owners understand app permissions and their privacy implications. Many analyses have been conducted to address consumer privacy issues with the current permission system in practice. However, few pay attention to how the global app markets have responded to recent privacy reforms. Using two data sets of 4,623 and 4,674 Android Application Packages (APK) on the Google Play Store we analyze the market changes of permissions in practice since the prior and post-enforcement of the GDPR. We compare popularity, category, data protection regime, and privacy law across three application categories (Game Age 5, Social, and Lifestyle) in three countries (United States, South Korea, and Germany) to examine influencing factors on Android permissions. We utilized the Android Parsing Package "Androguard" to extract permission data from the APK files. We then generated permission trends for both normal and dangerous run-time permissions to identify differences across three countries. Using this methodology we found one statistically significant change despite the small time window.

Additional Key Words and Phrases: Privacy regulation, General Data Protection Regulation (GDPR), Android apps, Privacy, Security, App permissions, Dangerous permissions, United States (US), European Union (EU), Germany, South Korea

1 INTRODUCTION

The Google Play store hosts millions of apps that can be downloaded for installation on devices running the Android operating system. The Google Play store guidelines require each app to declare the permissions it requires. Based on the notifications, the user can decide whether to grant each of the requested permissions.

However, people typically lack the technical knowledge necessary for understanding the implications of granting the various permissions. The notices regarding permissions often include technical and/or policy jargon, thus making them further inaccessible to the average user. As a result, people typically pay little attention to the notifications and tend to grant permissions whenever requested despite having the option to deny the requested permissions or not use the app. Moreover, there are frequent discoveries of apps using user-granted permissions in problematic ways, intentionally or unintentionally. Therefore, inadequate attention to the permissions granted to apps may significantly compromise the user's privacy and security.

The recent introduction of the General Data Protection Regulation (GDPR) by the European Union (EU) has the potential to have a significant impact the entire mobile ecosystem. In general the comprehensive nature and broad EU-wide jurisdictional reach of the GDPR means that any firm that wants access to the EU market is required to undertake a thorough analysis of its products and practices for GDPR compliance. Some organizations have taken the approach of creating GDPR-compliant versions of their products only for the EU market. On the other hand, given the costs of developing and maintaining multiple versions of the same product, many firms

Authors' address: Jonathan Schubauer; Jayti Dev; David Argast; L. Jean Camp; Sameer Patil, School of Informatics, Computing, and Engineering, Indiana University Bloomington, 901 E 10th St. Bloomington, Indiana, 47408, USA.

2019.

have chosen to offer GDPR-compliant products for their global user bases. The latter approach further ensures that the product will likely be compliant with privacy regulations in regions other than the EU even if these regions undertake privacy regulation reforms which many countries have chosen to do by drawing inspiration from the GDPR.

In the specific case of mobile apps, many have small development teams. If developers are required to minimize permissions for one jurisdiction then requiring additional permissions would require rewriting the code for different users, and ensuring that the correct versions were download by people in the corresponding market. Thus it is reasonable to believe the GDPR would have an effect on the overall use of permissions.

The interplay between privacy regulation and its impact on software is rather difficult to observe. However, the large extent to which implementation of the GDPR has affected industry practices and corresponding products provides a unique opportunity to examine the influence of privacy regulation on software systems on a global scale. we leveraged this opportunity to study whether the implementation of the GDPR impacted the implementation of Android apps in terms of their requests for permissions, especially ones that are particularly sensitive from the point of view of privacy and security.

To this end, we used the Google Play store to collect the Android Packages (APKs) of over 4,600 apps in three application categories (*Social*, *Lifestyle*, and *Ages 5 and Under*) from three different jurisdictions (US, Germany, and South Korea). We collected the APKs at two different times: once prior to the GDPR going into effect and again after the GDPR had been in effect for a few months. We then analyzed the APKs to compare the permissions requested by the apps before and after the GDPR went into effect.

We found that app requests for permissions that impact privacy and security did not increase after the GDPR went into effect even though the requests for other permissions were higher. We further found no notable post-GDPR differences in permission requests across the three targeted countries despite jurisdictional differences in privacy regulations. However, in each of the three countries, the permissions requested by apps differed based on the app category, with apps targeted at children requesting substantially fewer permissions compared to apps in the social and lifestyle categories targeted at teens and adults.

In the sections that follow we first outline the background of privacy and data protection regulation in the regions we targeted. We also address the role of permissions in the marketplace, with a focus on works studying consumer choice as well as over-permissioning. Next, we describe the details of our data collection and analysis processes followed by the main insight gained from our analyses. We close by addressing limitations and future work.

2 REGULATORY BACKGROUND

As the backdrop for our investigation, the following subsections outline the regulatory background regarding privacy and data protection in each of three countries we focused on: US, Germany, and South Korea. As a member of the EU, Germany is bound by privacy regulations from the EU in addition to its own country-specific aspects. This is an overview for the general reader, not legal analysis.

2.1 United States

The US takes a sectoral approach to privacy and data protection. As such, handling of privacy matters is dependent the purpose(s). Some prominent examples of sector-specific federal privacy and data protection laws include: The Fair Credit Reporting Act (FCRA), Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), and the Video Privacy Protection Act (VPPA). Any app will face different constraints based on its target industry, the data it handles, and even the demographics to which it is marketed. This is further complicated by the differences in states laws; sometimes also follow the sector based approach for state-specific privacy regulation.

With the sector based approach, regulatory compliance for privacy protection is narrow. For example, HIPAA compliance is not required for health relevant information collected by fitness tracking devices and apps because they do not meet the law's definition of 'covered entities' that are required to adhere to HIPAA. FCRA applies only to the protection of information contained in the records of the consumer credit reporting agencies. Yet payment for a medical product that has medical privacy implications is covered only by FCRA and not HIPAA. The sector-specific legislative scope can thus result in ostensibly personal information being unprotected because it falls outside regulatory coverage.

In order to manage for this range of protections, we selected the category of games targeted at five year old children, i.e., *Game Age 5*. As a result there is no question that the Children's Online Privacy Protection Act (COPPA) applies. COPPA provides clear and strong requirements for apps targeted at children; simultaneously five year olds will not have financial data nor be discussion scholarly or medical endeavors.

2.2 European Union

The EU defines privacy as "the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information." The EU considers privacy the fundamental human right that is recognized in the Universal Declaration of Human Rights. According to Article 8 of the European Convention on Human Rights (ECHR), an individual has the right to respect for "private and family life, of his home and his correspondence." just as the Universal Declaration declares freedom from interference in, "privacy, family, home or correspondence" in its own Article 12. The notion of 'family life' is not limited to other formal and legal relationships, but on relevant contexts equal to demonstrated commitment. The right to respect 'private life' is asserted as the right to privacy, the right to live, as far as one chooses, protected from the publicity of outside entities or public authority. In addition to the private life of an individual, Article 8 asserts that a public authority shall not interfere with exercise of private life with the exception of specific circumstances, such as national security interests. In addition, Articles 7 and 8 of the CRFEU conjointly reference the protection of personal data. The provisions of Articles 7 and 8 connect privacy in the context of private life, while linking control of personal information to an identifiable person, regardless of the context. .

2.3 Germany

In addition to the EU regulations, Germany has further enacted its own privacy regulations. The German laws were typically sector-specific akin to the US; but their citizens have the right to privacy as defined by the EU frameworks and practices. The primary German privacy and data protection law is the Federal Data Protection Act (*Bundesdatenschutzgesetz* – BDSG) which applies the EU Data Protection Directive to protect personal information from private and public entities. With the advent of the EU GDPR, Germany has revamped the BDSG to be GDPR-compliant via the German Data Protection Amendment Act (GDPAA).

2.4 South Korea

Protection of the private information of South Korean citizens is regulated in accordance with the Private Information Protection Act (PIPA). Chapter III of PIPA contains articles that detail the requirements which data processors using personally identifiable information must follow. In this, it is not unlike the HIPPA model. In particular, Article 22 of PIPA deals with methods permitted for obtaining consent from a data subject. Paragraph 2 of Article 22 states that consent can be obtained in the form of document that clearly informs the data subject about the type of information collected, its use and the purpose for which it is collected.

In conjunction with PIPA, South Korea follows additional sector-specific data protection laws. For instance, the Location Information Act regulates location information of mobile device users. Article 15 of the Location Information Act prohibits collecting the location information of a person without the explicit consent. Further,

Article 24 of the Location Information Act states that a person whose location information is collected can demand that the collector of the information stop or temporarily halt the collection or use and further allows the person to inspect how the collected information is used or shared with third parties.

3 RELATED WORK

In this section, we provide an overview of the literature which most informed this work. The vast literature of privacy provides a substrate but the two research threads most tightly woven into our research examine the influence of privacy regulation on industry and role of permission in decisions by developers as well as consumers of Android Apps.

3.1 Influences of Privacy Regulation

Two major questions addressed in the literature are the efficacy of regulating services providers and the effects of disclosure requirements. For instance, researchers have examined whether mandatory data breach disclosures incentivize firms to increase their investment in privacy and security. Acquisti et al. [1] found that a company's market value was negatively affected by a data breach, with the source of the breach and the market value of the company moderating the size of the effect. More recently, Martin et al. [10] showed that the negative effects of breaches further lead to spillovers leading to rival firms closely associated with the breached company experiencing loss of value as well. In addition to industry value and practices, literature has examined the impact of data breach regulation on consumers. In this regard, Romanosky et al. [12] found that data breach laws reduced identity theft by as much as 6.1%. While these studies examined immediate impact reflected in the stock market or gradual effects on consumer harm, our focus is on evolution of a company's product with changes in the relevant regulatory backdrop. A more similar study is the cross-state comparison of the growth of health information exchanges in the presence of both incentives to share data and privacy regulations. This comparison of state regulations found that privacy regulations in and of themselves do not effect information sharing in health exchanges (which exist to improve medical care). However, a combination of incentives for the creation of health information exchanges and privacy laws requiring clear consent did increase sharing of health information in HIEs for the purpose of improving patient outcomes. [3]

Other researchers have argued that privacy is a luxury good [6], with an upward sloping demand curve and consequently unusual market dynamics. This line of research was initially begun by Varian et al., who examined the distribution of subscribers to the DO Not Call List, and then analyzed the demographics of these zip codes. [14] By 2018, with ubiquitous voice spam and voice fraud, Sahin and Francillo found that adding a number to the DO Not Call lists in Spain and the UK reduced the volume of spam calls. Conversely, they also found that spammers appear to be using the Do Not Call list in the UK to identify valid numbers. [13] The more recent study did not explore the luxury good findings; but given the decreasing correspondence between location and phone number this would have been an uncertain endeavor.

Privacy is difficult to value. Surveys and expressed preferences find high valuations; while preferences revealed by market behavior often do not. [2] Sources of this variance include both irrational biases and rational choices. An example of a rational choice is not reading laborious privacy policies that are subject to immediate change. [16] The biases in privacy decision-making are those that are present in other risk/benefit decisions, and not unique to privacy. [9, 17]

3.2 Permission Requests by Android Apps

Permissions on Android apps have been extensively studies as a case of usable security and developer security behaviors. Android apps have been used by researchers to study the behavioral economics of privacy both by producers and consumers. Android apps permissions and their consequent impact on privacy and security has

received extensive research attention. Enck et al. [7] analyzed app permission request patterns to detect apps that could potentially be malicious and threaten privacy and security of the user. Felt et al. [8] analyzed 940 Android apps and found that nearly one third of them asked for more permissions than required for their operation. Such overprivileged apps were also observed by Vidas et al. [15]. Later Au [4] pointed out that there is a trade-off between supporting least-privilege security via fine-grained permissions and maintaining the stability of the permission specification as Android evolves. Yet some of the permissions noted by Felt et al. were not actually accessible to the app, or declinated and not longer available. This undermines the argument that the minimal app set is selected. Yet there can be a tradeoff in some situations. To address this trade-off, Barrera et al. [5]'s empirical analysis of Android apps applies visualization techniques to surface potential improvements to the permissions model that can increase expressiveness where needed without increasing the total number of permissions or overall complexity. While these technical approaches have typically examined permission request patterns across apps at a single point in time, we compare permission requests across different versions of the same app. The research efforts described above attempt to connect permissions with technical aspects, such as source code, Application Programming Interfaces (APIs), software architecture, etc. In contrast, we attempt to link observed permission patterns to external regulatory influences and jurisdictional differences.

4 METHOD

To tackle our research objective, we analyzed permission requests across datasets of Android apps collected at two different times, once prior to the GDPR going into effect and again after the GDPR had been in effect for a few months. In the next subsections, we describe our data collection processes and rationale.

As mentioned earlier, our investigation targeted three countries: US, Germany, and South Korea. The three countries differ in terms of regulatory and cultural considerations regarding privacy. Further, collectively they represent one of the major global market regions, North America, Europe, and Asia, respectively.

Given the large number and category of Android apps available in each of the chosen countries, we chose to focus on three app categories: Social, Lifestyle, and Ages 5 and Under. Apps in each of these categories are available in all three countries we targeted. In fact, the Social and Lifestyle are among the most popular app categories in each country. The Ages 5 and Under category was added to provide a potential contrast to the other two categories given the niche target audience and function and the greater privacy protection mandated for matters pertaining to children. In contrast, apps in the Social and Lifestyle categories typically cover a diversity of functions and target an audience of adults or teens. Moreover, narrowing the focus to three categories kept the scope of our study within reasonable limits. Further, we limited our collection only to apps available for free since we wished to download and analyze the app files for analysis.

Based on the above described scope, we used the Google Play stores of each of three targeted countries to retrieve lists of the top free apps in each of the three selected categories. Each of the 9 lists consists of the top apps in the respective country for the respective category, with each list containing a rank ordered list of 540 apps, which is the maximum number of apps listed by the Google Play store.

Since the Google Play store does not make it possible to download an app to a non-Android device, we used third party app download sites https://apkpure.com and https://www.apkmirror.com to retrieve each of the apps in the list based on the corresponding package identifier. As mentioned earlier, we carried out the data collection twice, one before and once after the GDPR had gone into effect, thus providing us with the two datasets we used for our comparative analyses.

We retrieve the list of permissions requested by each app by parsing the respective app file with the tool Androguard (https://github.com/androguard/androguard). For each of the requested permission in the list, we marked whether the permission was classified by Android as 'Normal' or 'Dangerous.' The Android developer documentation classifies permissions that pose minimal to no risk to privacy and security as Normal permissions

	Social		Lifestyles		Ages 5 & Under	
Country	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR
US	17.25	18.98	14.43	14.45	6.95	7.58
Germany	16.82	18.10	11.88	13.43	6.86	7.43
South Korea	19.03	20.59	14.05	14.52	7.80	9.00**

* = 0.05, ** = 0.01, *** = 0.001

Table 1. Average total permissions requests by apps before and after GDPR went into effect.

which are granted to an app automatically upon request. An example of such a permission is the SET_WALLPAPER permission that allows an app to set a background image for the home screen of the device. In contrast, permissions that can potentially have a notable impact on privacy and security are considered Dangerous permissions that require agreement from the user prior to being granted to an app. Specifically, Dangerous permission cover various permissions pertaining to accessing the calendar, call log, camera, contacts, location, microphone, phone, device sensors, SMS, and files stored on the device. For example, the READ_CONTACTS permission that allows an app to access a user's contacts is considered a Dangerous permission.

5 FINDINGS

Out of the possible 4860 apps for each dataset, we were able to download and parse 4,623 and 4,674 apps in the pre-GDPR and post-GDPR data collection, respectively. In this section, we report the salient insight gained by analyzing the permissions requests of these apps.

Overall, the 4,623 apps in the pre-GDPR dataset requested a minimum of 0 to a maximum of 436 permissions with a mean of 12.74 and a median of 9 permission requests. The 4,674 apps in the post-GDPR dataset request a minimum of 0 to a maximum of 436 permissions with a mean of 13.75 and median of 10.

Perhaps surprisingly, we found that the average number of permissions requested by apps taken together across countries and categories increased after the GDPR went into effect (pre-GDPR mean = 12.74 vs. post-GDPR mean = 13.75). Welch's two sample t-test indicates that the difference is statistically significant (t = -3.1989, df = 9294, p = 0.001384). Notably, the increase appears to be driven by increased requests for normal permissions (pre-GDPR mean = 9.67 vs. post-GDPR mean = 10.66; t = -3.5383, df = 9294.9, p = 0.0004046). The requests for dangerous permissions are nearly the same pre- and post-GDPR with no statistical difference between them (pre-GDPR mean = 3.06 vs. post-GDPR mean = 3.09).

Table 1 provides a more detailed overview of the pre- and post-GDPR permission requests split across the three countries and categories we studied. As can be expected, Table 1 shows that in all three countries apps targeted at children under the age of 5 request far fewer permissions compared to those in the Social and Lifestyles categories. Pairwise Welch's t-tests indicate that differences across permission categories are statistically significant pre- and post-GDPR (Bonferroni-correct $p < 0.001$ in all cases). The trend holds even when normal and dangerous permissions are examined separately. While the average number of permissions requested post-GDPR is slightly higher in all categories in all countries, the differences are not statistically significant with the exception of Ages 5 & Under apps in South Korea (t = -3.2464, df = 862.76, Bonferroni-corrected p = 0.01). The increase in permission requests in the Ages 5& Under category in South Korea may be attributed to a statistically significant increase in normal permissions (t = -3.5443, df = 862.69, Bonferroni-corrected p = 0.0037296); the corresponding differences in requests for dangerous permissions are not statistically significant.

Although we found no statistically significant differences in pre- and post-GDPR requests for dangerous permissions, given their impact on privacy and security, it is worth taking a deeper look at the individual

dangerous permission requests to identify patterns of potential effort. Tables 2, 3, and 4 provide the number of apps that requested each of the 26 dangerous permissions in each of the three countries, respectively. As the tables indicate, the request patterns are nearly the same across the three countries.

Requests for some of the permissions were far more common than others. The most commonly requested permissions include: CAMERA, READ_CONTACTS, GET_ACCOUNTS, ACCESS_FINE_LOCATION, RECORD_AUDIO, READ_PHONE_STATE, READ_EXTERNAL_STORAGE, and WRITE_EXTERNAL_STORAGE. However, with the exception of READ_PHONE_STATE and WRITE_EXTERNAL_STORAGE, even these commonly requested dangerous permissions were included by substantially fewer apps targeted at children ages 5 and under with some being not asked by any app at all.

Interestingly, not a single app in any category in any of the countries asked for any of the following dangerous permissions: READ_PHONE_NUMBERS, ANSWER_PHONE_CALLS, and ADD_VOICEMAIL. Additionally, the following dangerous permissions are requested by only a handful of apps: WRITE_CALL_LOG, USE_SIP, BODY_SENSORS, RECEIVE_WAP_PUSH, and RECEIVE_MMS. It may be the case that these permissions are not needed for the functionality offered by the apps in the specific categories we chose. For instance, we may find that apps in categories related to health and fitness request the BODY_SENSORS to a much larger extent. Alternatively, the specific aspects covered by these permissions may be rarely required by any app in general.

6 DISCUSSION AND IMPLICATIONS

When comparing app permission requests before and after the GDPR went into effect, we found a statistically significant but small increase in average requests for normal permissions when considering all apps taken together across countries and categories. We found no other statistically significant differences, even in the case of EU member Germany. Note that the increase in permissions predated the introduction of the GDPR. The particular permission READ_PHONE_STATE in games for children also dramatically decreased.

One issue in evaluating the impact of policy is the time period for the analysis. We risked finding no changes by targeting the collection window very tightly around the GDPR regulatory adoption date. With a larger window, we might search for more effects. Yet a larger window also includes more factors that could impinge the choice of permissions.

In fact, the lack of an increase in the privacy and security affecting dangerous permissions may itself be considered a regulatory success given that other permission requests increased during the same period. As such, the small increase in post-GDPR permissions requests appears to be driven primarily by core app functions unrelated to privacy and security. A long term analysis could determine if this is the case, particularly given access to datasets compiled well before the GDRP.

Additionally the dangerous permissions on Android require explicit user opt-in by design, thus met GDPR consent requirements even before the GDPR went into effect. Given the literature included on the efficacy of the interaction, this arguably reflects a limitation of the GDPR which does not address the timing or efficacy of the notification.

Of course we simply may have selected the wrong inflection point. The GDPR included a multiple year preparatory period prior to the date on which it went into full effect. As a result, app makers may have already taken GDPR into account by the time we collected our pre-GDPR data. Alternatively, it may be the case that our post-GDPR data collection occurred before app makers had fully implemented GDPR compliance since comprehensive software changes can sometimes take a substantial amount of time. The statistically significant differences in permission requests by apps targeted at young children, suggest that app makers do indeed seem to be taking regulatory compliance into account and attempting to minimize requests for permissions. That said, the differences in request patterns could also be attributed to differences in the core functionality of apps in a given category.

	Social		Lifestyles		Ages 5 & Under	
Country	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR
READ_CALENDAR	3%	4%	4%	0%	0%	0%
WRITE_CALENDAR	2%	3%	3%	3%	0%	0%
READ_CALL_LOG	4%	5%	1%	1%	0%	0%
WRITE_CALL_LOG	2%	2%	0%	0%	0%	0%
PROCESS_OUTGOING_CALLS	4%	4%	1%	2%	0%	0%
CAMERA	39%	42%	34%	36%	9%	10%
READ_CONTACTS	25%	29%	13%	14%	0%	1%
WRITE_CONTACTS	8%	8%	1%	2%	0%	0%
GET_ACCOUNTS	38%	39%	25%	27%	4%	4%
ACCESS_FINE_LOCATION	46%	45%	49%	52%	4%	3%
ACCESS_COARSE_LOCATION	45%	43%	43%	46%	5%	4%
RECORD_AUDIO	31%	30%	10%	12%	7%	8%
READ_PHONE_STATE	43%	39%	34%	33%	21%	11%
READ_PHONE_NUMBERS	0%	0%	0%	0%	0%	0%
CALL_PHONE	6%	7%	9%	11%	0%	0%
ANSWER_PHONE_CALLS	0%	0%	0%	0%	0%	0%
ADD_VOICEMAIL	0%	0%	0%	0%	0%	0%
USE_SIP	1%	1%	0%	0%	0%	0%
BODY_SENSORS	0%	0%	0%	0%	0%	0%
SEND_SMS	8%	7%	4%	4%	0%	1%
RECEIVE_SMS	8%	9%	6%	4%	0%	1%
READ_SMS	6%	7%	3%	3%	0%	0%
RECEIVE_WAP_PUSH	1%	1%	0%	0%	0%	0%
RECEIVE_MMS	2%	1%	0%	0%	0%	0%
READ_EXTERNAL_STORAGE	54%	59%	38%	46%	12%	12%
WRITE_EXTERNAL_STORAGE	84%	79%	67%	75%	67%	57%

Table 2. Number of apps in the US requesting dangerous permissions before and after GDPR went into effect.

Finally, changes in permission requests are only one aspect of an app that is affected by considerations of compliance with privacy regulation. Privacy and security can be affected by a number of other components of the app system, such as third party libraries included within the app, mechanisms and policies for remote storage of app data, operational functionality. Pre-GDPR hardening of privacy and security owing to changes in such non-permission aspects cannot be captured by our method.

A thorough examination of regulatory impact that addresses the above issues would require longitudinal data collection of app permissions at multiple points over the course of several years along with supplementary investigations of non-permission app components and app developer practices. Moreover, analysis of specific permission could be important for relevant sector-specific regulation. For instance, the permissions related to location can be examined for compliance with laws pertaining to the handling of location information. Our findings further suggest that analyzing app permissions could help identify individual apps for further scrutiny regarding regulatory compliance. Apps with permission request patterns that are unusual in comparison with

	Social		Lifestyles		Ages 5 & Under	
Country	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR
READ_CALENDAR	3%	4%	2%	3%	0%	0%
WRITE_CALENDAR	2%	3%	1%	2%	0%	0%
READ_CALL_LOG	4%	4%	2%	2%	0%	0%
WRITE_CALL_LOG	2%	2%	0%	0%	0%	0%
PROCESS_OUTGOING_CALLS	4%	3%	1%	2%	0%	0%
CAMERA	36%	39%	30%	31%	8%	8%
READ_CONTACTS	22%	21%	8%	11%	0%	1%
WRITE_CONTACTS	7%	7%	1%	1%	0%	0%
GET_ACCOUNTS	34%	35%	21%	20%	3%	4%
ACCESS_FINE_LOCATION	44%	41%	40%	42%	4%	2%
ACCESS_COARSE_LOCATION	42%	38%	34%	37%	4%	4%
RECORD_AUDIO	27%	29%	10%	12%	7%	8%
READ_PHONE_STATE	34%	34%	28%	29%	22%	11%
READ_PHONE_NUMBERS	0%	0%	0%	0%	0%	0%
CALL_PHONE	6%	6%	5%	7%	0%	0%
ANSWER_PHONE_CALLS	0%	0%	0%	0%	0%	0%
ADD_VOICEMAIL	0%	0%	0%	0%	0%	0%
USE_SIP	1%	1%	0%	0%	0%	0%
BODY_SENSORS	0%	1%	0%	0%	0%	0%
SEND_SMS	6%	6%	1%	3%	0%	1%
RECEIVE_SMS	8%	9%	5%	3%	0%	0%
READ_SMS	5%	5%	2%	2%	0%	0%
RECEIVE_WAP_PUSH	1%	1%	0%	0%	0%	0%
RECEIVE_MMS	1%	1%	0%	1%	0%	0%
READ_EXTERNAL_STORAGE	48%	52%	39%	43%	10%	17%
WRITE_EXTERNAL_STORAGE	80%	79%	69%	71%	68%	56%

Table 3. Number of apps in Germany requesting dangerous permissions before and after GDPR went into effect.

other apps in the same category or region could be selected for regulatory oversight by policy makers as well as app distributors.

Our findings suggest that the number of permissions that are requested by apps is increasing. Given that previous examinations showed over-permissions it is highly unlikely that a large majority of app makers appear to be requesting only the permissions they need. Other than games for children these was not evidence in avoiding overprivileging. Similarly minimization does not appear to be practiced regarding the precision of the permissible data collected. This is aptly illustrated by the ACCESS_COARSE_LOCATION being dominated by ACCESS_FINE_LOCATION. Presumably, the functionality of at least some of the apps would probably not be affected by less precise location information. Yet, without exceptions, app makers seem to request highly precise location. Recall that the Android dialog asking for user consent for granting location access to an app does not specify whether an app is requesting fine or coarse location information.

The lack of notable differences in permission patterns across the three countries we studied indicates that app makers are likely to maintain the same permission profiles for an app in all regions of the world. As such, apps

Country	Social		Lifestyles		Ages 5 & Under	
	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR	Pre-GDPR	Post-GDPR
READ_CALENDAR	3%	4%	2%	3%	0%	0%
WRITE_CALENDAR	2%	4%	1%	2%	0%	0%
READ_CALL_LOG	4%	5%	2%	2%	0%	0%
WRITE_CALL_LOG	1%	2%	1%	1%	0%	0%
PROCESS_OUTGOING_CALLS	5%	5%	3%	3%	0%	0%
CAMERA	44%	48%	28%	31%	16%	20%
READ_CONTACTS	25%	25%	13%	16%	0%	4%
WRITE_CONTACTS	8%	9%	5%	5%	0%	0%
GET_ACCOUNTS	47%	44%	38%	33%	7%	13%
ACCESS_FINE_LOCATION	39%	41%	39%	39%	3%	6%
ACCESS_COARSE_LOCATION	38%	39%	34%	34%	4%	5%
RECORD_AUDIO	30%	32%	9%	8%	8%	13%
READ_PHONE_STATE	57%	52%	52%	51%	30%	18%
READ_PHONE_NUMBERS	0%	0%	0%	0%	0%	0%
CALL_PHONE	15%	14%	24%	25%	0%	0%
ANSWER_PHONE_CALLS	0%	0%	0%	0%	0%	0%
ADD_VOICEMAIL	0%	0%	0%	0%	0%	0%
USE_SIP	1%	1%	0%	0%	0%	0%
BODY_SENSORS	0%	1%	0%	0%	0%	0%
SEND_SMS	10%	10%	5%	7%	0%	1%
RECEIVE_SMS	15%	15%	16%	16%	1%	4%
READ_SMS	7%	8%	8%	7%	0%	1%
RECEIVE_WAP_PUSH	1%	1%	1%	1%	0%	0%
RECEIVE_MMS	1%	1%	3%	2%	0%	0%
READ_EXTERNAL_STORAGE	60%	64%	46%	49%	17%	24%
WRITE_EXTERNAL_STORAGE	84%	82%	70%	70%	69%	54%

Table 4. Number of apps in South Korea requesting dangerous permissions before and after GDPR went into effect.

that have a broad distribution are likely to require regulatory compliance regarding privacy and security with the strictest regulations across the regions they serve. Strict and comprehensive regulations in a major global market, such as the EU GDPR, can improve privacy and security of apps even for those that are outside its jurisdiction.

7 LIMITATIONS AND FUTURE WORK

While we can conjecture that privacy and data protection regulation has at least some influence as a factor that explains our findings, the extent of regulatory impact would require additional corroboration via complementary methods, such as a study software development and privacy compliance practices. Apart from confirming the extent of regulatory influence, such complementary research can surface additional impact on the app architecture beyond permissions requests.

Since many apps are distributed and used on a broad global scale, we found many of the same apps present in our lists for the three targeted countries. For instance, 151 top Social apps appeared in US as well as South Korea, 319 were found in the US and Germany, and 161 were common to Germany and South Korea. On the one

hand, such large overlap in apps can impact the comparisons of apps across countries. On the other hand, the overlap can surface how app makers are implementing permission requests across countries. Future work can refine our insight by additional analyses that compare permission patterns for apps that are available only in a single country or region.

Our data covers only three countries and only three app categories within those countries. Further, our data is restricted to free and top ranked Android apps within these countries and categories. Future studies that include additional countries, app categories, and operating systems are needed to verify the extent of generalizability of our findings. Such studies can further examine paid apps and apps that are ranked lower than top 540.

The data range of our study was small. The first data was compiled November 20, 2017 and the second June 6, 2018. Yet even in this window there were conflating events. The goal was to concentrate on the response to GDPR. Even then there are other events that may have impinged the data compilations. In December, 2018 consumer groups presented the Federal Trade Commission with a demand based on a study of COPPA violations of children‘s apps. [11] The effects of the research and the concurrent GDPR deadline cannot be separated without qualitative inquiries with decision-makers.

8 CONCLUSION

We have conducted a quantitative analysis on Android application permissions to determine if these Android permissions are shaped by underlying factors such as location, file size, ranking, category, age and Privacy Legislation. In total, two datasets of 4623 and 4674 applications were collected and analyzed across three locations (United States, South Korea and Germany) and three categories (Social, Lifestyle and Games Ages 5 and Under) in different time periods.

The comprehensive nature and simultaneous large-scale rollout of the EU GDPR provided a unique opportunity to compare privacy and data protection handling by apps before and after the GDPR went into effect, thus providing a potential means to surface regulatory impact. To this end, we examined pre-GDPR and post-GDPR app permission requests which are one of the means by which apps handle privacy and data protection. In fact, Android designates certain permissions as dangerous permissions due to their potential impact on user privacy and security. We found no post-GDPR increase in the requests for these dangerous permissions while there was an increase in the requests for other permissions it was not statistically significant.

Even though the GDPR affects only the EU, we found no differences between the three countries we targeted, only one of which is in the EU.

The reason for lack of a difference cannot be determined. There is a critical need for such qualitative investigation. One possibility is that makers of apps that are used worldwide may be likely to take a global rather than regional approach to privacy and security compliance. Such an approach would require adhering to the strictest of the privacy and data protection regulations across the world, thus potentially resulting in indirect broadening of regulatory impact beyond the jurisdiction in which it originates.

Longitudinal collection and analysis of app permissions on a global scale can serve as one of the tools for gauging the impact and helping identify targets for additional scrutiny and oversight.

ACKNOWLEDGMENTS

We thank Yonjae Lee for guidance regarding South Korean policy. This research was supported in part by funding from the National Science Foundation (Grant CNS 1565375), Cisco Research (Award 591000), and Comcast Innovation Fund. The contents of the paper are solely the work of the authors and do not represent the views of the sponsors.

REFERENCES

[1] Alessandro Acquisti, Allan Friedman, and Rahul Telang. 2006. Is there a cost to privacy breaches? An event study. http://aisel.aisnet.org/icis2006/94. *Proceedings of the Twenty-Seventh International Conference on Information System*, 1563–1580.

[2] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of Economic Literature* 54, 2 (2016), 442–92.

[3] Idris Adjerid, Alessandro Acquisti, Rahul Telang, Rema Padman, and Julia Adler-Milstein. 2015. The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science* 62, 4 (2015), 1042–1063.

[4] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, and David Lie. 2012. PScout: Analyzing the Android Permission Specification. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*. ACM, New York, NY, USA, 217–228. https://doi.org/10.1145/2382196.2382222

[5] David Barrera, H. Güneş Kayacik, Paul C. van Oorschot, and Anil Somayaji. 2010. A Methodology for Empirical Analysis of Permission-based Security Models and Its Application to Android. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*. ACM, New York, NY, USA, 73–84. https://doi.org/10.1145/1866307.1866317

[6] Rainer Böhme, Sven Koble, and TU Dresden. [n.d.]. On the viability of privacy-enhancing technologies in a self-regulated business-to-consumer market: Will privacy remain a luxury good?. In *Workshop on the Economics of Information Security*.

[7] William Enck, Machigar Ongtang, and Patrick McDaniel. 2009. On Lightweight Mobile Phone Application Certification. In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*. ACM, New York, NY, USA, 235–245. https://doi.org/10.1145/1653662.1653691

[8] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android Permissions Demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11)*. ACM, New York, NY, USA, 627–638. https://doi.org/10.1145/2046707.2046779

[9] Vaibhav Garg and Jean Camp. 2013. Heuristics and biases: implications for security design. *IEEE Technology and Society Magazine* 32, 1 (2013), 73–79.

[10] Kelly D. Martin, Abhishek Borah, and Robert W. Palmatier. 2017. Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing* 81, 1 (2017), 36–58. https://doi.org/10.1509/jm.15.0497 arXiv:https://doi.org/10.1509/jm.15.0497

[11] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. âĂIJWonâĂŹt Somebody Think of the Children?âĂİ Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83.

[12] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti. 2011. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management* 30, 2 (2011), 256–286. https://doi.org/10.1002/pam.20567 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/pam.20567

[13] Merve Sahin and Aurélien Francillon. 2018. On the effectiveness of the national do-not-call registries. In *Workshop on Technology and Consumer Protection*. IEEE Symposium on Security and Privacy.

[14] Hal Varian, Fredrik Wallenberg, and Glenn Woroch. 2005. The demographics of the do-not-call list [security of data]. *IEEE Security & Privacy* 3, 1 (2005), 34–39.

[15] Timothy Vidas, Nicolas Christin, and Lorrie Cranor. 2011. Curbing android permission creep. In *Proceedings of the Web 2.0 Security and Privacy (W2SP 2011)*, Vol. 2. 91–96.

[16] Tony Vila, Rachel Greenstadt, and David Molnar. 2003. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In *Proceedings of the 5th international conference on Electronic commerce*. ACM, 403–407.

[17] Ryan West. 2008. The psychology of security. *Commun. ACM* 51, 4 (2008), 34.