Kesler, Reinhold; Kummer, Michael E.; Schulte, Patrick

Working Paper

Mobile applications and access to private data: The supply side of the Android ecosystem

ZEW Discussion Papers, No. 17-075

Provided in Cooperation with:
ZEW - Leibniz Centre for European Economic Research

Suggested Citation: Kesler, Reinhold; Kummer, Michael E.; Schulte, Patrick (2017) : Mobile applications and access to private data: The supply side of the Android ecosystem, ZEW Discussion Papers, No. 17-075, Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim, https://nbn-resolving.de/urn:nbn:de:bsz:180-madoc-441770

This Version is available at:
https://hdl.handle.net/10419/173248

Discussion Paper No. 17-075

Mobile Applications and Access to Private Data: The Supply Side of the Android Ecosystem

Reinhold Kesler, Michael Kummer,
and Patrick Schulte

ZEW

Zentrum für Europäische
Wirtschaftsforschung GmbH

Centre for European
Economic Research

Discussion Paper No. 17-075

Mobile Applications and Access to Private Data: The Supply Side of the Android Ecosystem

Reinhold Kesler, Michael Kummer,
and Patrick Schulte

Mobile Applications and Access to Private Data:

The Supply Side of the Android Ecosystem*

Reinhold Kesler†
Centre for European
Economic Research (ZEW)

Michael Kummer‡
Georgia Inst. of Tech. &
Centre for European
Economic Research (ZEW)

Patrick Schulte§
Centre for European
Economic Research (ZEW)

December 2017

Abstract

We analyze the data collection strategies of 65,000 developers in the market for mobile applications and track 300,000 applications over four years. Many apps belong to developers with multiple apps. This fact generates variation in the privacy behaviors of the same developer for our analysis. We uncover three stylized facts: First, developers "learn" to use increasingly intrusive data strategies as they become more experienced. Second, intrusive data collection is most likely in apps that target the 13+, and 16+ age category, which raises concerns for the protection of young app consumers. Third, even within developers, critical and atypical permissions predict problematic usage of private user data most successfully. Our findings inform both regulators and scientists who wish to model supply in the market for mobile apps.

Keywords: Mobile Applications, Developers, Learning, Data Collection, Privacy
JEL Classification Numbers: O3, L1, D62, D85, D29

*We thank Ginger Jin, Alessandro Acquisti, and the participants in seminars at the PEP scholar conference at George Mason University and at the FTC for their thoughtful suggestions. Financial support from the PEP privacy fellowship and the Thyssen foundation is gratefully acknowledged.

†P.O. Box 103443, D–68034 Mannheim, Germany. Email: kesler@zew.de.

‡Corresponding Author. 221, Bobby Dodd Way Atlanta, GA, 30332, U.S.A; Phone: +1-404-385-4802; Email: michael.kummer@econ.gatech.edu.

§P.O. Box 103443, D–68034 Mannheim, Germany. Email: schulte@zew.de.

1 Introduction

The value of private data has become a central theme of the (economic) public debate. On the one hand, new technologies like mobile apps bear enormous potential to increased welfare by facilitating better information flows, choices, and efficiency. On the other hand, too much data in the wrong hands may also imply significant societal risks.[1]

In this paper, we use transaction-based evidence to study developers' strategies with respect to privacy-sensitive information in this market. Specifically, we focus on predicting which types of applications, and which types of developers are more likely to request intrusive access to user information. To this end we analyze data on 300,000 mobile applications (henceforth "apps") from more than 65,000 developers on Google's Play Store. The app market is relevant for our question, because apps have transformed information exchanges in less than eight years, and they offer unseen potentials for collecting private user information at low cost. Moreover, Android's operating system highlights an app's ability to access private information of users.

We combine the information on each app's ability to collect personal information with a rich data set on 300,000 apps from Google's Android Market in 2012. The data covers all publicly available app-specific information including each app's number of installation, its price and even each app's closest competitors. We collected the data repeatedly in 2012 (over 6 months) and once in 2014. We augmented these data with information from *privacygrade.org* to add further background information about app providers and permissions, and collected an additional data wave in 2016.

With these data we analyze two overarching questions: (i) What strategies do developers use regarding private data? (ii) Which app developers are more prone to privacy-intrusive choices? We first analyze, whether developers are "born" with different strategies, or whether they "learn" to use more or less intrusive data strategies as they become more experienced. Second, we analyze, whether intrusive data collection and sharing

[1]Experts had issued warnings about the possibilities of tracking individuals online already for many years. While these were widely ignored before 2013, the news of the U.S. National Security Administration's (NSA) data gathering and analysis has increased public awareness and raised considerable concerns. According to the Pew Research Center, 68% of adults believe current laws to insufficiently protect individuals' online privacy (Rainie et al., 2013).

with third parties varies by app category, by maturity rating, or by the competitive environment. Finally, we study which of these factors are the most relevant predictors for problematic usage of private user data two years later.

In our main analysis, we study how the same developers vary their behavior in different app environments, and how these differences affect their app's success. Focusing on apps by the same developer is useful, because it would be misleading to analyze merely the cross-sectional correlation between an app's environment and its behavior concerning user data due to the heterogeneity among app developers and their potentially different programming and marketing strategies. Therefore, we limit the role of developer heterogeneity using a panel approach with a developer fixed effect, where we compare only app developers that have gathered some experience.

Our findings inform both policy makers who consider regulating the market for mobile apps and scientists who wish to model this market's supply side. We provide the first large-scale and transaction-based evidence to help understand developers' privacy strategies and how they influence app success. By shedding light on the developers' trade offs, our research informs the debate about privacy concerns and regulation in the market for mobile apps. Additionally the insights from our project will serve as the foundational input to developing a structural approach to estimating the value of privacy-sensitive data for app developers.

2 Contribution to the Literature

The main result from the literature on privacy in economics has uncovered a substantial tension between the suppliers and the users of digital services. While consumers demand privacy and might lose their trust in the market if *too much* personal data is stored (Acquisti et al., 2016, 2015; Miller and Tucker, 2009), market success of new digital technologies may depend on the services' ability to collect and analyze *enough* personal information (Aziz and Telang, 2016; Goldfarb and Tucker, 2011; Johnson, 2013). Our paper provides insight into this tension, by analyzing how developers of mobile apps request

access to user data, and how they vary their strategies for data collection.

A large stream of literature studied the demand for privacy. Generally users were found to demand privacy (Marthews and Tucker, 2017; Turow et al., 2009), and demand was found to change over time (Goldfarb and Tucker, 2012), and to depend on context or framing (Acquisti et al., 2013; Gross and Acquisti, 2005). Existing research on private information in app markets is based on experimental and survey data, and the estimated valuations ranged from zero to very large numbers (Beresford et al., 2012; Carrascal et al., 2013; Grossklags and Acquisti, 2007; Racherla et al., 2011; Tsai et al., 2011). Savage and Waldman (2015) find an average valuation of $4 as the self-reported willingness to accept for giving away personal information that is typically shared with app developers of mobile apps. More technical studies investigated the implications of certain permissions for the privacy of the device's owner (e.g. Chia et al., 2012; Egelman et al., 2013; Sarma et al., 2012), their potential intrusiveness (e.g. Chia et al., 2012; Fahl et al., 2012), and positive effects of locally storing sensitive user data (Sutanto et al., 2013).[2]

A small but growing stream of research focused on private information and supply in online markets. Preibusch and Bonneau (2013) analyze data collection policies of Internet sites, and a series of related studies analyzes how privacy policies affect users of social networks or the success of targeted advertisement (Aziz and Telang, 2016; Goldfarb and Tucker, 2011; Johnson, 2014; Tucker, 2012, 2014).[3]

Hardly any of the above-mentioned studies analyzes transaction-based empirical evidence on the role of personal data in the market for mobile applications, and none of them focuses on developers' strategies to obtain private user data. We fill this gap by providing the first large-scale quantitative evidence on the role of privacy-sensitive information for app developers' strategies and their success in the market for mobile apps. Most closely

[2]For a survey of the literature on the economics of privacy, see Acquisti et al. (2016).

[3]Theory models suppliers who use their knowledge about an agent's preferences to price discriminate (Acquisti and Varian, 2005; Conitzer et al., 2012; Taylor, 2004; Taylor et al., 2010; Wathieu, 2002). Alternatively, they may attempt direct marketing, which consumers might seek to avoid (Hann et al., 2008; Johnson, 2013; Taylor et al., 2010). Taken together, these models see reduced privacy as disadvantageous for consumers. However, reduced privacy may allow to provide valuable services "for free" and can create benefits for users. Several papers studied the general functioning of app markets, and focused on structurally estimating the demand for selected apps (Ghose and Han, 2014), innovation (Davis et al., 2014; Yin et al., 2014), the role of bestseller ranks (Carare, 2012), or large scale promotions on sales (Askalidis, 2015; Chaudhari, 2015).

related to this paper is Kummer and Schulte (2016) analyzing the role of privacy as a second currency in app markets.[4] We build on their limited analysis of supply side behavior, and expand the data with outcomes from *privacygrade.org*, third-party data sharing and survival until 2016 to focus on developers of multiple apps, and how they vary their data strategies with time and their app's environment.

We provide the first evidence on the role of personal data in the market for mobile applications. We base this evidence on large and detailed panel data that covers almost all apps in the Android Market from 2012 and tracks them until 2016. Our data set is unique, because we observe app ownership, and see which permissions developers requested for each of their individual apps, before they could be installed. This information allows us to investigate developers' strategies regarding personal information and privacy, and to which extent app success depends on personal user information. We are the first to analyze multiple apps of the same supplier and how they negotiate the trade-offs surrounding privacy-sensitive information.

3 Background

Mobile applications from Google's Play Store are both relevant and suitable for the purposes of our study. Google's Android operating system was released in 2008 and nowadays dominates the market. Google's platform for the distribution of apps is the "*Google Play Store*." The platform, which serves as a distribution channel for apps, books, movies, music and newspapers featured approximately 300,000 apps in 2012, and 1.6 million apps in 2016. In 2015, the revenue of the store was near $40 billion and is expected to reach $100 billion in 2020 (App Annie, 2016).

Specifically, app market data are informative for analyzing how developers use private user data, because we can exploit Google's unique policy of highlighting an app's ability to access private information of users. Android's operating system confronts all users with the complete list of rights (henceforth "permissions") that an app requests. The

[4]Casadesus-Masanell and Hervas-Drane (2015) analyzed privacy as a "second currency" in a model where suppliers compete in both price and privacy.

permission system is not only a central feature of the Android app ecosystem, it is also the enabling feature of this study. The fact that users must grant an app the right to use the requested permissions before installation introduces a real cost to developers, who request excessive access to user information. Users might avoid granting these excessive rights and it might generate negative publicity.

Figure A2 illustrates the way the permissions were displayed in the Android Market in 2012. In 2012 developers could choose among 136 predefined permissions.[5] This large number illustrates the quantity and diversity of information app developers can potentially collect about app users. It is worth noting that such explicit consumer consent to the set of permissions does not exist in Apple's operating system. There, the information remains implicit before installation. In its essence this procedure remained stable since 2012, and is still in place today despite the fast growth of the Android Market.

Since 2012, Google introduced several small modifications to how permissions are displayed to the user. Before 2014, the list of permissions provided permission names next to short explanations of the permissions. Since 2014 the system shows only the names of aggregated permission groups (but users can open a more detailed dialogue for each permission group). Still, users must approve of the permission list before proceeding with the installation process. Very recently, Google allows users to withdraw individual permissions from an app after the installation. However, this is only possible since a recent version of the Android operating system (Version 6.0, named "Marshmallow").

Generally, developers can monetize their apps via four important channels. According to AppBrain (2016) around 20 percent of the apps are paid apps, whereas the remaining apps are for free.[6] Alternative revenue channels are in-app advertisement, in-app purchases and data trade. The importance of these alternative revenue channels has been relatively stable since 2012 except for in-app purchases, which were introduced shortly before our period of observation.[7] In 2012, when we collected our data, the "freemium"

[5]Today, the count stands at 147 permissions (although the precise contents of some permissions changed; see http://developer.android.com/reference/android/Manifest.permission.html).

[6]Developers receive 70 percent of the app price, and 30 percent go to distribution partners and operating fees (see https://support.google.com/googleplay/android-developer/answer/112622?hl=en).

[7]Only in 2011, Google added in-app billing to the Android Market, allowing apps

model based on in-app purchases hardly existed. Since then the market has seen a distinctive increase of this model, where users may install the apps for free, but must pay a fee to unlock important functions. The two other channels, in-app advertisement and data trade were already common. Data trading is deemed the more privacy-sensitive way of creating revenue from an app, whereas in-app advertisement is deemed more acceptable by many users.

Yet, data trading for monetization purposes is very common in the mobile app industry. Christl and Spiekermann (2016) survey several studies which have shown that apps very commonly shared data with third parties.[8] They also provide a brief discussion of the data sharing business model, which was also confirmed in our conversations with industry experts. App developers have several ways of exploiting their app usage data to generate revenues. Most importantly, they can simply use the information to sell anonymized targeted advertisements. However, doing so is very costly and only pays off for very large apps with sufficient traffic. Smaller apps can achieve better targeting by sharing their data with a third-party broker, who can provide advertisers with access to users from a bigger pool of multiple apps (and developers to more advertisers). While this type of information brokerage potentially offers greater matching efficiency of the advertisements, sharing the data implies that the app users' information is passed on, and their safety depends only on the integrity of the developer's advertisement partner.

In addition, there are several other common ways that app developers can trade in their data with third parties. First, they can exchange their data for direct monetary benefit. A second more prevalent channel of data flows arises when developers trade their data for valuable third-party services. The most important example of such services are

to sell in-app products (see https://android-developers.googleblog.com/2011/03/in-app-billing-on-android-market-ready.html).

[8]The most common transmitted pieces of information about the user are identifying information (name, user's mail address, phone ID, gender, age or birthdate), location data, contacts, or usage data. Sometimes 'data input' (such as search terms etc.) are transmitted as well. In some contexts, like health, this information is more sensitive than in others (Reference 1, 2, 3, and 4). However, most of these studies analyse very small samples. For example, Seneviratne et al. (2015) analyzed the apps on the smartphones of 338 users and identified 124 different trackers in 509 unique apps in Australia, Brazil, Germany and the United States. Trackers were categorized as: 'advertising' (e.g. Google Ads, Millennial Media, InMobi, MoPub), 'analytics' (e.g. Flurry, Google Analytics, ComScore, Health and Amazon Insights, Localytics, Kontagent, Apsalar) and 'utilities' (e.g. Crashlytics, Bugsense). Moreover they found that 50% of these users were exposed to more than 25 trackers.

app analytics. App analytics help the developer to gain insight on who uses their app when and where and together with which other processes that take place on the phone. Combined with the developer's own knowledge of the user's in-app behavior, this can be a useful input for improving the app or, again, for advertisement purposes. Like with third-party advertisement, the secondary usage of the user data depends on the analytics site's own policy and integrity. There is no mechanism to enforce that developers choose a careful and trustworthy provider of analytics or other third-party services.

4 Data

We extracted all the publicly available information on as many apps as we could find on the English Android Market website in 2012 (later "Google Play Store"). We collected the data about these apps monthly from April to October 2012, once in 2014, and again in July 2016. The repeated data collection in 2012 allows us to use panel data methodology and compute improved demand measure, based on the variable's differences. The additional wave from 2014, and 2016 was gathered to use a low-density panel for quantifying long-term outcomes, such as survival over four years or the *privacygrade* in 2014.

Our main data set from 2012 covers nearly the full population of products available in that year (around 300,000 apps),[9] and after merging our data with the data from *privacygrade.org*, and eliminating inactive apps we still observe more than 180,000 apps.[10] In 2012, we could discern 136 distinct permissions in apps and record the permission requirements of each app. In order to evaluate privacy intrusiveness we combine this data with information from *privacygrade.org*.

Figure A1 shows the design of Google's Android Market in 2012 which corresponds to the information we were able to collect. To study our research questions we need three types of information: a demand measure, a price measure and a measure of apps'

[9]The data in this paper is based on the data we used in Kummer and Schulte (2016). A more detailed description can be found there.

[10]Apps are dropped if they are unavailable at some point in the panel, lack key variables, have no installations/ratings or are outliers with respect to demand measures.

ability to collect private information. In the following section we introduce each of these measures as well as the core control variables.

Main Outcomes - *Privacygrade* and Sharing with Third Parties: Our main outcome is the choice of developers to build privacy-sensitive features into their apps. To evaluate an app's privacy behavior we use two approaches. First, we combine our data with information from *privacygrade.org*, which is the thus far most comprehensive effort of computer scientists to evaluate potential privacy intrusiveness of apps. They analyzed detailed information about more than one million apps' privacy-related behaviors (Lin et al., 2014, 2012). They summarize these behaviors in the form of a grade, ranging from A+ (best privacy protection) to F (least privacy protection).[11] Grades were assigned using a privacy model that measures the gap between people's expectations of an app's behavior and the app's actual behavior. For example, most people do not expect games like "Cut the Rope" to use location data, but many of them actually do. This kind of surprise is represented as a penalty to an app's overall *privacygrade*. In contrast, most people do expect apps like Google Maps to use location data. This lack of surprise was represented as a small or no penalty.[12] *Privacygrades* were computed in 2014 and 2016, which allows us to get a measure of the app's future behavior. Moreover, we can run a cluster analysis to see which permissions are typically associated with bad *privacygrades*, and can apply this prediction ex-post to our 2012 wave.

Second, we use the data from 2016 to evaluate with how many third parties developers shared their data. This information is publicly available on specialized app web sites like *AppBrain.com*. We obtained the number of libraries from there and classify the apps in four groups: (1) apps that do not share any data, (2) apps that share data, (3) apps that share data with three or more third parties, and (4) apps that share data with seven or more third parties. Clearly, the more parties developers share their data with, the smaller is the protection of the app's users and their data.

[11] Their results are provided publicly, see: http://privacygrade.org/. The current version, which uses "D" rather than "F," can be found on http://cmuchimps.org/projects/privacy_grade/.

[12] The description was taken from http://privacygrade.org/faq.

Additional Outcomes - Success: In addition, we want to quantify an app's success, which we do by analyzing whether an app remained in the market for four more years and by analyzing demand. Survival is measured by whether we observe the app in 2016. Our baseline demand measure is the number of installations of an app. Our data set contains direct information on the total number of installations (i.e. sales) for each app. However, this measure is only available in a discrete form (17 levels, e.g. 1-5 installations, 6-10 installations, 11-50 installations, etc.). However, this granularity is too rough to quantify contemporaneous downloads, because the threshold values are only infrequently crossed. We thus improve our baseline demand measure, by exploiting information on the number of ratings of an app, which is available as a continuous measure. Using strategies that were developed in previous literature (see e.g. Chevalier and Mayzlin, 2006; Garg and Telang, 2013; Ghose and Han, 2014), we exploit the continuous number of ratings to predict a continuous number of installations per app, which we then use in our panel analysis.

Privacy Sensitiveness of Apps - Permissions: To measure an app's ability to collect private information, we take advantage of the fact that, as described before, Google provides precise insights into the permissions an app uses.[13] This feature allows us to understand in a detailed way which functions an app can perform, including functions which allow an app to collect private information about the app user. In 2012, developers could choose from 136 different permissions, which included e.g. 'read SMS or MMS', 'fine (GPS) location', 'read browser data', etc. All of these permissions have to be declared in the app description and have to be accepted by the app user before installing the app.[14] Among the 136 permissions, some can be considered innocuous with respect to the privacy of the user, while others grant an app access to sensitive information. To identify such privacy-sensitive permissions, we use four alternative permission classifications.

Our main classification (i) is derived from previous research by Sarma et al. (2012). Alternative classifications are (ii) a category-specific modification thereof, and (iii) a

[13] We build on the measures and techniques developed in Kummer and Schulte (2016) and augment them with the information from *privacygrade* to study developers' strategic behavior.

[14] We use the standardized short explanation to inform users about the permission's meaning by Google.

classification based on Google's assessment.

Our baseline definition of privacy-sensitive permissions follows Sarma et al. (2012) who analyze the benefits and risks of Android app permissions and classify them according to different risk types. 26 permissions are classified as critical, and among these 13 are considered as being a risk to privacy.[15] Based on this classification, we construct our main variable of interest ($D_{Privacy}$), which is a dummy equal to one if an app uses at least one of the 13 privacy-sensitive permissions and zero otherwise. To capture the intensity of an app's ability to collect private information, in addition, we make use of the number of privacy-sensitive permissions per app. While this strategy allows us a deep insight into the permissions an app requests, it does not provide us with an evaluation of the app's actual privacy intrusiveness.

In Table 1 a description of all the relevant variables as well as corresponding summary statistics are provided.[16]

[15]For the permission *read calender* we were not able to collect information, such that we only have information on twelve privacy-sensitive permissions.

[16]Summary statistics by developer's experience and age category are given in Table A1 and Table B1.

Table 1: Summary statistics for the main variables and privacy measures

	mean	sd	min	p50	max
Privacygrade (88,893 Obs.)					
App Grade	2.04	0.656	1	2	5
Failgrade	0.053	0.225	0	0	1
Data Sharing w. 3rd Parties (53,644 Obs.)					
Any Sharing with 3rd Parties	0.644	0.478	0	1	1
Sharing with 3+ parties	0.298	0.457	0	0	1
Sharing with 7+ parties	0.115	0.320	0	0	1
Other Outcome Variables					
Installations (in 1000)	67.00	1252.77	0	0	300000
Δ Installations (in 1000)	6.51	257.19	-6.71e-10	0.0001	45000
Δ Ratings	40.53	1159.18	-1147	0	322881
Average Rating	3.91	0.83	1	4	5
App Survived until 2016	0.468	0.498	0	0	1
Permissions					
$\#_{TotalPerm.}$	3.62	3.90	0	3	114
$\#_{CriticalPerm.}$	2.43	2.30	0	2	23
$\#_{PrivacyPerm.}$	0.86	1.33	0	0	12
$\#_{MaliciousPrivacyPerm.}$	0.34	0.69	0	0	7
$\#_{NonmaliciousPrivacyPerm.}$	0.51	0.79	0	0	4
$D_{Privacy}$	0.40	0.49	0	0	1
$D_{PrivCatSpec}$	0.18	0.39	0	0	1
$D_{MaliciousPrivacy}$	0.25	0.43	0	0	1
$D_{NonmaliciousPrivacy}$	0.35	0.48	0	0	1
$D_{Internet}$	0.68	0.47	0	1	1
D_{Ads}	0.45	0.50	0	0	1
D_{Other}	0.36	0.48	0	0	1
App Characteristics					
Price	0.80	3.29	0	0	157
App Version	16.88	148.32	0	2	9561
Size (in KB)	3048.15	7326.62	4	960	809000
Length Description	805.08	809.78	1	504	12285
Number Screenshots	3.40	1.83	0	3	8
Dummy: Video	0.10	0.30	0	0	1
Dummy: Top-Developer	0.01	0.08	0	0	1
Apps by Developer	157.36	412.24	1	10	2963
Average Installations of Developer	79.08	1050.53	0	5	300000
Observations	180040				

NOTES: List of core variables: For **developers** we observe the name of the developer, the top developer status (yes/no), number of its apps, the set of its available apps. The main variables at the **app-level** are: total number of installations, (monthly) downloads of an app, information on updates (date, textual information on what is new, version number), names and IDs of similar apps, the permissions requested upon installation, number and values of quantitative ratings (from 1 to 5 stars), is the app an editor's choice (yes/no), text of reviews (date, rating from 1 to 5 stars, content, availability of a developer-response), price (in Euro),in-app purchases (yes/no) and price-range of items, in-app advertisements (yes/no), app category (e.g. Personalization, Traveling, Weather, etc.), code size (in KB), apps' description (length, content) and its illustration in the Play Store (video and screen-shot availability), content rating (USKs), availability of interactive elements (e.g. 'users interact', 'digital purchases' etc.), Android version required for installation.

5 Methodology and Empirical Approach

We aim at answering two overarching questions: (i) What strategies do developers use with respect to private data? (ii) Which app developers are more prone to privacy-intrusive choices?

Hence, we pursue our analysis in three steps. First, we use reduced-form analysis of developer behavior to understand the role of data in developers' strategies. Second, we analyze their data collection strategies over time. In the third step, we focus on how the *same* developers vary their behavior in different app environments. This is important, because it is insufficient to analyze the cross-sectional correlation between app's environment and its behavior regarding user data. App developers are very heterogeneous and might use fundamentally different programming and marketing strategies. In the third step of our analysis we limit the role of developer heterogeneity. We use a panel approach with a developer fixed effect, and compare only apps of developers who have acquired some experience.

Model Free Analysis: Our analysis is not guided by a model, and this is a conscious choice. We believe that knowledge about app developers (let alone privacy-abusive app developers) is currently so limited that a model guided analysis is hard to achieve. Developers might attempt hit and run strategies, or try to build reputation and increase their permission requests later. They might target valuable consumers or aim at tricking "easy victims."

Hence, rather than deriving the analysis from theory, we hope to generate valuable stylized facts that can inform future theoretical or structural analysis.

5.1 Single- vs. Multi-App Developers

The main goal of our analysis is to gain insights into the drivers of privacy-intrusive app design. Moreover, we want to shed light on both the first order and the second order effect of data access for the success of an app. Most importantly, we can also analyze what drives excessive data use. Hence, this first part will shed light on what types of developers

use 'excessive' data strategies, and which patterns in an app's development render such strategies more likely? Among other things, we will analyze whether developers of single apps are different, in the sense that they ask for more or less privacy-intrusive permissions.

$$Privacy_i = \beta D_i^{SingleAppDeveloper} + \theta X_i + \varepsilon_i. \tag{1}$$

In this regression $Privacy_i$ represents the app's potential threat to a user's privacy. We measure that by the app's use of permissions, and its *privacygrade*. The indicator $D_i^{SingleAppDeveloper}$ is the variable of interest which is equal to one, if the developer offers only a single app. We further include control variables (X_i) comprising app and developer characteristics as well as the competitive environment.

5.2 App Developers over Time

Beyond the plain cross-sectional analysis, we can exploit a special feature in our data. We can observe developers with multiple apps in this market, and we want to exploit this fact in the core part of the analysis. Frequently, we see that apps from the same developer vary in how much access to private information they request. Using a fixed effects design, we can leverage this variation to study how varying access to personal data influences the success of apps by the *same* developer. Comparing apps by the same developer serves two purposes: First, it massively strengthens our research design to effectively analyze learning of developers. For example we can understand whether the first app is different from subsequent apps. Secondly, we can answer the questions with regards to the dynamics within an app.

Being able to track developers over time allows us to analyze how they experiment with access to data and how their strategies change with more experience. For this step of the analysis we exploit our ability to run our analyses within and between apps of the same developer (as they introduce new apps). Specifically, focusing on developers with multiple apps we start by asking whether the first apps are different, and then move on to characterize dynamic strategies of developers. Similarly, we can characterize the relative hostility, or dynamism of the app's competitive environment, based on app category,

initial app demand, or the 'initial' data requirements. Using permissions, the *privacgrade*, and third-party data sharing as outcomes of interest to quantify data behavior, we can analyze dynamic data strategies over time. This analysis can shed light on the dynamic data strategies of the same developers, and how they vary with the environment, or the initial app success. Continued success and innovation on the app are the other crucial economic outcomes in this big picture.[17]

5.3 Fixed Effects Analysis at the Developer-Level

We now turn to a fixed effects analysis, which allows us to understand how the data strategies of the same developer vary with the environment in which they place their apps. We observe a series of important environmental factors that could influence a developer's data strategy. Among these factors are the app's competitive environment, the app category, the app's past success, or whether the app is offered for free or for pay. To shed light on the relationship between an app's environment and its requested data access, it is insufficient to analyze the correlation between these two variables. Apps may provide completely different functionality, and their developers might use fundamentally different programming and marketing strategies. It is thus important to minimize the role of app heterogeneity. In these specifications we can limit the role of app heterogeneity by using a panel approach with a developer fixed effect, and by excluding every developer's first two apps.[18] We thus compare apps by the same experienced developer (j) and use permissions or the *privacgrade* to measure their app (i)'s data behavior. This results in the following regression:

$$Privacy_{ij} = \alpha_j + \theta X_{ij} + \varepsilon_{ij}. \tag{2}$$

In this regression $Privacy_{ij}$ measures the privacy sensitiveness of developer j's app i. The developer's fixed effect is measured by α_j, and X_{ij} are other control variables, such

[17] In section C of the Appendix an alternative approach is employed to study apps over time by analyzing the early app development and the accompanied data collection of selected apps.

[18] We chose to ignore the first two apps, based on the informal notion that it takes three attempts to do it right. However, our key results do not depend on excluding exactly two, as is shown in a robustness check.

as the app's competitive environment, its price (which is potentially 0), or its category. Thus analyzing a developer's data strategy across different apps, we can highlight which factors drive the same developer to use more problematic data strategies. Subsequently, we provide supplementary results on how app success varies for a developer's different data strategies. While access to more user information could influence app success (measured in demand and survival) in both ways, we would expect the marginal effect in success to decrease when requesting additional access to user data.

First, access to data enables a healthy ecosystem, in which developers have a better understanding of their user's needs, and can monetize their services. Both are critical ingredients for further improving the app. Thus, among other things, we would suspect that better access to more user information (directly and indirectly) facilitates innovative activity, which could be a major channel to explain any positive relationship. Second, however, excessive requests for access to data cannot easily translate to additional benefit, especially if the requested data is neither typical in an app's category, nor can it be associated with improved functionality. Like in the previous specification, it is important to minimize the role of app heterogeneity. We aim to achieve this by excluding developers' first two apps, and by using a panel approach with a developer fixed effect:

$$Success_{ij} = \alpha_j + \beta D^{Privacy_{ij}} + \theta X_{1,ij} + \varepsilon_{ij}. \tag{3}$$

We thus analyze the success of the same experienced developer j's app i as a function of its data requirements. $Success_{ij}$ is measured (1) by contemporaneous demand between April and September 2012,[19] and (2) by whether the app survives until 2016. $Privacy_{ij}$ is measured by the app's access to potentially privacy-sensitive data. We contrast the role of data access to other variables of interest, such as the app's competitive environment, its category or its pricing strategy.

[19]We measure demand by using a proxy variable that is based on the new ratings that the app received between April and September 2012. Since the Google Play Store provides only a coarse measure of installation ranges, ratings are a reasonable measure to approximate installations that occurred in a short period of time (see Kummer and Schulte (2016)).

6 Description of the Variables

6.1 Key Variables

As previously discussed, the main variables were obtained from our full cross section in 2012, which contains up to 300,000 apps. These data were merged with data from *privacygrade.org*, to add the *privacygrade*, and a derived dummy *failed* which takes the value one, if an app received grades C or D. After merging our data with the 2014 data from *privacygrade.org* we still observe more than 180,000 apps, which are our main sample.

6.2 Stylized Facts

We first compare the apps of single-app developers to the apps of multi-app developers, and then use a fixed effects analysis to analyze the behavior of multi-app developers. Single-app developers might be more prone to reverting to data selling if their app is unsuccessful, whereas multi-app developer might have a reputation to lose. Tables 2 and 3 show the descriptives for single-app developers' apps and multi-app developers seperately. Moreover, in Figure 1 we visualize this comparison. It is easy to see from this raw comparison, that the apps of multi-app developers appear to be more professional and more demanded (more installations, ratings, and higher price). Yet, the apps of single-app developers use slightly more permissions, and still have similar ratings.

Figures A3 and A4 complete the descriptive picture. They highlight that single-app developers are more active in Entertainment, Health, and Business, but relatively less in Education and Games. Single-, and multi-app developers require very similar maturity levels. The vast majority of apps are for everyone or for low maturity (13+).

Table 2: Single-App Developers

	mean	sd	min	p10	p50	p90	max
Number of Installs	55.39548	812.772	.003	.075	3	30	75000
Number of Ratings	347.1522	6174.736	1	1	8	134	439719
Rating	3.995473	.8979601	1	2.8	4.1	5	5
Price	.2794387	1.778883	0	0	0	.75	105.43
Number of Permissions	3.884763	3.915905	0	0	3	9	114
Number of Malicious Perm.	2.613125	2.243873	0	0	2	6	21
Observations	35275						

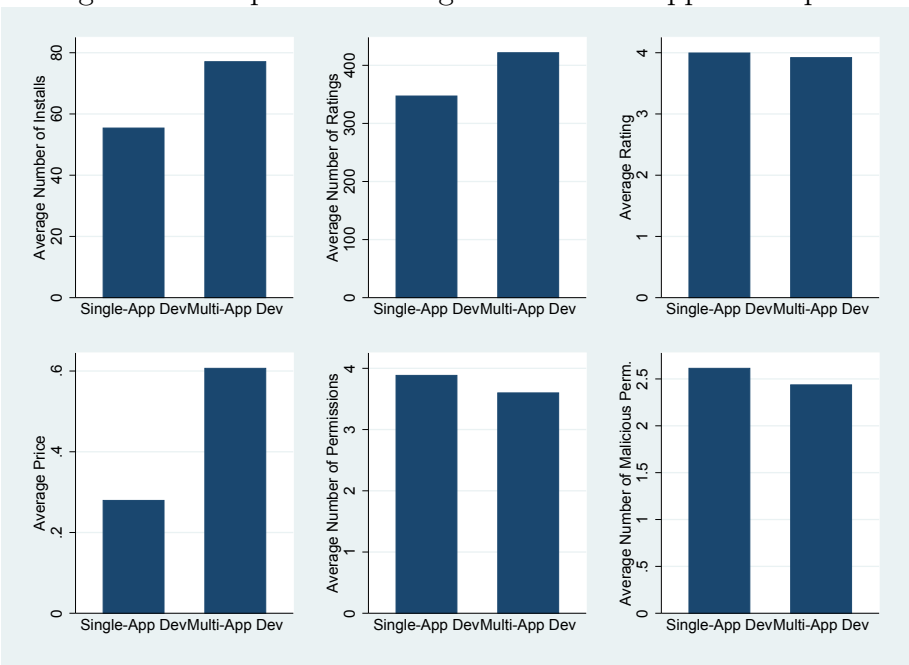
NOTES: The table shows the averages and distribution for the most important variables of single-app developers. It shows the mean, standard deviation, minimum value, median, maximum value, and the 10th and 90th percentile of the distribution.

Table 3: Multi-App Developers

	mean	sd	min	p10	p50	p90	max
Number of Installs	77.07398	1432.493	.003	.03	3	30	300000
Number of Ratings	421.6965	7780.803	1	1	7	174	1101035
Rating	3.919851	.9778243	1	2.6	4.1	5	5
Price	.6066419	2.521879	0	0	0	1.5	136.49
Number of Permissions	3.598694	3.778822	0	0	3	9	114
Number of Malicious Perm.	2.436763	2.22157	0	0	2	5	23
Observations	144765						

NOTES: The table shows the averages and distribution for the most important variables of multi-app developers. It shows the mean, standard deviation, minimum value, median, maximum value, and the 10th and 90th percentile of the distribution.

Figure 1: Comparison of Single- and Multi-App Developers



NOTES: The figure compares the apps of single-app developers and multi-app developers. Each plot shows a variable of interest in the 2012 data (from top left to bottom right): (i) average number of installations, (ii) average number of ratings, (iii) average rating, (iv) average price, (v) average number of permissions and (vi) average number of malicious permissions. On each panel the left bar shows the value for single-app developers and the right bar shows the average value of multi-app developers' apps.

7 Results

7.1 Regression Results

Single- vs. Multi-App Developers: We use the new variable that measures the privacy intrusiveness in 2014 via the *privacygrade* to shed light on which types of apps are more likely to be problematic. We first ask whether apps of single-app developers or multi-app developers are more likely to become abusive. In Table 4, we show the results of this descriptive cross section. Surprisingly, multi-app developers are more than 2% more likely to obtain a $failgrade$ in 2014. This relationship remains stable as we introduce control variables that account for (a) the app's characteristics (b) developer characteristics and the competitive environment, and (c) the app's privacy policy. None of these controls affect the finding that single-app developers are less likely to obtain a $failgrade$, and the relationship is equally true when using the *privacygrade* on a 5 grade scale (where 1 corresponds to A+, and 5 to F) instead of the dummy.

When looking at the control variables, we find interesting results. First, successful apps are more at risk of having high privacy requirements and receiving a $failgrade$. Second, apps with a privacy policy were more likely to fail in 2014 by a substantial 5%, and obtained a lower grade (0.17 grade points on average).

Finally, in column 6, we look at the probability, that an app will share their data with three or more outside parties. For this dependent variable we see the reverse picture, since single-app develpers are more likely to share their data with outside parties.

Developers "Learn" to use Privacy-Sensitive Permissions over Time: The next step in our analysis focuses on developers' behavior over time. To answer this question we identified an app's launch date and analyzed whether developers use more or less intrusive permissions on their first apps.

The results of this analysis are shown in Table 5. The table controls for developer heterogeneity by using developer fixed effects (cf. above). It shows two major results: First, developers ask for less intrusive permissions on their first three apps, independent

of whether we look at sensitive permissions, Google's "potentially malicious" permissions, or the *privacygrade*.[20] Even for the likelihood of finding a $failgrade$ we observe small and negative effects, which are significant for the third, but not the first two apps. Sharing with outside third parties is less frequently observed on the first two apps, but not the third. Overall, we see a pattern of increasing intrusiveness, which indicates that "rookie apps" of later multi-app developers ask for less access to data, while their second and third apps become less moderate, in particular on the dimensions of using sensitive apps, and sharing the data.

The second finding comes from the analysis of the maturity ratings. The analysis shows that rated apps are generally more likely to be intrusive. Most importantly, for all measures including a $failgrade$ from *privacygrade.org*, we see that apps in the low maturity (13+) group are most intrusive and potentially abusive, followed by the medium maturity (16+) group. This suggests that apps in the 13+ category bear the greatest risk of intrusive access to personal information. Since this specification includes a developer fixed effect, this means that the same developer will use more intrusive permissions and libraries in an app for teenagers.

In a deeper analysis (shown in Table B2) we analyze the correlation of developer characteristics and whether they request intrusive permissions. Specifically, we include developers' initial success on their first three apps. While most developer characteristics have little value for predicting intrusive behaviors, we find a very small positive association of previous app demand (installations on the first, ratings on the second app) with future apps' intrusiveness. However, this correlation does not control for the first app's intrusiveness, and might thus be confounded by developer heterogeneity.

[20] In this dataset A+ takes the value of 1 and F takes the value 5, and a negative coefficient means better protection.

Table 4: Privacygrade and Sharing with 3rd Parties: Single- vs. Multi-App Developers

	failing	failing	failing	failing	priv. grade	3rd Parties
	(1)	(2)	(3)	(4)	(5)	(6)
Single App Developer	-0.027***	-0.024***	-0.027***	-0.028***	-0.062***	0.036***
	(0.002)	(0.002)	(0.002)	(0.002)	(0.006)	(0.007)
Dummy: Top-Developer		0.048***	0.048***	0.036**	0.114**	0.070*
		(0.015)	(0.017)	(0.017)	(0.044)	(0.036)
Apps by Developer		0.000***	0.000***	0.000***	0.000***	0.001***
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Price		-0.003***	-0.003***	-0.003**	-0.012**	-0.003
		(0.001)	(0.001)	(0.001)	(0.006)	(0.003)
Number Screenshots		0.005***	0.005***	0.004***	0.028***	0.051***
		(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
Dummy: Video		0.012***	0.011***	0.008**	0.012	0.074***
		(0.003)	(0.003)	(0.003)	(0.009)	(0.009)
Number Ratings		0.000***	0.000***	0.000***	0.000***	0.000
		(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Average Rating		-0.002***	-0.002**	-0.002**	-0.042***	-0.004
		(0.001)	(0.001)	(0.001)	(0.003)	(0.004)
Installations (in M)			0.168	-0.003	1.733	17.866***
			(1.082)	(1.029)	(3.712)	(3.380)
Competitor Inst.(Mln)			0.149**	0.124*	2.323***	1.520***
			(0.065)	(0.067)	(0.184)	(0.247)
Avg. Install Developer			-0.000	-0.000**	-0.000**	0.000
			(0.000)	(0.000)	(0.000)	(0.000)
#ExtremPrivPerm				0.004	0.037	-0.032
				(0.015)	(0.040)	(0.032)
#UnusualPrivPerm				0.029***	0.162***	0.069***
				(0.010)	(0.023)	(0.022)
Privacy Policy				0.042***	0.178***	0.247***
				(0.005)	(0.014)	(0.012)
Constant	0.059***	0.047***	0.046***	0.047***	2.092***	0.123***
	(0.001)	(0.004)	(0.004)	(0.004)	(0.012)	(0.015)
Observations	88893	88893	67685	64731	64731	28451
Adjusted R^2	0.002	0.010	0.010	0.012	0.024	0.090

NOTES: The table compares the permission usage of single- and multi-app developers. The regressions are cross-sectional OLS regressions. The dependent variable in columns 1-4 is a dummy that indicates that the app will receive a failing *privacygrade* (C or F) in 2014. In column 5 we use the grade itself (1=A+, 5=F) as dependent variable. Col. 6 analyzes the data sharing behavior in 2016. The dummy takes the value 1 if the app shares with more than three third parties (0 otherwise). Col. 1-4 start from the raw correlation and gradually add control variables. Col. 5 shows the result with all controls for the *privacygrade* directly. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

Table 5: Multi-App Developers Learning - Permission Usage and Experience

	sensitive	pot. malic.	# pot. malic.	priv. grade	failgrade	3rd Parties
	(1)	(2)	(3)	(4)	(5)	(6)
Developer's 1st App	-0.012***	-0.022***	-0.103***	-0.008	-0.004	-0.017**
	(0.004)	(0.004)	(0.018)	(0.008)	(0.003)	(0.008)
Developer's 2nd App	-0.009**	-0.015***	-0.058***	-0.013*	-0.004	-0.025***
	(0.004)	(0.004)	(0.017)	(0.008)	(0.003)	(0.008)
Developer's 3rd App	-0.006	-0.010**	-0.071***	-0.013*	-0.007**	-0.011
	(0.004)	(0.004)	(0.016)	(0.008)	(0.003)	(0.008)
Average Rating	-0.005***	-0.004***	-0.005	-0.004	0.002	0.006*
	(0.001)	(0.001)	(0.005)	(0.003)	(0.001)	(0.004)
# Ratings in 1000	0.001***	0.000	0.008***	0.003**	0.001**	0.002***
	(0.000)	(0.000)	(0.003)	(0.001)	(0.000)	(0.000)
Dummy: Video	0.033***	0.043***	0.232***	0.073***	0.024***	0.064***
	(0.008)	(0.007)	(0.031)	(0.016)	(0.006)	(0.013)
Dummy: Website	0.023***	0.040***	0.137***	0.035*	0.008	0.038**
	(0.009)	(0.012)	(0.041)	(0.021)	(0.006)	(0.019)
Privacy Policy	0.070***	0.046**	0.535***	0.049	0.006	0.132***
	(0.021)	(0.018)	(0.107)	(0.032)	(0.012)	(0.029)
Log. Price	0.039***	0.075***	0.324***	0.048	-0.001	-0.009
	(0.006)	(0.007)	(0.036)	(0.047)	(0.010)	(0.011)
DPrice	-0.523***	-1.043***	-4.417***	-0.639	0.015	-0.063
	(0.076)	(0.089)	(0.444)	(0.538)	(0.116)	(0.126)
Matur. Rating n.a.	-0.009	-0.071***	-0.183***	0.003	0.004	-0.100***
	(0.013)	(0.016)	(0.053)	(0.019)	(0.006)	(0.015)
High Maturity (18+)	0.172***	0.059***	0.716***	0.113***	0.036***	0.009
	(0.017)	(0.012)	(0.075)	(0.022)	(0.009)	(0.027)
Med. Maturity (16+)	0.206***	0.088***	0.923***	0.151***	0.031***	0.074***
	(0.013)	(0.008)	(0.058)	(0.019)	(0.007)	(0.020)
Low Maturity (13+)	0.424***	0.162***	1.788***	0.254***	0.057***	0.080***
	(0.011)	(0.009)	(0.064)	(0.014)	(0.006)	(0.013)
Local Market Share	0.014	-0.005	0.135**	0.035*	-0.000	0.099***
	(0.010)	(0.012)	(0.056)	(0.019)	(0.007)	(0.018)
Competitor Inst.(Mln)	0.965***	1.056***	4.756***	1.233***	0.140	0.981***
	(0.146)	(0.125)	(0.609)	(0.243)	(0.101)	(0.318)
Constant	0.780***	1.606***	5.721***	2.510***	0.016	0.137
	(0.074)	(0.085)	(0.418)	(0.541)	(0.120)	(0.127)
Observations	103937	103937	103937	51457	51457	32050
Developers	26857	26857	26857	19755	19755	13147
Adjusted R^2	0.166	0.095	0.226	0.039	0.015	0.068

NOTES: The table analyzes whether app developers' permission usage changed over time, and whether this affects the resulting *privacygrade* in 2014. The regressions are panel OLS regressions with a developer fixed effect. The dependent variables in the five columns are: (1) usage of sensitive permissions (2) usage of potentially malicious permissions (according to Google) (3) number of potentially malicious permissions (according to Google) (4) the *privacygrade* that was obtained in 2014 (1=A+, 5=F), and (5) a dummy that indicates that the app will receive a failgrade (C or F). Column 6 analyzes an indicator which takes the value 1 if the app was sharing its data with 3 or more third parties. The reference of content rating are apps rated as "Everybody." Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

7.2 Fixed Effects Analysis of Experienced Developers

Our main strategy to control for developers' varying abilities, strategies and intentions relies on using a developer fixed effects analysis. We used this strategy in Table 5, and will use it in all subsequent result tables. Doing so, we can contrast the intrusiveness of apps by the same developer in different market environments. Moreover, we exclude developers' first and second apps to ensure that the apps belong to developers who have gathered initial experience on their first two apps, which allows us to investigate the robustness and external validity of the patterns that emerged from the analysis of control variables.

Privacygrade: In Table 6 we analyze which observable factors in 2012 predict a bad *privacygrade* in 2014 in four distinct columns.[21] We analyze OLS regressions with developer fixed effects excluding each developer's first two apps. The main result from Table 6 highlights that age rating and permission use in 2012 (columns 3, 4, 7 and 8) are the most powerful predictors of potentially intrusive privacy behavior. Age rating and permissions achieve a much larger increase in *adjusted* R^2 than an app's pricing strategy, its category, or its competitive environment (columns 1, 2, 5 and 6).

Analyzing the four factors in detail, we see that paid apps had a considerably better *privacygrade* in 2014 (columns 1 and 5). Moreover, we see that a developer was more likely to use potentially problematic data practices on apps that faced very large competitive pressures, but that the app's category is not predicitive of such practices (columns 2 and 6). Note, however, that the significance of these coefficients, and hence the predictive power of pricing, competitor strength and app category is low, which suggests that they help little to predict abusive behavior. We would also like to highlight the fairly strong effect of having a privacy policy, which continues to be associated with a bad *privacygrade*.

An app's content rating (in columns 3 and 7) has a much larger predictive power for the *privacygrade* in 2014. As might be expected, the same developer will obtain worse

[21] Table B4 repeats these regressions excluding single-app developers, but uses developers' first two apps. This increases the number of observations, but accepts potential learning as a confounding effect.

Table 6: Multi-App Developers Without Their First Two Apps - Outcome: *privacygrade*

	privacygrade				failgrade			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Average Rating	-0.005	-0.004	-0.003	-0.003	0.000	0.001	0.001	0.000
	(0.004)	(0.004)	(0.004)	(0.003)	(0.002)	(0.002)	(0.002)	(0.002)
# Ratings in 1000	0.002*	0.003*	0.002*	0.001*	0.000*	0.001	0.000	0.000
	(0.001)	(0.002)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.000)
Dummy: Video	0.039**	0.043**	0.037**	0.019	0.016**	0.022**	0.015**	0.013*
	(0.019)	(0.022)	(0.019)	(0.017)	(0.007)	(0.009)	(0.007)	(0.007)
Dummy: Website	0.027	0.031	0.027	0.010	0.007	0.012	0.007	0.004
	(0.025)	(0.030)	(0.025)	(0.024)	(0.008)	(0.010)	(0.008)	(0.008)
Log. Size (in KB)	0.039***	0.043***	0.035***	0.013***	0.007***	0.008***	0.006***	0.003*
	(0.005)	(0.005)	(0.005)	(0.004)	(0.001)	(0.002)	(0.001)	(0.001)
Privacy Policy	0.032	0.030	0.013	-0.033	0.002	0.000	-0.002	-0.011
	(0.033)	(0.041)	(0.032)	(0.033)	(0.012)	(0.015)	(0.012)	(0.012)
DPrice	-1.436*				-0.025			
	(0.764)				(0.174)			
Log. Price	0.116*				0.003			
	(0.065)				(0.015)			
Local Market Share		0.024				-0.004		
		(0.023)				(0.009)		
Competitor Inst.(Mln)		1.433***				0.289*		
		(0.379)				(0.169)		
Categ: Education		-0.031				-0.003		
		(0.031)				(0.011)		
Categ: Entertain.		-0.026				-0.004		
		(0.027)				(0.012)		
Categ: Games		-0.034				0.006		
		(0.031)				(0.010)		
Categ: Tools/Perso.		-0.052*				0.005		
		(0.029)				(0.011)		
Categ: Lifestyle		-0.022				-0.001		
		(0.028)				(0.009)		
Categ: Health		-0.072*				-0.013		
		(0.043)				(0.017)		
Matur. Rating n.a.			0.045*				0.005	
			(0.025)				(0.008)	
High Maturity (18+)			0.093***				0.026***	
			(0.022)				(0.008)	
Med. Maturity (16+)			0.155***				0.033***	
			(0.021)				(0.008)	
Low Maturity (13+)			0.248***				0.061***	
			(0.018)				(0.007)	
DPrivacy				0.001				-0.039***
				(0.023)				(0.010)
DGoogle				0.072**				0.049***
				(0.032)				(0.013)
#CriticalPerm.				0.116***				0.019***
				(0.008)				(0.003)
DPrivCatSpec				0.061***				0.048***
				(0.021)				(0.012)
Constant	3.171***	1.820***	1.769***	1.668***	0.057	0.001	0.006	-0.002
	(0.757)	(0.052)	(0.041)	(0.039)	(0.178)	(0.020)	(0.014)	(0.014)
Observations	37074	28397	37074	37074	37074	28397	37074	37074
Developers	9677	8436	9677	9677	9677	8436	9677	9677
Adjusted R^2	0.010	0.015	0.038	0.132	0.003	0.005	0.015	0.042

NOTES: The table analyzes the driving factors of developers' permission usage and the resulting *privacygrade* that the app was given in 2014. The regressions are panel fixed OLS regressions with a developer fixed effect. The dependent variable in columns 1-4 is the 2014 *privacygrade* (1=A+, 5=F) and, in columns 5-8, we use a dummy that indicates receiving a failgrade (C or F). Col. 1&5 analyze paid and free apps seperately. Col. 2&6 analyze environmental factors, such as the competitors' strength and the app-categories seperately (baseline: "Business"). Col. 3&7 shows how intrusiveness varies for different maturity ratings (baseline: "Everybody"), and col. 4&8 add variables that measure the permission use in 2012. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

privacygrades on apps for mature users than on apps for "Everybody." However, it turns out that developers use the most data intensive practices on apps for the 16+ and the 13+ groups. In particular apps for the 13+ maturity group carry a 6% higher risk of obtaining a $failgrade$ in 2014, while the risk on an adult app is only 2.6% higher.

Finally, in columns 4 and 8, we show that permission use is the most powerful predictor of obtaining problematic data practices two years down the road, as it explains more than 12% of the developers' within variation in their *privacygrade*. Permissions that are atypical for their category, and problematic permission that are flagged by Google are the strongest predictors. A large number of critical permissions is another sign of trouble, but initially the positive coefficient is offset by the negative coefficient for the dummy $D_{Privacy}$. In other words, a small number of critical permissions (less than three) is not associated with an increased risk of a $failgrade$ (column 8).

App Success and Survival: In Table A3 we analyze app success in terms of future survival (until 2016) and 2012 demand. We measure demand by using a proxy variable that is based on the new ratings that the app received between April and September 2012. Since the Google Play Store provides only a rough measure of installation categories, ratings are a reasonable alternative to approximate installations that occurred in a short period of time (see Kummer and Schulte (2016)). Future survival is measured by the likelihood of staying in the market for the subsequent four years, that is until 2016. We use our ratings-based measure of demand in columns 1 to 4 of Table A3, and app survival until 2016 in columns 5 to 8.

Columns 1 and 5 analyze paid and free apps seperately. Despite the developer fixed effect, paid apps have drastically lower demand and are significantly less likely to survive the following four years. This is an important finding, because it highlights, that app adoption by the users critically depends on the availability of apps that did not require any payment upfront (see Kummer and Schulte (2016)). Columns 2 and 6 analyze the role of competitors' strength and app categories, and columns 3 and 7 show how intrusiveness varies for different maturity ratings (baseline: "Everybody"). Rated apps have generally more installations, which, in the case of low and medium maturity, gives additional weight

to the fact that they were found to be more intrusive. Interestingly, only high maturity apps (18+) are more likely to stay in the market. Columns 4 and 8 analyze the role of an app's permission requirements in 2012 for its success and survival. First, we note that the total number of permissions (sensitive and unproblematic) has no discernible relationship with survival and a positive but declining association with app installations. Second, we note that sensitive permissions, even if they are atypical, have no significant relation with app demand, but have a strong negative effect if they are flagged by Google. We want to caution, that these results do not account for the functionality of an app. Especially the measure of installations will be highly confounded by the relationship of permissions and functionality, as was shown in Kummer and Schulte (2016). Hence, it is important to bear in mind that the relationships that we document highlight correlations when conditioning on the developer, but we do not claim that these relationships are causal. We consider these results important though, because they highlight that most users only refrain from installing apps that carry sensitive permissions if Google flags them.

Robustness and Supplementary Results on Permissions and Data Sharing: In the Appendix we supply a series of robustness checks and supplementary results. Table A2 shows analogous but adjusted regressions for analyzing the drivers of permission usage. This table confirms the patterns in Table 6 and highlights, that more intrusive permissions are the most likely channel for the greater risk of problematic behavior in the low maturity (13+) and medium maturity (16+) categories. Table A4 analyzes the same specification, but explores the finding on data sharing in 2016 in greater depth. The dependent variable in columns 1 to 4 is a dummy that indicates whether the app will share data with any outside parties in 2016. In columns 5 to 8, an indicator whether the app will share data with more than seven outside parties. Like before, paid apps do not only request less data, they are also less likely to hand it out to third parties, in particular sharing with more than seven outside parties, is most likely for apps in the low maturity (13+) category. Unlike before, strong apps (with greater market share) are also more likely to share their data with (many) outside parties. Noting the contrast to the analogous coefficients in Table 6, apps with strong market positions do access and even

share user data, but successfully avoid openly abusive data practices.

Tables B3 and B4 show the same regressions but use a developers' first two apps (while still excluding single-app developers). This allows us to run a fixed effects regression for all multi-app developers. While this leads to much larger number of observations, the regressions are confounded by potential learning effects. Nevertheless, these regressions compare apps of the same developer and thus allow to study how the use of permissions depends on an app's environment.

In Table B3, we show the results for the developers' permission usage when restricting our attention to multi-app developers. The dependent variable in columns 1 to 4 is a dummy indicating the usage of privacy-sensitive permissions and, in columns 5 to 8, a dummy that indicates potentially malicious permissions. Columns 1 and 5 analyze paid and free apps seperately. The negative coefficient for paid apps implies that sensitive permissions occur far more likely in free apps. Columns 2 and 6 analyze categories seperately, and highlight a tendency for fewer sensitive permissions in educational apps and games, when comparing them to business apps. However, the other patterns for categories are not consistent. Columns 3 and 7 shows how intrusiveness varies for different maturity ratings. Since the baseline group are apps for "Everybody", the positive coefficients reveal even stronger patterns than in the main specification in Table 6. Columns 3 and 6 add variables that measure (i) the strength of the competitors, and (ii) the app's market share, measured by its strength relative to its closest substitutes. The results show a significant but very small positive effect of competitive pressure on permission usage. They also show that the market share is strongly correlated with using intrusive permissions. Stronger apps seem to use their market power for acquiring more data.

In general terms we find consistent patterns for both permission usage and the *privacygrade* in 2014, both for the control variables and the effect of competitive pressure. However, apart from earlier permission use, hardly any of the variables is important for predicting $failgrades$. The small size of the significant coefficients in the fixed effects regression with $failgrade$ as dependent variable could be due to smaller sample sizes. However, it is more plausible that the developer fixed effect is the most important factor

when accounting for privacy-endangering behaviors. Similarly, finding no effect for the market share suggests that strong apps use their market power for acquiring more data (as follows from the results on data collection), but without taking it too far.

Future Work and Limitations: Despite this being the first analysis of developer's behavior regarding privacy, and the fact that we consider our focus on variation in apps by the same experienced developers a considerable contribution to the literature, several limitations remain. The most important concern is the lack of any well-defined exogeneous variation in the system. Instead, our results are largely based on an augmented cross section of data on mobile applications from 2012. Analysing the behavior of multi-app developers between 2012 and 2016 could shed additional light on the relationships of interest and might allow using experimental variation. Moreover, we do not observe in-app purchases. While this is arguably no problem for 2012, and hence the present cross-sectional analysis in app purchases is an important consideration for dynamic analysis of the data. In future research we will attempt to use the information from *privacygrade* to solve this issue. Next, it is challenging to cleanly disentangle monetization from functionality. Future research could parse updated descriptions and reviews, or alternatively use free/paid pairs to spot typically redundant permissions. Finally, there is additional potential in seeking additional sources of exogenous variation, such as the roll out of Android 6 that enabled revoking permissions after installing the app. Finally, we shed first light on the relationship between data collection, developers' privacy strategies and how they influence app success and other outcomes. While these findings might reveal the role of data availablilty and privacy for the supply side, our insights can only be considered as foundational input to developing a structural approach to estimate the value of accessing privacy-sensitive data for the developers. Such a structural approach is the next logical step towards understanding the role of data in the market of mobile apps. Basing such a structural approach on carefully researched stylized facts, will ensure modelling improvements which help to better evaluate the harm (or its absence) of more rigorous privacy regulation in this market. Such future research will be needed to clarify which levels of data access are necessary for the market to thrive, and which levels are not.

8 Conclusions

The last decade alone has seen the creation of more than three million mobile applications, which generate tremendous value for users. Given the recent rise of smartphones and mobile apps as well as their transformative power on human interaction and the economy as a whole, the issue of privacy concerns in this market is arguably a very important one.

In this paper, we study mobile applications to understand the data collection strategies of mobile app developers. We tracked more than 300,000 apps of the Google Play Store over four years, and combine these data with additional information from *privacygrade.org* on the apps' behavior. When analyzing the relationship between an app's environment and its behavior regarding user data it is insufficient to analyze the cross-sectional correlation, because app developers are very heterogeneous due to for example different programming and marketing strategies. In our main analysis, we limit the role of developer heterogeneity, by using a panel approach with a developer fixed effect, and by comparing only apps of developers who have acquired some experience.

We uncover three stylized facts about developers' privacy strategies. First, developers "learn" to use increasingly intrusive data strategies as they become more experienced. App developers are less likely to use intrusive permissions, and generally obtain better *privacygrades* on their first apps. The same is true for single-app developers, as they are less likely to run intrusive apps, and have better *privacygrades*. Second, intrusive data collection and sharing with third parties is most likely in apps that target the 13+, and 16+ age category. While this positive relationship may be due to monetization pressures, it raises concerns for the protection of young app consumers. Third, even within developers, critical and atypical permissions remain the most powerful predictor for problematic usage of private user data two years later. Critical and atypical permissions contribute much more to predicting problematic behaviors than the pricing strategy, the app category, or the app's competitive environment. Additionally, we show that free apps are also more likely to share data with outside parties, and that a privacy policy is highly predictive of problematic levels of access to user data. Finally, strong competition results

in a small but positive pressure to produce more intrusive apps.

Our paper is a first step towards understanding the collection and sharing of personal user data. We analyze which user groups are most exposed, how developers gain access to sensitive information, and how they react to the factors that motivate them to engage in excessive data collection. We argue that it is important to anticipate the risk of excessive collection of private user data early, to take well informed measures to protect consumers and control these risks without unnecessarily curtailing the market's impressive potentials for generating user welfare. Understanding these questions should help decision makers to successfully design the market and protect users. Moreover our paper generates additional value, by creating a unique database on privacy in the market for mobile applications, and by providing carefully researched stylized facts about developers' data collection and sharing behavior. Future work can build on this foundation when developing a structural model that allows for a counterfactual analysis of potential regulatory or other measures.

References

Acquisti, Alessandro and Hal R Varian, "Conditioning Prices on Purchase History," *Marketing Science*, 2005, *24* (3), 367–381.

_ , Curtis R Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature*, 2016.

_ , Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science*, 2015, *347* (6221), 509–514.

_ , Leslie K John, and George Loewenstein, "What is Privacy Worth?," *The Journal of Legal Studies*, 2013, *42* (2), 249–274.

App Annie, "App Annie Mobile App Forecast: The Path to $100 Billion," 2016. Available at https://www.appannie.com/en/landing/forecast.

AppBrain, "Free vs. Paid Android Apps," 2016. Available at http://www.appbrain.com/stats/free-and-paid-android-applications.

Askalidis, Georgios, "The Impact of Large Scale Promotions on the Sales and Ratings of Mobile Apps: Evidence from Apple's App Store," Technical Report 2015.

Aziz, Arslan and Rahul Telang, "What is a Digital Cookie Worth?," Technical Report 2016.

Beresford, Alastair R, Dorothea Kübler, and Sören Preibusch, "Unwillingness to Pay for Privacy: A Field Experiment," *Economics Letters*, 2012, *117* (1), 25–27.

Carare, Octavian, "The Impact of Bestseller Rank on Demand: Evidence from the App Market," *International Economic Review*, 2012, *53* (3), 717–742.

Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira, "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online," in "Proceedings of the 22nd international conference on World Wide Web" International World Wide Web Conferences Steering Committee 2013, pp. 189–200.

Casadesus-Masanell, Ramon and Andres Hervas-Drane, "Competing With Privacy," *Management Science*, 2015, *61* (1), 229–246.

Chaudhari, Harshal, "The Impact of Zero-Price Promotions on Sales: A Case Study of Amazon Appstore," Technical Report 2015.

Chevalier, Judith A and Dina Mayzlin, "The Effect of Word of Mouth on Sales: Online Book Reviews," *Journal of Marketing Research*, 2006, *43* (3), 345–354.

Chia, Pern H, Yusuke Yamamoto, and N Asokan, "Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals," in "Proceedings of the 21st International Conference on World Wide Web" ACM 2012, pp. 311–320.

Christl, Wolfie and Sarah Spiekermann, *Networks of Control - A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*, Facultas, Wien, 2016.

Conitzer, Vincent, Curtis R Taylor, and Liad Wagman, "Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases," *Marketing Science*, 2012, *31* (2), 277–292.

Davis, Jason P, Yulia Muzyrya, and Pai-Ling Yin, "Experimentation Strategies and Entrepreneurial Innovation: Inherited Market Differences in the iPhone Ecosystem," Technical Report 2014.

Egelman, Serge, Adrienne P Felt, and David Wagner, "Choice Architecture and Smartphone Privacy: There is a Price for That," in "The Economics of Information Security and Privacy," Springer, 2013, pp. 211–236.

Fahl, Sascha, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith, "Why Eve and Mallory Love Android: An Analysis of Android SSL (in) Security," in "Proceedings of the 2012 ACM Conference on Computer and Communications Security" ACM 2012, pp. 50–61.

Garg, Rajiv and Rahul Telang, "Inferring App Demand from Publicly Available Data," *MIS Quarterly*, 2013, *37* (4), 1253–1264.

Ghose, Anindya and Sang Pil Han, "Estimating Demand for Mobile Applications in the New Economy," *Management Science*, 2014, *60* (6), 1470–1488.

Goldfarb, Avi and Catherine Tucker, "Privacy Regulation and Online Advertising," *Management Science*, 2011, *57* (1), 57–71.

_ and _ , "Shifts in Privacy Concerns," *American Economic Review: Papers and Proceedings*, 2012, *102* (3), 349–353.

Gross, Ralph and Alessandro Acquisti, "Information Revelation and Privacy in Online

Social Networks," in "Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society" ACM 2005, pp. 71–80.

Grossklags, Jens and Alessandro Acquisti, "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," in "Sixth Workshop on the Economics of Information Securtiy (WEIS)" 2007.

Hann, Il-Horn, Kai-Lung Hui, Sang-Yong T Lee, and Ivan PL Png, "Consumer Privacy and Marketing Avoidance: A Static Model," *Management Science*, 2008, *54* (6), 1094–1103.

Johnson, Garrett A, "The Impact of Privacy Policy on the Auction Market for Online Display Advertising," Technical Report 2014.

Johnson, Justin P, "Targeted Advertising and Advertising Avoidance," *The RAND Journal of Economics*, 2013, *44* (1), 128–144.

Kummer, Michael E and Patrick Schulte, "When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications," *ZEW Discussion Paper 16-031*, 2016.

Lin, Jialiu, Jason I Hong, and Norman Sadeh, "Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings," 2014.

_ , Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang, "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing," 2012, pp. 501–510.

Marthews, Alex and Catherine Tucker, "Government Surveillance and Internet Search Behavior," Technical Report 2017.

Miller, Amalia R and Catherine Tucker, "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science*, 2009, *55* (7), 1077–1093.

Preibusch, Sören and Joseph Bonneau, "The Privacy Landscape: Product Differentiation on Data Collection," in "Economics of Information Security and Privacy III," Springer, 2013, pp. 263–283.

Racherla, Pradeep, Jeffry S Babb, and Mark J Keith, "Pay-What-You-Want Pricing for Mobile Applications: The Effect of Privacy Assurances and Social Information," in "Conference for Information Systems Applied Research Proceedings," Vol. 4 2011, pp. 1–13.

Rainie, Lee, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish, "Anonymity, Privacy, and Security Online," Technical Report 2013.

Sarma, Bhaskar P, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy, "Android Permissions: A Perspective Combining Risks and Benefits," in "Proceedings of the 17th ACM symposium on Access Control Models and Technologies" ACM 2012, pp. 13–22.

Savage, Scott J and Donald M Waldman, "Privacy Tradeoffs in Smartphone Applications," *Economics Letters*, 2015.

Seneviratne, Suranga, Harini Kolamunna, and Aruna Seneviratne, "A Measurement Study of Tracking in Paid Mobile Applications," in "Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '15)" ACM 2015.

Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang, "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly*, 2013, *37* (4), 1141–1164.

Taylor, Curtis R, "Consumer Privacy and the Market for Customer Information," *The RAND Journal of Economics*, 2004, *35* (4), 631–650.

_ , Vincent Conitzer, and Liad Wagman, "Online Privacy and Price Discrimination," Technical Report 2010.

Tsai, Janice Y, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research*, 2011, *22* (2), 254–268.

Tucker, Catherine, "The Economics of Advertising and Privacy," *International Journal of Industrial Organization*, 2012, *30* (3), 326–329.

_ , "Social Networks, Personalized Advertising and Privacy Controls," *Journal of Marketing Research*, 2014, *51* (5), 546–562.

Turow, Joseph, Jennifer King, Chris J Hoofnagle, Amy Bleakley, and Michael Hennessy, "Americans Reject Tailored Advertising and Three Activities that Enable It," Technical

Report 2009.

Wathieu, Luc, "Privacy, Exposure and Price Discrimination," Technical Report 2002.

Yin, Pai-Ling, Jason P Davis, and Yulia Muzyrya, "Entrepreneurial Innovation: Killer Apps in the iPhone Ecosystem," *American Economic Review: Papers and Proceedings*, 2014, *104* (5), 255–259.

A Additional Tables and Figures

Figure A1: App Information in the Android Market 2012

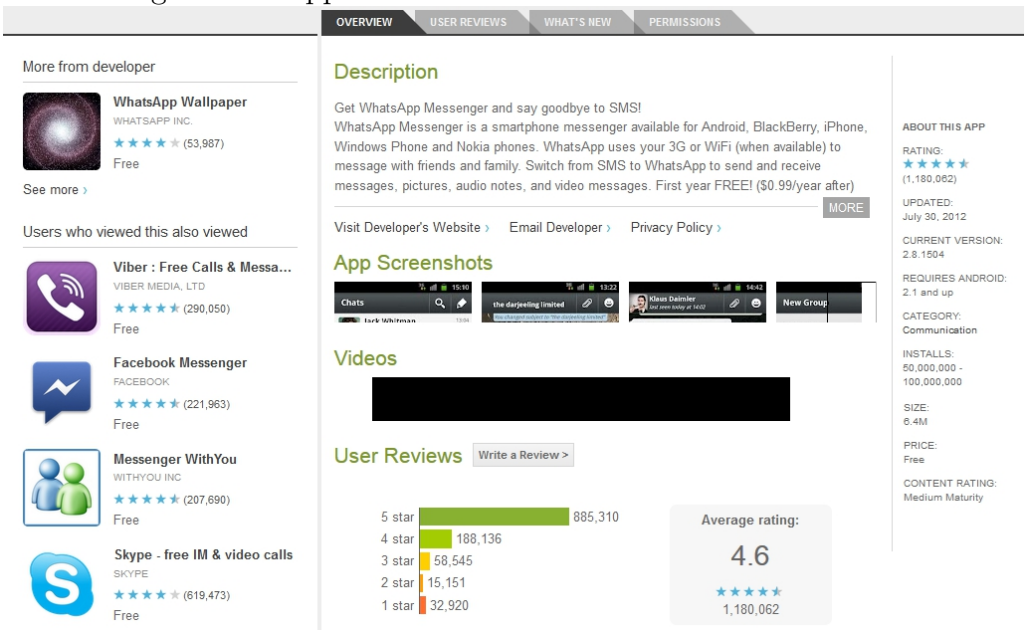


Figure A2: Permission Information in the Android Market 2012

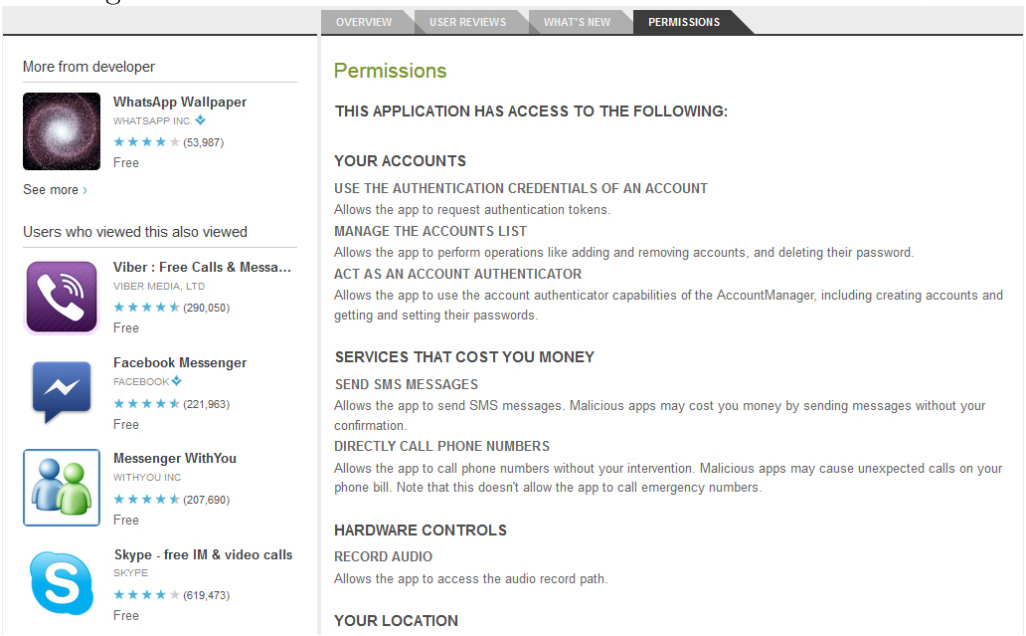


Figure A3: Comparison of Categories of Single- and Multi-App Developers

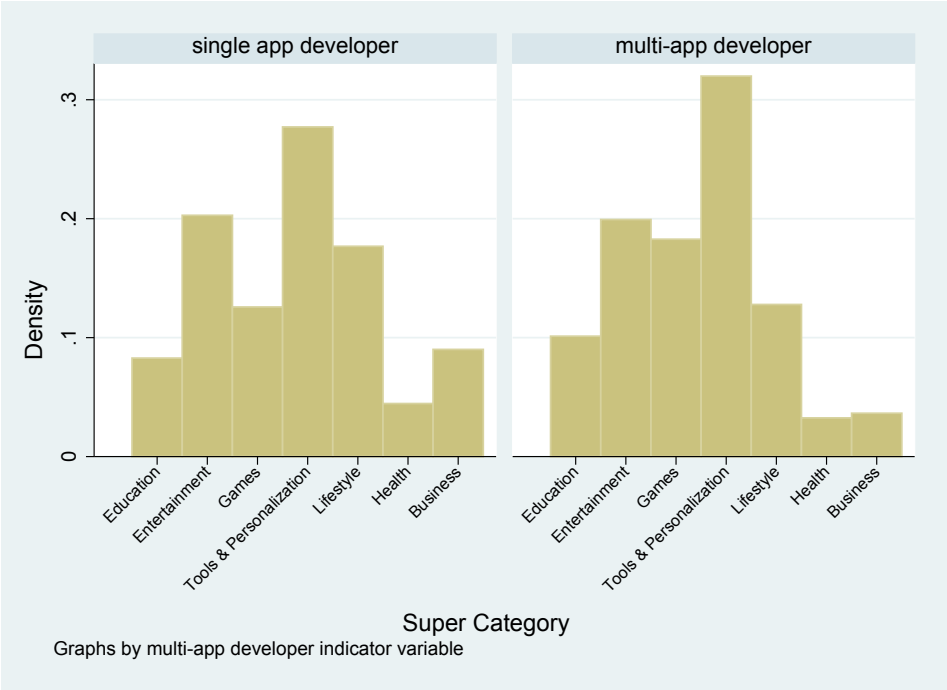


Figure A4: Comparison of Maturity Requirements of Single- and Multi-App Developers

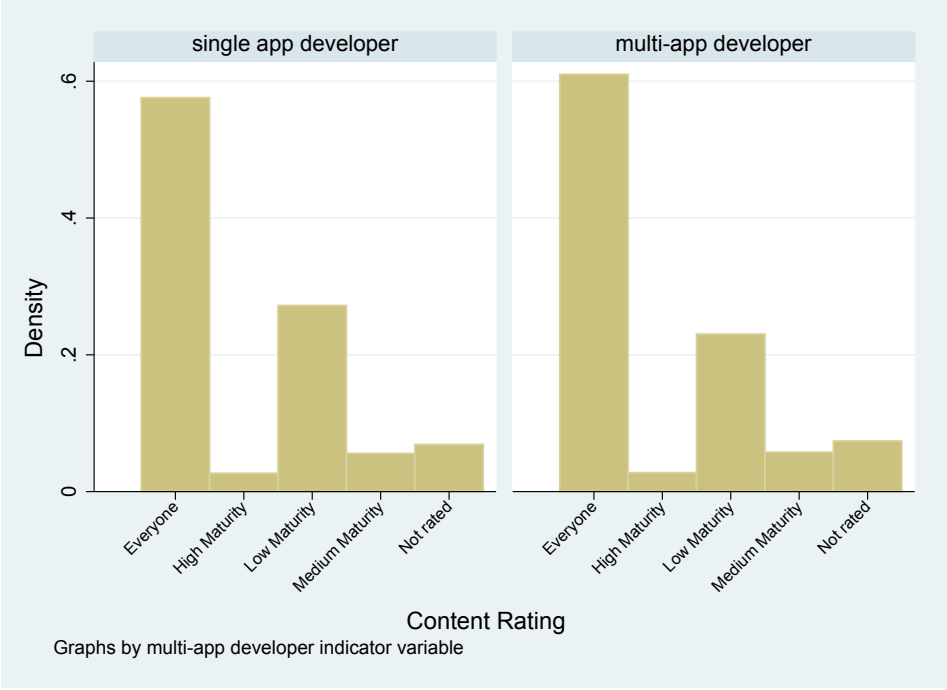


Table A1: Summary Statistics on Apps by Developer's Experience

	Developer's xth app				
	1	2	3	>4	Total
D_Privacy	0.448	0.419	0.422	0.452	0.444
	(65300)	(25026)	(13515)	(76199)	(180040)
App grade	1.997	2.002	2.014	2.119	2.042
	(36152)	(13958)	(7653)	(31130)	(88893)
Failing	0.0342	0.0387	0.0413	0.0855	0.0535
	(36152)	(13958)	(7653)	(31130)	(88893)
App exit by 2016	0.497	0.475	0.471	0.591	0.532
	(65300)	(25026)	(13515)	(76199)	(180040)
>7 3rd parties	0.127	0.0878	0.0928	0.122	0.116
	(22214)	(8552)	(4591)	(18287)	(53644)
>3 3rd parties	0.313	0.263	0.281	0.302	0.298
	(22214)	(8552)	(4591)	(18287)	(53644)
D_Price	0.180	0.283	0.287	0.340	0.270
	(65300)	(25026)	(13515)	(76199)	(180040)
Local Market Share	0.0350	0.0385	0.0414	0.0464	0.0408
	(65300)	(25026)	(13515)	(76199)	(180040)
Competitor Inst.(Mln)	0.00447	0.00393	0.00361	0.00362	0.00396
	(49218)	(19117)	(10280)	(59677)	(138292)
Categ: Education	0.0838	0.0842	0.0900	0.115	0.0976
	(65300)	(25026)	(13515)	(76199)	(180040)
Categ: Entertain.	0.199	0.197	0.195	0.203	0.200
	(65300)	(25026)	(13515)	(76199)	(180040)
Categ: Games	0.156	0.195	0.199	0.173	0.172
	(65300)	(25026)	(13515)	(76199)	(180040)
Categ: Tools/Perso.	0.293	0.313	0.316	0.326	0.311
	(65300)	(25026)	(13515)	(76199)	(180040)
Categ: Lifestyle	0.157	0.129	0.125	0.126	0.137
	(65300)	(25026)	(13515)	(76199)	(180040)
Categ: Health	0.0416	0.0377	0.0351	0.0282	0.0349
	(65300)	(25026)	(13515)	(76199)	(180040)
Everyone	0.594	0.629	0.634	0.597	0.603
	(65300)	(25026)	(13515)	(76199)	(180040)
High Maturity (18+)	0.0254	0.0241	0.0247	0.0311	0.0276
	(65300)	(25026)	(13515)	(76199)	(180040)
Med. Maturity (16+)	0.0539	0.0508	0.0482	0.0641	0.0574
	(65300)	(25026)	(13515)	(76199)	(180040)
Low Maturity (13+)	0.249	0.218	0.218	0.240	0.239
	(65300)	(25026)	(13515)	(76199)	(180040)
Installations (in 1000)	76.09	81.59	78.06	66.23	72.83
	(65300)	(25026)	(13515)	(76199)	(180040)
Average Rating	3.951	3.927	3.899	3.929	3.935
	(65300)	(25026)	(13515)	(76199)	(180040)
# Ratings in 1000	0.471	0.481	0.462	0.318	0.407
	(65300)	(25026)	(13515)	(76199)	(180040)
Privacy Policy	0.0416	0.0351	0.0371	0.0445	0.0416
	(61610)	(23571)	(12698)	(71499)	(169378)
Dummy: Top-Developer	0.00285	0.00519	0.00740	0.0114	0.00714
	(65300)	(25026)	(13515)	(76199)	(180040)
Single App Developer	0.540	0	0	0	0.196
	(65300)	(25026)	(13515)	(76199)	(180040)
Observations	180040				

NOTES: The table shows the means and N.obs. of the main variables for the developer's first, second, third and later apps. The unit of observations is the app i in 2012. no. of developers = 65300; no. of apps = 180040.

Table A2: Multi-App Developers (Excl. First Two Apps) and Permission Usage

	sensitive				potential malicious			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Average Rating	-0.004***	-0.007***	-0.005***	-0.006***	-0.005***	-0.008***	-0.008***	-0.008***
	(0.002)	(0.002)	(0.001)	(0.002)	(0.001)	(0.001)	(0.001)	(0.002)
# Ratings in 1000	0.001***	0.001***	0.001***	0.001***	0.000	0.001**	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Dummy: Video	0.026**	0.024**	0.020**	0.021**	0.018*	0.012	0.010	0.008
	(0.010)	(0.010)	(0.010)	(0.010)	(0.010)	(0.009)	(0.009)	(0.010)
Dummy: Website	0.023**	0.023**	0.021**	0.019*	0.022	0.022	0.021	0.021
	(0.010)	(0.010)	(0.009)	(0.011)	(0.013)	(0.014)	(0.015)	(0.016)
Log. Size (in KB)	0.026***	0.027***	0.018***	0.024***	0.028***	0.025***	0.022***	0.027***
	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.004)
Privacy Policy	0.101***	0.106***	0.074***	0.099***	0.059***	0.069***	0.052**	0.058**
	(0.027)	(0.028)	(0.025)	(0.033)	(0.022)	(0.026)	(0.025)	(0.029)
DPrice	-0.729***				-1.076***			
	(0.131)				(0.140)			
Log. Price	0.051***				0.074***			
	(0.011)				(0.011)			
Categ: Education		-0.056***				-0.060***		
		(0.016)				(0.015)		
Categ: Entertain.		0.007				0.003		
		(0.013)				(0.010)		
Categ: Games		-0.041***				-0.029**		
		(0.015)				(0.013)		
Categ: Tools/Perso.		0.021				-0.047***		
		(0.014)				(0.011)		
Categ: Lifestyle		0.024*				-0.018		
		(0.014)				(0.012)		
Categ: Health		-0.023				-0.035***		
		(0.015)				(0.013)		
Matur. Rating n.a.			0.008				-0.036*	
			(0.017)				(0.020)	
High Maturity (18+)			0.174***				0.064***	
			(0.020)				(0.015)	
Med. Maturity (16+)			0.200***				0.090***	
			(0.015)				(0.011)	
Low Maturity (13+)			0.406***				0.181***	
			(0.016)				(0.016)	
Local Market Share				0.080***				0.102***
				(0.016)				(0.017)
Competitor Inst.(Mln)				1.144***				1.228***
				(0.258)				(0.198)
Constant	0.887***	0.268***	0.201***	0.279***	1.466***	0.611***	0.551***	0.550***
	(0.128)	(0.026)	(0.022)	(0.024)	(0.135)	(0.027)	(0.025)	(0.028)
Observations	84196	84196	84196	65711	84196	84196	84196	65711
Developers	13180	13180	13180	11725	13180	13180	13180	11725
Adjusted R^2	0.035	0.014	0.154	0.013	0.087	0.014	0.049	0.018

NOTES: The table analyzes the driving factors of developers' permission usage. The regressions are panel fixed OLS regressions with a developer fixed effect. The dependent variable in columns 1-4 is a dummy indicating the usage of sensitive permissions and, in columns 5-8, a dummy that indicates potentially malicious permissions. Col. 1&5 analyze paid and free apps seperately. Col. 2&6 analyze categories seperately (baseline: "Business"). Col. 3&7 shows how intrusiveness varies for different maturity ratings (baseline: "Everybody"), and col. 4&8 add variables that measure the strength of the competitors. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

Table A3: Multi-App Developers' (Excl. First Two Apps) Success

	Log(Demand)				App survives until 2016			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Average Rating	0.104***	0.039	0.024	0.033	0.006***	0.008***	0.006***	0.006***
	(0.021)	(0.024)	(0.023)	(0.022)	(0.001)	(0.002)	(0.001)	(0.001)
# Ratings in 1000	0.019***	0.009	0.027***	0.024***	0.001**	0.001*	0.001**	0.001**
	(0.007)	(0.006)	(0.010)	(0.008)	(0.001)	(0.001)	(0.001)	(0.001)
Dummy: Video	1.322***	0.985***	1.139***	1.067***	0.036***	0.031***	0.036***	0.037***
	(0.122)	(0.136)	(0.126)	(0.124)	(0.008)	(0.009)	(0.008)	(0.008)
Dummy: Website	0.053	-0.005	0.058	0.005	0.005	-0.002	0.007	0.006
	(0.168)	(0.199)	(0.190)	(0.184)	(0.016)	(0.021)	(0.016)	(0.016)
Log. Size (in KB)	0.337***	0.257***	0.248***	0.178***	0.007***	0.009***	0.007***	0.007***
	(0.026)	(0.030)	(0.026)	(0.027)	(0.003)	(0.003)	(0.002)	(0.003)
Privacy Policy	1.876***	1.608***	1.883***	1.608***	0.091***	0.098**	0.093***	0.092***
	(0.232)	(0.244)	(0.261)	(0.225)	(0.034)	(0.043)	(0.034)	(0.035)
DPrice	-12.994***				-0.258**			
	(1.049)				(0.117)			
Log. Price	0.734***				0.022**			
	(0.088)				(0.010)			
Local Market Share		7.822***				0.055***		
		(0.244)				(0.012)		
Competitor Inst.(Mln)		7.785***				-0.081		
		(2.072)				(0.170)		
Categ: Education		0.135				0.023		
		(0.191)				(0.015)		
Categ: Entertain.		0.652***				-0.004		
		(0.179)				(0.015)		
Categ: Games		0.472**				0.011		
		(0.198)				(0.015)		
Categ: Tools/Perso.		0.689***				0.038***		
		(0.173)				(0.014)		
Categ: Lifestyle		0.278				0.017		
		(0.178)				(0.014)		
Categ: Health		0.431**				0.037**		
		(0.211)				(0.017)		
Matur. Rating n.a.			-0.632***				-0.020	
			(0.199)				(0.014)	
High Maturity (18+)			0.673***				0.044*	
			(0.153)				(0.023)	
Med. Maturity (16+)			1.061***				0.006	
			(0.129)				(0.012)	
Low Maturity (13+)			1.070***				-0.009	
			(0.127)				(0.006)	
Total Perm.				0.387***				0.002
				(0.027)				(0.002)
(Total Perm.)^2				-0.004***				-0.000
				(0.001)				(0.000)
DPrivacy				0.155				-0.015
				(0.122)				(0.010)
DGoogle				-0.506***				0.004
				(0.119)				(0.009)
DPrivCatSpec				0.147				-0.004
				(0.107)				(0.007)
Constant	2.319**	-7.667***	-6.942***	-7.402***	0.602***	0.317***	0.350***	0.348***
	(1.045)	(0.328)	(0.263)	(0.262)	(0.119)	(0.029)	(0.022)	(0.023)
Observations	83743	65331	83743	83743	84196	65711	84196	84196
Developers	13154	11698	13154	13154	13180	11725	13180	13180
Adjusted R^2	0.111	0.076	0.017	0.029	0.004	0.006	0.005	0.004

NOTES: The table analyzes the driving factors of developers' permission usage and the resulting outcome that was obtained in 2016. The first outcome measures contemporaneous demand (based on ratings the app received between April and September 2012 (5 months) as demand proxy; col. 1-4). The second outcome is is app survival until 2016 (col. 5-8). The regressions are panel fixed effects OLS regressions with a developer fixed effect. Col. 1&5 analyze paid and free apps seperately. Col. 2&6 analyze environmental factors, such as the competitors' strength and the app-categories seperately (baseline: "Business"). Col. 3&7 shows how intrusiveness varies for different maturity ratings (baseline: "Everybody"), and col. 4&8 add variables that measure the app's permission requirements in 2012. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

Table A4: Multi-App Developers (Excl. First Two Apps) and 3rd Party Sharing

	App shares with 3rd Parties				App shares with >7 3rd Parties			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Average Rating	0.000	-0.015***	-0.017***	-0.012***	0.001	-0.001	-0.001	-0.000
	(0.004)	(0.005)	(0.005)	(0.004)	(0.002)	(0.003)	(0.002)	(0.002)
# Ratings in 1000	-0.000	0.000	0.001***	0.000	0.003***	0.003***	0.003***	0.003***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)	(0.001)	(0.001)
Dummy: Video	0.008	-0.026	-0.011	-0.017	0.020**	0.013	0.017*	0.016*
	(0.016)	(0.018)	(0.017)	(0.015)	(0.010)	(0.011)	(0.010)	(0.010)
Dummy: Website	0.028	-0.003	0.024	0.017	0.016	0.005	0.015	0.014
	(0.020)	(0.023)	(0.020)	(0.019)	(0.019)	(0.021)	(0.019)	(0.020)
Log. Size (in KB)	0.049***	0.042***	0.043***	0.024***	0.014***	0.012***	0.013***	0.009***
	(0.005)	(0.005)	(0.005)	(0.004)	(0.003)	(0.003)	(0.002)	(0.002)
Privacy Policy	0.077***	0.068*	0.080**	0.053*	0.019	0.026	0.019	0.014
	(0.026)	(0.035)	(0.034)	(0.027)	(0.021)	(0.022)	(0.021)	(0.020)
DPrice	-0.962***				-0.054			
	(0.170)				(0.094)			
Log. Price	0.055***				0.000			
	(0.014)				(0.008)			
Local Market Share		0.200***				0.049***		
		(0.022)				(0.013)		
Competitor Inst.(Mln)		1.992***				-0.003		
		(0.451)				(0.264)		
Categ: Education		0.004				0.002		
		(0.041)				(0.021)		
Categ: Entertain.		0.026				-0.000		
		(0.038)				(0.021)		
Categ: Games		0.055				0.031		
		(0.039)				(0.021)		
Categ: Tools/Perso.		-0.019				-0.003		
		(0.037)				(0.019)		
Categ: Lifestyle		0.027				0.016		
		(0.038)				(0.024)		
Categ: Health		-0.000				-0.024		
		(0.044)				(0.024)		
Matur. Rating n.a.			-0.058*				-0.014	
			(0.034)				(0.011)	
High Maturity (18+)			0.022				-0.006	
			(0.030)				(0.014)	
Med. Maturity (16+)			0.061***				0.003	
			(0.022)				(0.015)	
Low Maturity (13+)			0.127***				0.027***	
			(0.019)				(0.009)	
DPrivacy				-0.018				0.017
				(0.019)				(0.012)
DGoogle				-0.170***				-0.035**
				(0.022)				(0.015)
#CriticalPerm.				0.117***				0.019***
				(0.008)				(0.003)
DPrivCatSpec				-0.012				0.006
				(0.017)				(0.013)
Constant	0.991***	0.376***	0.360***	0.277***	0.010	0.016	0.011	-0.008
	(0.172)	(0.057)	(0.043)	(0.040)	(0.096)	(0.034)	(0.027)	(0.028)
Observations	21845	17473	21845	21845	21845	17473	21845	21845
Developers	6443	5642	6443	6443	6443	5642	6443	6443
Adjusted R^2	0.124	0.034	0.030	0.118	0.017	0.013	0.010	0.019

NOTES: The table analyzes the driving factors of developers' permission usage and the resulting outcome that was obtained in 2016. The first outcome is sharing data with any outside parties, the second outcome is sharing data with several outside parties (> 3). The regressions are panel fixed OLS regressions with a developer fixed effect. The dependent variable in columns 1-4 is a dummy that indicates whether the app will share data with any outside parties in 2016. and, in columns 5-8, an indicator whether the app will share data with more than 7 outside parties. Col. 1&5 analyze paid and free apps separately. Col. 2&6 analyze environmental factors, such as the competitors' strength and the app-categories separately (baseline: "Business"). Col. 3&7 shows how intrusiveness varies for different maturity ratings (baseline: "Everybody"), and col. 4&8 add variables that measure the app's permission requirements in 2012. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

B Additional Tables - Online Appendix

Table B1: Summary Statistics on Apps by Age Category

	Categories					
	Everyone	High	Low	Medium	Not rated	Total
D_Privacy	0.265	0.570	0.895	0.627	0.248	0.444
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
>7 3rd parties	0.0748	0.138	0.239	0.195	0.0129	0.116
	(35797)	(745)	(12451)	(2249)	(2402)	(53644)
>3 3rd parties	0.240	0.338	0.489	0.425	0.0570	0.298
	(35797)	(745)	(12451)	(2249)	(2402)	(53644)
App grade	1.897	2.142	2.378	2.179	1.903	2.042
	(53910)	(1503)	(23502)	(4239)	(5739)	(88893)
Failing	0.0198	0.0785	0.134	0.0840	0.0110	0.0535
	(53910)	(1503)	(23502)	(4239)	(5739)	(88893)
App exit by 2016	0.493	0.657	0.559	0.638	0.632	0.532
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
D_Price	0.325	0.237	0.135	0.201	0.322	0.270
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Local Market Share	0.0407	0.0296	0.0417	0.0447	0.0397	0.0408
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Competitor Inst.(Mln)	0.00301	0.00376	0.00635	0.00492	0.00356	0.00396
	(84902)	(3472)	(32587)	(7653)	(9678)	(138292)
Categ: Education	0.112	0.0628	0.0767	0.0497	0.0972	0.0976
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Categ: Entertain.	0.163	0.272	0.241	0.327	0.244	0.200
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Categ: Games	0.178	0.269	0.116	0.315	0.149	0.172
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Categ: Tools/Perso.	0.365	0.181	0.244	0.128	0.288	0.311
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Categ: Lifestyle	0.1000	0.128	0.224	0.129	0.175	0.137
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Categ: Health	0.0368	0.0397	0.0346	0.0270	0.0244	0.0349
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Installations (in 1000)	60.15	49.78	98.26	174.6	23.24	72.83
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Average Rating	4.001	3.971	3.935	3.944	3.368	3.935
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
# Ratings in 1000	0.310	0.300	0.577	1.165	0.101	0.407
	(108640)	(4967)	(42952)	(10329)	(13152)	(180040)
Privacy Policy	0.0371	0.0436	0.0584	0.0691	0.00201	0.0416
	(102409)	(4634)	(40190)	(9703)	(12442)	(169378)
Observations	180040					

NOTES: The table shows the means of the main variables by Age Rating. The unit of observations is the app i in 2012. Column 1 shows Apps rated for "everyone" and Column 2, 3, and 4 show the other 3 matruity levels. Col. 5 shows apps that provided no rating information. No. of developers = 65300; no. of apps = 180040.

Table B2: Multi-App Developers Learning - First App Success

	sensitive	potential malic.	# pot. malic.	privacygrade	failgrade	Data Sharing
	(1)	(2)	(3)	(4)	(5)	(6)
Dummy: Top-Developer	0.112	0.144**	0.131	0.103	0.016	-0.069
	(0.092)	(0.059)	(0.323)	(0.138)	(0.039)	(0.084)
Apps by Developer	0.000	0.000	0.000	0.000	-0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
App1: installations (mln)	-21.693**	0.045	-41.742	8.972	2.043	11.339
	(9.617)	(8.517)	(51.321)	(10.938)	(3.044)	(9.170)
App1: ratings (1000s)	0.004**	0.002	0.007	0.008**	0.002*	0.001
	(0.002)	(0.001)	(0.008)	(0.003)	(0.001)	(0.002)
App1: rel market share	0.039	-0.084	0.496	-0.465***	-0.114**	-0.042
	(0.139)	(0.153)	(0.882)	(0.176)	(0.048)	(0.119)
App2: installations (mln)	33.872*	34.262*	123.306	14.587	-2.616	14.526
	(18.744)	(19.374)	(112.325)	(32.056)	(10.894)	(15.216)
App2: ratings (1000s)	-0.003**	-0.002*	-0.011	0.000	0.001	-0.001
	(0.001)	(0.001)	(0.007)	(0.003)	(0.001)	(0.001)
App2: rel. market share	-0.038	-0.119	0.043	-0.010	0.026	0.193*
	(0.118)	(0.137)	(0.758)	(0.146)	(0.046)	(0.112)
App3: installations (mln)	16.638*	6.146	39.423	45.907**	10.573	22.174
	(9.917)	(9.186)	(48.896)	(23.245)	(6.883)	(21.123)
App3: ratings (1000s)	0.002	-0.003	0.013	-0.002	0.001	0.002
	(0.003)	(0.003)	(0.017)	(0.007)	(0.002)	(0.004)
App3: rel. market share	-0.016	0.069	-0.332	-0.101	0.008	-0.139*
	(0.105)	(0.061)	(0.291)	(0.154)	(0.054)	(0.078)
Log. Developers' app # x	-0.017	-0.047***	-0.062	0.114**	0.049***	0.010
	(0.016)	(0.016)	(0.078)	(0.048)	(0.018)	(0.019)
Average Rating	-0.019**	-0.042***	-0.071**	-0.036***	-0.002	0.003
	(0.008)	(0.007)	(0.031)	(0.013)	(0.005)	(0.009)
# Ratings in 1000	0.002***	0.001***	0.009***	0.001	0.000	0.005***
	(0.000)	(0.000)	(0.003)	(0.001)	(0.000)	(0.001)
Dummy: Video	-0.020	0.007	-0.261*	-0.034	0.005	0.024
	(0.037)	(0.035)	(0.136)	(0.038)	(0.012)	(0.025)
Dummy: Website	-0.001	0.018	-0.154	0.056	0.016	0.093***
	(0.037)	(0.037)	(0.181)	(0.045)	(0.017)	(0.027)
Privacy Policy	0.094**	0.079**	0.654***	0.078	0.011	0.128***
	(0.044)	(0.037)	(0.251)	(0.098)	(0.027)	(0.049)
Constant	0.543***	1.007***	3.011***	1.950***	-0.043	0.161***
	(0.053)	(0.051)	(0.244)	(0.135)	(0.048)	(0.053)
Observations	70000	70000	70000	29710	29710	17461
Adjusted R^2	0.009	0.032	0.009	0.036	0.035	0.024

NOTES: The table analyzes whether app developers' success on the first and second apps is associated with their permission usage and the resulting (2014) *privacygrade* on subsequent apps. The regressions are panel OLS regressions clustered standard errors at the developer level. The dependent variables in the five columns are: (1) usage of sensitive permissions (2) usage of potentially malicious permissions (according to Google) (3) number of potentially malicious permissions (according to Google) (4) the *privacygrade* that was obtained in 2014 (1=A+, 5=F), and (5) a dummy that indicates that the app will receive a failgrade (C or F). Col. 6 includes a dummy of whether the app will share its data with three or more 3rd (outside) parties. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

Table B3: Multi-App Developers and Environment - Permission Usage

	sensitive				potential malicious			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Average Rating	-0.005***	-0.009***	-0.006***	-0.009***	-0.004***	-0.009***	-0.009***	-0.009***
	(0.001)	(0.001)	(0.001)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)
# Ratings in 1000	0.001***	0.001***	0.001***	0.001***	0.000**	0.001***	0.001***	0.001**
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Dummy: Video	0.044***	0.044***	0.032***	0.035***	0.045***	0.038***	0.032***	0.039***
	(0.007)	(0.007)	(0.007)	(0.008)	(0.007)	(0.007)	(0.007)	(0.007)
Dummy: Website	0.024***	0.025***	0.021***	0.024**	0.037***	0.037***	0.035***	0.037***
	(0.008)	(0.008)	(0.007)	(0.009)	(0.010)	(0.010)	(0.010)	(0.012)
Privacy Policy	0.110***	0.114***	0.077***	0.098***	0.066***	0.073***	0.055***	0.058***
	(0.019)	(0.020)	(0.018)	(0.023)	(0.015)	(0.018)	(0.017)	(0.020)
DPrice	-0.673***				-1.093***			
	(0.086)				(0.091)			
Log. Price	0.049***				0.078***			
	(0.007)				(0.007)			
Categ: Education		-0.031**				-0.058***		
		(0.012)				(0.011)		
Categ: Entertain.		0.033***				0.006		
		(0.011)				(0.008)		
Categ: Games		-0.022*				-0.035***		
		(0.012)				(0.010)		
Categ: Tools/Perso.		0.046***				-0.053***		
		(0.011)				(0.008)		
Categ: Lifestyle		0.066***				-0.006		
		(0.012)				(0.009)		
Categ: Health		0.003				-0.032***		
		(0.013)				(0.010)		
Matur. Rating n.a.			-0.010				-0.078***	
			(0.012)				(0.013)	
High Maturity (18+)			0.178***				0.064***	
			(0.016)				(0.011)	
Med. Maturity (16+)			0.206***				0.092***	
			(0.011)				(0.008)	
Low Maturity (13+)			0.432***				0.177***	
			(0.010)				(0.010)	
Local Market Share				0.086***				0.110***
				(0.013)				(0.013)
Competitor Inst.(Mln)				1.559***				1.481***
				(0.196)				(0.149)
Constant	1.018***	0.415***	0.319***	0.430***	1.687***	0.783***	0.714***	0.739***
	(0.083)	(0.013)	(0.008)	(0.010)	(0.087)	(0.012)	(0.010)	(0.012)
Observations	136078	136078	136078	105371	136078	136078	136078	105371
Developers	29530	29530	29530	26857	29530	29530	29530	26857
Adjusted R^2	0.018	0.009	0.158	0.008	0.058	0.007	0.041	0.009

NOTES: The table analyzes the driving factors of developers' permission usage. The regressions are panel fixed OLS regressions with a developer fixed effect. It includes a developer's first two apps, and developers where the order in which the developer developed their apps could not be identified. The dependent variable in columns 1-4 is a dummy indicating the usage of sensitive permissions and, in columns 5-8, a dummy that indicates potentially malicious permissions. Col. 1&5 analyze paid and free apps seperately. Col. 2&6 analyze categories seperately (baseline: "Business"). Col. 3&7 shows how intrusiveness varies for different maturity ratings (baseline: "Everybody"), and col. 4&8 add variables that measure the strength of the competitors. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

Table B4: Multi-App Developers and Environment - Future Outlook *privacygrade*

	privacygrade				failgrade			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Average Rating	-0.006**	-0.003	-0.005*	-0.004	-0.000	0.002	-0.009***	-0.000
	(0.003)	(0.004)	(0.003)	(0.003)	(0.001)	(0.001)	(0.001)	(0.001)
# Ratings in 1000	0.002***	0.003***	0.002***	0.001**	0.001***	0.001**	0.001***	0.000**
	(0.001)	(0.001)	(0.001)	(0.001)	(0.000)	(0.000)	(0.000)	(0.000)
Dummy: Video	0.072***	0.075***	0.065***	0.027**	0.020***	0.024***	0.032***	0.013***
	(0.014)	(0.016)	(0.013)	(0.012)	(0.005)	(0.006)	(0.007)	(0.005)
Dummy: Website	0.037**	0.037*	0.037**	0.003	0.008	0.008	0.035***	0.005
	(0.017)	(0.021)	(0.017)	(0.014)	(0.005)	(0.006)	(0.010)	(0.005)
Privacy Policy	0.075***	0.066**	0.054**	-0.001	0.013	0.010	0.055***	-0.001
	(0.026)	(0.032)	(0.026)	(0.024)	(0.009)	(0.012)	(0.017)	(0.009)
DPrice	-0.640				0.054			
	(0.453)				(0.096)			
Log. Price	0.047				-0.005			
	(0.039)				(0.008)			
Local Market Share		0.043**				0.001		
		(0.019)				(0.007)		
Competitor Inst.(Mln)		1.492***				0.211**		
		(0.252)				(0.103)		
Categ: Education		-0.000				0.003		
		(0.022)				(0.007)		
Categ: Entertain.		0.016				0.003		
		(0.019)				(0.008)		
Categ: Games		0.023				0.015**		
		(0.021)				(0.007)		
Categ: Tools/Perso.		-0.031				0.004		
		(0.020)				(0.007)		
Categ: Lifestyle		0.032				0.006		
		(0.020)				(0.007)		
Categ: Health		0.010				0.003		
		(0.030)				(0.011)		
Matur. Rating n.a.			0.004				-0.078***	
			(0.016)				(0.013)	
High Maturity (18+)			0.118***				0.064***	
			(0.018)				(0.011)	
Med. Maturity (16+)			0.159***				0.092***	
			(0.015)				(0.008)	
Low Maturity (13+)			0.256***				0.177***	
			(0.012)				(0.010)	
DPrivacy				0.045***				-0.004
				(0.011)				(0.004)
DGoogle				0.507***				-0.043***
				(0.014)				(0.004)
#CriticalPerm.				0.068***				0.025***
				(0.004)				(0.002)
Constant	2.579***	2.013***	1.958***	1.445***	-0.004	0.035***	0.714***	0.026***
	(0.451)	(0.028)	(0.018)	(0.018)	(0.098)	(0.010)	(0.010)	(0.006)
Observations	67404	51504	67404	67404	67404	51504	136078	67404
Developers	22410	19755	22410	22410	22410	19755	29530	22410
Adjusted R^2	0.005	0.009	0.038	0.214	0.003	0.003	0.041	0.033

NOTES: The table analyzes the driving factors of developers' permission usage and the resulting *privacygrade* that was obtained in 2014. The regressions are panel fixed OLS regressions with a developer fixed effect (and they include a developer's first and second app). The dependent variable in columns 1-4 is the grade that was obtained in 2014 (1=A+, 5=F) and, in columns 5-8, a dummy that indicates that the app will receive a failgrade (C or F). Col. 1&5 analyze paid and free apps seperately. Col. 2&6 analyze categories seperately (baseline: "Business"). Col. 3&7 shows how intrusiveness varies for different maturity ratings (baseline: "Everybody"), and col. 4&8 add variables that measure the strength of the competitors. Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01

C Additional Approach: Apps over Time

C.1 Analyzing Apps over Time

To deepen the analysis we exploit the fact that we can study apps over time. To shed light on developers' main strategies of gaining and managing access to personal user data over time, we can analyze two strategies. We can show to which extent developers added permissions as a function of success, by investigating the slope with which permissions are added. Second, we can analyze whether developers initially roll out their apps at low levels of intrusiveness, and add in more intrusive permissions on later updates. Note, however, that this analysis can only be performed on a very limited number of observations, which is why we did not include it in the body of the paper.

Specifically, we can study the apps on a weekly interval in 2012, and then observe it in 2014 and 2016, in combination with the data from *privacygrade.org*. This allows us to move beyond the cross section and highlight how the development of an app over time can predict its behavior with respect to privacy. For example, we study whether it is possible to predict the *privacygrade* in 2014 based on behavior in 2012, and specifically we can study whether a bad grade in 2014 is a function of 2012-6-month success and the competitive situation in the market. Moreover, we can study what happens when apps switch from the paid to the free model. Finally, we want to highlight at what point in an app's life cycle developers tend to introduce privacy-sensitive permissions (if at all).

$$Privacy_{it+1} = \alpha_i + \gamma P_{it} + \theta X_{2,it} + \varepsilon_{it}. \tag{4}$$

In this regression $Privacy_{it+1}$ measures the app's future privacy sensitiveness, α_i is a fixed effect, P_{it} measures the app's price (which is potentially 0), and $X_{2,it}$ are other control variables, such as the app's competitive environment or the app's past success (corresponding to the user base).

Exploiting the time dimension within apps also allows us to gain a deeper insight on how developers' data strategies influence their apps' success and continued innovation. This question is actually hard to analyze in cross-sectional data and can only be understood if the temporal dynamics in the data can be exploited. Our strategy is to look for major shifts in the permissions, and/or for sensitive permissions that were introduced without improved functionality. We want to use such shifts in a regression discontinuity design, where we estimate the counterfactual growth path of the app absent the new permissions based on its previous growth path, or based on the growth path of comparable app. Any kinks in the growth path would be attributed to the change in permissions. While permissions may be negatively correlated with demand, the data might be a valuable input for continued innovation. Hence, we will also study the frequency of updates as a measure of an app's innovativeness.

$$AppSuccess_{it+1} = \alpha_i + \beta D_{it}^{Privacy} + \gamma P_{it} + \theta X_{1,it} + \varepsilon_{it}. \tag{5}$$

We measure *AppSuccess* via continued demand, innovativeness and long-term survival as indicators of viability. Privacy, price and the control variables have been described above. The key challenge in this analysis will be capturing redundant permissions. We will use three strategies to tackle this challenge: First, we exploit the categorical information from the Google Play Store, to identify permissions which are hardly ever used by apps in the same category. Second, we can exploit pairs of free and paid apps in the data, where the paid app can serve as "technological benchmark," that allows the researcher to see what is needed for the app's functionality. Third and finally, we can use the information on *privacygrade.org* to filter out which apps are malicious and which permissions they typically use.

Special Identification Strategy - Early App Development and "Excessive" Data Use Our main strategy for identification exploits apps that were newly launched during our first data acquisition in 2012. Our data structure allows us to identify apps that were launched between April and September 2012 and to focus on this inflow sample of apps. For these apps, we can analyze and categorize their early success on the market, and their continued development. Figures C1 and C2 show the early development of ratings by free and paid apps respectively. Important dimensions for this issue are variables like initial growth, the competitive environment, the app's initial permission usage, and the developer's experience. Once we characterized the app's early properties and success patterns, we can predict the app's grade on *privacgrade.org* as a primary outcome that measures data behavior, and we can identify early-stage patterns that are more likely to result in a problematic *privacygrade*.

C.2 Correlational Results

In this section we show results for a selected sample of 750 apps which were all launched at the same point in time (Spring 2012) and were all featured by Google as a "top new app." Conditioning on a such narrowly defined set of apps allows us to study their development over time. Moreover, being able to observe the app's adolescence allows us to leverage greater variation in our measure of installations, because Google's step function has much smaller intervals initially. The results in Table C1 evaluate the timing of when permissions were introduced and how initial dynamics translate into better or worse *privacygrades* in 2014.

Specifically, the table analyzes the driving factors of developers' permission usage and the resulting *privacygrade* that was obtained in 2014. The regressions are panel fixed effects OLS regressions with a developer fixed effect. The dependent variable is a dummy variable indicating that the app will receive a $failgrade$ (C to F) in 2014 (columns 1 and 2), the 5 grade scale that was obtained in 2014 (1=A+, 5=F; in columns 3 and 4), and the number of permissions used in 2016 (columns 5 and 6). The results in Table C1 show, that neither app growth in the app's first months (columns 1, 3 and 5), nor growth acceleration based on ratings (columns 2, 4 and 6) are extremely powerful predictors of the future *privacygrade*, but both predict permission usage in 2016. Regarding the grade in 2014 it seems that initial growth is weakly negatively related to receiving a $failgrade$ (if anything). Regarding permission usage, initial growth and growth acceleration are positively related to future permission usage.

Note, however, that the confidence bands in this analysis are generally much wider than in the previous analysis, because we only have data on entrants in the summer of 2012, who were among the top 500 new apps, which gives us a few hundred observations. Moreover, while the *privacygrade* is a solid outcome, permission use in 2016 may be confounded with the developers' efforts to build new features into their apps, which is likely to be also related to an app's initial success.

Figure C1: Development of Ratings during an App's Adolescence: Free Apps

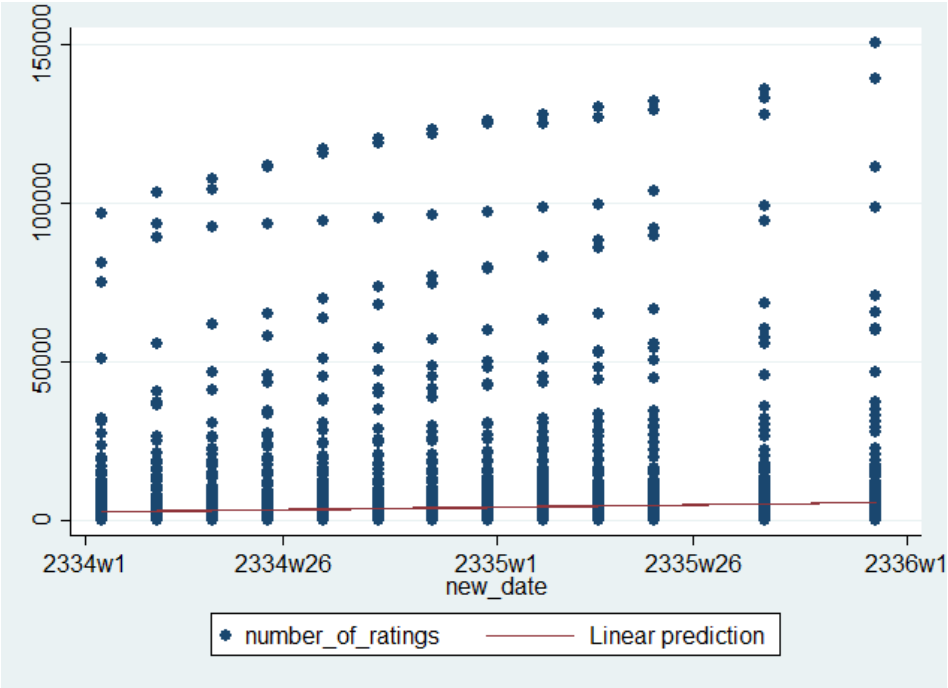


Figure C2: Development of Ratings during an App's Adolescence: Paid Apps

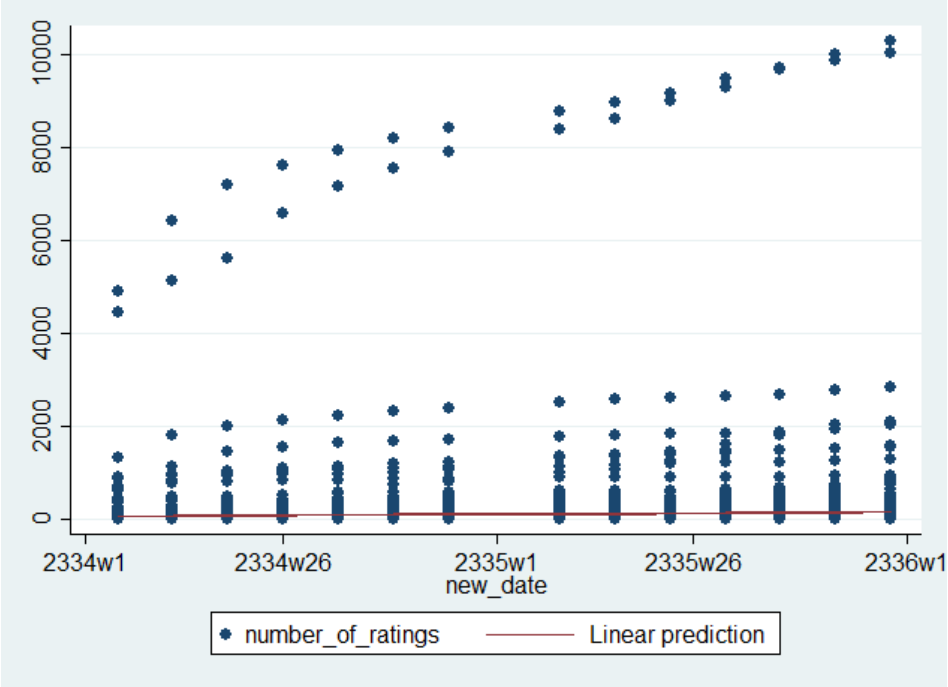


Table C1: App Adolescence and Future *privacygrade*/2016 Permissions

	failgrade		privacygrade		# permissions 2016	
	(1)	(2)	(3)	(4)	(5)	(6)
Average Rating	0.034	0.028	0.054	0.035	-0.447	-0.689
	(0.029)	(0.034)	(0.075)	(0.087)	(0.397)	(0.430)
# Ratings in 1000	-0.001	0.002	-0.001	0.002	-0.030	0.007
	(0.005)	(0.003)	(0.011)	(0.007)	(0.046)	(0.019)
Dummy: Video	0.090	0.101	0.297*	0.320**	0.415	1.135
	(0.064)	(0.065)	(0.152)	(0.156)	(0.668)	(0.744)
Dummy: Website	0.062	0.076	0.156	0.188	0.668	0.349
	(0.063)	(0.065)	(0.148)	(0.152)	(0.725)	(0.722)
Dummy: Privacy Policy	-0.050	-0.062	-0.080	-0.114	2.972***	2.486**
	(0.063)	(0.063)	(0.145)	(0.146)	(0.952)	(0.975)
Initial Growth: Ratings	0.000		0.000		0.000	
	(0.000)		(0.000)		(0.000)	
Initial Growth: Inst. Levels	-0.072**		-0.146		0.822**	
	(0.035)		(0.090)		(0.376)	
Initial Growth: # Instal.	-0.000		-0.000		0.000	
	(0.000)		(0.000)		(0.000)	
Early Growth Acceleration		0.149		0.342		4.642***
		(0.109)		(0.286)		(1.170)
Constant	0.096	-0.103	2.306***	1.886***	6.414***	4.253*
	(0.118)	(0.189)	(0.314)	(0.487)	(1.853)	(2.398)
Observations	274	265	274	265	372	310
Adjusted R^2	0.012	0.007	0.009	0.011	0.065	0.099

NOTES: The table analyzes the driving factors of developers' permission usage and the resulting *privacygrade* that was obtained in 2014. The regressions are panel fixed OLS regressions with a developer fixed effect. The dependent variable in columns 1&2 is a dummy indicating a 2014-failgrade (C or F) and, in columns 3 & 4, we use the grade that was obtained in 2014 (1=A+, 5=F). Col. 5 & 6 show the number of permissions used in 2016. Col. 1, 3 & 5 analyze app growth in the app's first months, and col. 2, 4 & 6 analyze growth acceleration (based on ratings). Robust standard errors in parentheses; * p<0.10, ** p<0.05, *** p<0.01