Privacy, Data and Competition: The Case of Apps For Young Children

Cecere, G.[*] Le Guel, F.[†] Lefrere, V.[‡] Tucker, C.[§] Yin, P.[¶]

April 3, 2022

Abstract

How does firm size affect privacy protections offered to customers? On the one hand, it could be that larger firms use their size to amass more data. On the other hand, smaller firms may be less careful in their data protection practices. We empirically analyze a special subset of apps where privacy concerns are very important - apps targeted at very young children. Our results suggest that larger firms offer more privacy protections to young children than smaller firms. Larger app developers request fewer pieces of sensitive data from consumers. This effect is stronger in countries with laxer standards of privacy protection. We also investigate whether a platform can help regulate privacy protection successfully, and we find that self-certification programs offered by platforms can help reduce data collection from children.

Keywords: data and competition, economics of privacy, apps for young children

JEL CODE: D82, D83, M31, M37

[*] Institut Mines-Telecom, Business School. Email: grazia.cecere@imt-bs.eu.

[†] University of Paris Saclay, RITM. Email: fabrice.le-guel@universite-paris-saclay.fr.

[‡] Institut Mines-Telecom, Business School. Email: vincent.lefrere@imt-bs.eu.

[§] Massachusetts Institute of Technology (MIT) - Management Science (MS). Email: cetucker@mit.edu.

[¶] Marshall School of Business, Greif Center for Entrepreneurial Studies, University of Southern California. Email: pailingy@marshall.usc.edu.

This paper previously circulated under the title "Privacy and Children: What Drives Digital Data Protection for Very Young Children?". We are grateful to Babur De Los Santos, Jose De Sousa, Philippe Gagnepain, Qinhou Li and Wilfried Sand-Zantman for helpful comments and suggestions. An earlier version of this paper was presented at IIOC Indiana 2018, AFSE Paris 2018, the Peex Lab Carnegie Mellon University, the ZEW ICT Conference 2018, the 11th Conference on Digital Economics Paris, 2019 INFORMS Marketing Science Conference, the Summer Institute Munich 2019, the Louvain Economics of Digitization 2020, Zurich Workshop & Lecture Series on the Law & Economics of Innovation 2021, APIOC 2021. The underlying work for this paper was supported by the CARNOT TSN and the DAPCODS/IOTics ANR project (ANR-16-CE25-0015). We are grateful to Clara Jean, Theo Marquis, Hugo Allouard, and Enxhi Leka for their research assistance. All errors are the sole responsibility of the authors.

1 Introduction

Many recent antitrust cases focus on allegations of larger firms collecting too much data. In 2019, the German regulator challenged Facebook, claiming that its size meant that consumers were obliged to provide personal data to gain access to its products. However, it is not clear from an economics point of view whether larger or smaller firms have more incentives to collect more privacy-intruding data. On the one hand, larger firms may collect more data on a given subject because they have the size and scale to use data better, and may offer better products that result in being able to request more data from consumers to service them. On the other hand, smaller firms may collect more data as a result of being less cautious about the negative risks of consumer-data collection, and believing that they need more data to compete. Since theoretical arguments could go both ways, this paper investigates the question of how firm size relates to data collection in a case where privacy protection undoubtedly matters: Data collection of sensitive information from very young children.

Children may not understand the potential negative outcomes of revealing personal information online, so regulation often requires parental consent to collect children's data (Livingstone *et al.*, 2019; Bleier *et al.*, 2020). There are evident reasons to want to safeguard the data of toddlers and preschoolers, and this is also a useful market to study because of the amount of discretion developers have in choosing what data to collect from their users. Apps which target very young children tend to be simple, and provide content based primarily on images and sound. They do not require large swathes of user data to operate better. In addition, the simplicity of these apps means this is a market where apps are low-cost to develop (Ghose and Han, 2014), and many developers from many countries compete in this market.

We collected weekly data on the apps published in the US market available in Google Play Store over the period July 2017 to January 2021. The Google Play Store has a self-certification program called "Designed for Families" (DFF) to help parents identify child-appropriate content. Developers who opt in to the program self-declare that the app complies with Google Play Store's internal DFF policy and the USA's Children's Online Privacy Protection Act (COPPA). We collected data on both apps that opted into DFF and those that did not. We identified apps by using search terms such as "preschool" and "toddler." Our dataset includes 27,785 apps and 11,343 developers located in 127 countries leading to 1,510,745 observations. COPPA protects the privacy of American children under 13 years of age and defines what is sensitive data in the case of children. We use the COPPA definition of sensitive data to determine whether an app requires sensitive data.

We examine the relationship between developer size and the pieces of sensitive data requested. The dynamic structure of our large panel data combined with the large set of controls and fixed effects included in our main models allow us to interpret how developer size affects the likelihood of collection of sensitive data. We address the identification challenge by exploiting variation in country privacy regulation and the availability of repeated observations of a time-invariant individual app fixed effect.

We find that child apps produced by larger developers are less likely to collect sensitive data: 41.4% of apps produced by small developers requested at least one type of sensitive data, compared to only 17.7% of the apps produced by larger developers. The results are robust to a broader definition of sensitive data and a fine-grained definition of developer location. We use several empirical strategies to demonstrate robustness of our results. We estimate different functional forms and run the main specification with a set of developer size measures and different sub-samples to estimate the effect of regulation regimes. We then evaluate whether these results are driven by developer privacy regime, or by underlying developer experience.

We also find evidence that the relative stringency of privacy protection for children in the US may have led developers in the US to be more reluctant to develop apps targeted at the children's market, leading to an opening for international developers to gain market share. Given that this is a market with many small developers from countries with laxer standards of child privacy protection than the US, we then investigate whether platform regulation and governance can help improve privacy protection. We find positive evidence that platform compliance programs improve child privacy protection, especially among developers from countries with laxer privacy regulations. We find that 25.83% of apps that self-select into the platform's self-certification program request at least one piece of sensitive data from their child users compared to 49.48% of apps which do not opt in.

Our work builds upon four streams of academic literature. The first stream of literature is on privacy regulation. Most of these articles have documented a tradeoff between protecting privacy and innovation, in sectors such as health (Miller and Tucker, 2009, 2011, 2017) and advertising (Goldfarb and Tucker, 2011, 2012; Montes *et al.*, 2019; Jia *et al.*, 2020; Johnson *et al.*, 2020). Several articles have documented distortions in terms of firm location (Rochelandet and Tai, 2016) and creating incentives for firms to collect more data (Adjerid *et al.*, 2015). By contrast, in this paper we focus on the question of what drives whether firms collect data from vulnerable individuals, and how this appears to be shaped by firm size, platform regulation, government regulation and the global app economy.

The second stream of literature is the app market. This literature has focused on app-developer strategies to gain attention, through distorting popularity information (Bresnahan *et al.*, 2014a,b), using free apps to build demand for paid apps (Deng *et al.*, 2022), overcoming search costs and navigation costs (Yin *et al.*, 2014; Ershov, 2021) and offering low price points in return for user data (Kummer and Schulte, 2019). This literature has also documented how app store policy affects app developer strategies, for example through its product rating system. Leyden (2021) shows that this policy change led to higher-quality products but less frequent product updates. Comino *et al.* (2019) show how developers' ability to post updates influences downloads. Bian *et al.* (2021) show consumers reduce the demand for apps that disclosure data collection practices after the platform's privacy policy change. There is a smaller literature which has attempted to characterize the market for child apps. Kesler *et al.* (2017) document that apps that target the 13+ and 16+ age categories are more intrusive than others. In addition, Liu *et al.* (2016) and Reyes *et al.* (2018) document that most apps do not comply with US child privacy regulation. Our paper builds on this literature by trying to uncover what shapes app developers' decisions to collect sensitive data from children.

The third stream of literature is that of the relationship between privacy protection and competition. Our results are important for competition economists and competition authorities, because to our knowledge this is one of the first papers that explicitly asks whether larger or smaller firms collect more personal or intrusive data. Our results also suggest there is a tradeoff between privacy regulation and competition - something that has been alluded to in theoretical work (Athey, 2015; Campbell *et al.*, 2015; Fuller, 2017; Tucker, 2019; de Cornière and Taylor, 2021) and empirical work (Marthews and Tucker, 2019; Jia *et al.*, 2021; Peukert *et al.*, 2022). Our results suggest that privacy protection designed to limit data collection will affect smaller firms more than larger firms.

The final stream of literature we contribute to is that which tries to understand the relationship between data and market power. Much of this economics literature has been devoted to the question of whether there are economies of scale and scope in data. Most of these papers have found evidence instead of decreasing returns to data (Chiou and Tucker, 2017; Bajari *et al.*, 2019; Claussen *et al.*, 2019; Farboodi *et al.*, 2019). By contrast, we ask whether firm size appears to influence the amount of sensitive data collected.

Our results are important for regulators because of the importance of protecting children's privacy, and because of some of the intricacies of global competition in the digital space. Children's privacy issues are particularly pressing, as 59% of the children interviewed use mobile devices to download apps.[1] Our results suggest that policies directed towards improving privacy need to be mindful that in a globally competitive market, it may be more advantageous to encourage platform governance of privacy, rather than focusing on national regulations which may be limited in their global reach.

The paper is structured as follows. Section 2 describes the data sources and presents the descriptive statistics. Section 3 presents our empirical strategy and our variables of interest. Section 4 shows the econometric results based on different specifications and provides robustness checks. The conclusion follows.

2 Data

We use data from the Google Play Store. This is the largest worldwide platform that distributes apps for the Android ecosystem. We study children's apps published in the US Google Play Store that have been released worldwide. Apps in the Google Play Store are automatically released worldwide with automated translation of app descriptions unless the developer specifies otherwise.[2] We collect weekly data on the full relevant market of chil-

[1] Mobile Kids Report published by Nielsen (2017). Last accessed, January 8, 2018.

[2] Certain countries may impose additional requirements on developers to comply with local regulations.

dren's apps over a three-year period. We follow each app from mid-July 2017 to January 2021, tracking each app starting from its first appearance to the end of the sample period.[3] Our final sample includes 106 weeks as we keep only weeks which contain the full sample of data. We collect data on average every two weeks. The final sample includes 1,510,745 observations with 27,785 apps and 11,343 developers. This large number of apps reflects the fact it is easy to produce and commercialize apps worldwide for children and especially those under five, since these apps are mainly based on images, sounds, and colors. This is something that has been estimated by Ghose and Han (2014) as part of a broader demand estimation exercise.

An important regulatory enforcement tool in the context of privacy legislation is industry self-certification, which can affect an industry's competitive structure (Brill, 2011; Acquisti *et al.*, 2016). We look at the DFF program. Developers choose whether the app should be included in this category or not and no additional monetary costs are associated with opting into the program. Developers who produce children's apps can therefore decide to opt in to the DFF, or they can post their apps in the Google Play Store without it. Developers who opt in to the DFF declare compliance with COPPA, along with other requirements specified by Google Play Store. Figure 3 in Appendix B shows that consent is based on a checkbox indicating agreement for inclusion in the DFF. Apps included in the program are easier for parents to find.[4] Our data collection strategy allows us to collect apps inside the DFF and apps that do not belong to this program using keyword searches aimed at children to capture all children's apps published in the US Google Play Store.[5]

First, we collect the characteristics of apps in the DFF aimed at children aged under 13. It represents 70.59% of our sample.[6] The DFF program includes three broad age categories aimed at children ages 0-5, 6-8 and 9+, with an additional six categories: Action & Adventure, Brain Games, Creativity, Education, Music & Video, and Pretend Play. While the choice of

[3] Publicly available data was collected every week via webscraping using the Python programming language. Apps collect with keywords can overlap with apps inside the DFF. In this case, we consider them as part of the DFF.

[4] Figure 2 in the Appendix B shows a screenshot of DFF.

[5] We collect all apps from the search results lists with the maximum scroll-down possible in each page up to the limits of the Google Play Store. In the DFF program, there are 540 apps available in each page and in keyword searches, there are 250 apps available.

[6] An observation is at app and week level.

thematic category is optional, developers must choose appropriate age categories.

Second, we construct a benchmark group of apps aimed at children using keyword searches. We identify the list of keywords most frequently associated with children's apps using the Google Adwords keyword planning tool. Table 1 presents the list of these keywords. Google's keyword search algorithm analyzes the app description given by the developer. Google Play search allows users to find relevant and popular apps in the Google Play Store. Algorithmic search is based on title, app description, app icons, images, and screenshots.[7] The search was repeated weekly to identify new benchmark apps. The benchmark group represents 29.41% of the sample.

Apps identified at least once by keyword search in the Google Play Store during the study period are included to our list of apps. This allows us to include broad apps that appeal to children. This aligns with recent COPPA cases, as the FTC declares that general-audience content should comply with COPPA rules if they can potentially appeal to children. Thus, general-audience content are required to comply with COPPA even if it is only particular parts of their websites or apps (including content uploaded by third parties) that are directed at children under age 13.

Table 2 presents descriptive statistics. We collect all publicly available data over time such as type of sensitive data required by apps, number of apps produced by developers, developer addresses, and app characteristics. The Google Play Store provides 21 ranges of downloads for each app from 0 to 5 installs to more than 5 billion installs. We include a set of dummies representing each range (see Table 13 in the Appendix D).

We have an unbalanced panel which allows for entry and exit. New apps appear over time while others become unavailable.

[7] App description is the result of developers' strategic behavior. `https://support.google.com/googleplay/android-developer/answer/4448378?hl=en`. Last accessed, November 24, 2020.

Table 1: **Designed for Family and List of Keywords Used in the Data Collection**

Data Collection Strategy			
DFF Categories	Ages 5 & Under		
	Ages 6-8		
	Ages 9 & Up		
	Action & Adventure		
	Brain Games		
	Creativity		
	Education		
	Music & Video		
	Pretend Play		
List of Keywords	2 year old	child	preschoolers
	3 year old	children	monitoring
	4 year old	kids	toddler
	5 year old	boy	toddlers
	6 year old	girl	children’s
	7 year old	baby	educational
	8 year old	babies	
	9 year old	kindergarten	
	10 year old	kindergartners	
	11 year old	preschool	
	12 year old	kid monitoring	

Notes: The first part of the table presents the list of DFF categories used to collect apps that belong to the program. To each age app category developers can associate any of the categories proposed by the DFF: Action & Adventure, Brain Games, Creativity, Education, Music & Video, and Pretend Play. The second part of the table presents the list of keywords used in the data collection. We use the Google AdWords keyword planning tool which provides keywords most frequently associated with children’s apps.

Table 2: **Panel Data Summary Statistics**

	Mean	SD	Min	Max
Dependent Variables				
Sensitive Data	0.586	1.120	0	11
Sharing	0.081	0.316	0	3
Location Data	0.188	0.551	0	4
Identity Information	0.275	0.510	0	2
User Surveillance	0.042	0.282	0	5
Prob Sensitive Data	0.328	-	0	1
Measures of Size				
Nb of Apps by Developer	18.03	33.700	1	248
1 App	0.284	-	0	1
2-4 Apps	0.219	-	0	1
5-18 Apps	0.250	-	0	1
19-45 Apps	0.148	-	0	1
46+ Apps	0.099	-	0	1
New App	0.291	-	0	1
Nb of New Apps by Developer	3.699	9.277	0	113
0 New App	0.489	-	0	1
1-3 New Apps	0.292	-	0	1
4-10 New Apps	0.123	-	0	1
11+ New Apps	0.096	-	0	1
New Single App Developer	0.094	-	0	1
Large # Installs	0.079	-	0	1
Self-Certification				
DFF	0.706	-	0	1
Privacy Regulation Regime				
OECD	0.559	-	0	1
US	0.249	-	0	1
EU	0.302	-	0	1
Recognized by the EU	0.318	-	0	1
With Legislation	0.234	-	0	1
Independent Authority	0.094	-	0	1
No Privacy Law	0.052	-	0	1
Advertising				
Contains Ad	0.534	-	0	1
# Distinct Apps		27,785		
# Distinct Developers		11,343		
Observations		1,510,745		

Notes: This table presents descriptive statistics for the overall sample.

3 Empirical Analysis

3.1 Model Specification

We investigate the tradeoffs between promoting competition and protecting children's privacy. Strong privacy protections can protect children, but may adversely affect smaller developers. We investigate how digital platforms help to enforce legislation requirements. This might differently affect national and foreign developers. This in turn makes the empirical effect of privacy rules ambiguous.

We formalize the key considerations of an app deciding whether or not to request sensitive data. The decision to request sensitive data given the app quality can be correlated with developer size; this is a proxy for developer ability to extract value from data and the ability to internalize compliance costs. Apps commercialized in the US are produced by US and non-US developers. Each developer faces a binary choice and will decide to enter or not into the DFF. We use variation in privacy regulation worldwide to estimate the effect of different kinds of privacy laws on the types of sensitive data collected. Our empirical work aims to:

1. measure the effect of developer size in collecting sensitive data,
2. measure the effect of platform policy on protecting children's privacy,
3. test whether the developer size effect varies within developer's country regulation regime.

Building on our conceptual framework, we model how developer size and self-certification policy are likely to influence the types of sensitive data requested. Our dependent variable, *Sensitive Data*, measures the pieces of sensitive data requested by each app i (i= 1 to N = 27,785) in week t (t= 1 to T=106). We use our panel data to estimate an OLS model with individual app fixed effects and time fixed effects and standard errors clustered on the app level.

We model the intensity of data collection using the following specification:

$$\textbf{Sensitive Data}_{\textbf{it}} = \alpha_0 + S_{it}\beta + D_{it}\omega + \theta_{it} + \zeta_i + \rho_t + \epsilon_{it} \tag{1}$$

Our primary variable of interest is S which indicates developer size of app i at time t. D indicates whether the app i belongs to the DFF program at week t. θ is a vector of other time-varying app characteristics, ζ is the vector of app i fixed effects. Adding the app fixed effects ensures that identification of the coefficient is based on within-app variation over time rather than cross-app variation. The equation also includes time (week) effects ρ_t which capture market trends related to privacy over time in our sample. ϵ_{it} is the error term.

3.2 Dependent Variable: Sensitive Data

COPPA regulation defines the list of child-sensitive data collection covered by the law. It includes geolocation details (sufficiently precise to identify street name and city), photos, videos, and audio files that contain children's images or voices, usernames, and persistent identifiers to recognize an app user over time and across different apps.[8] User data can be requested and collected using the permissions system implemented by the Google Play Store. To measure whether children's apps possibly violate COPPA, we identify the Google Play Store permissions and interactive elements (see Appendix A for details) that allow apps to collect these sensitive data on children.

We identify eleven permissions and three interactive elements that require personal data covered by the COPPA regulation. We created the variable *Sensitive Data* which counts the types of sensitive data covered. We identify four broad categories of sensitive data: *Sharing*, *Location Data*, *Identity Information* and *User Surveillance* (see Table 9 in Appendix A to check the permissions and interactive elements required to construct the main dependent variable *Sensitive Data*).

Table 2 presents the descriptive statistics of the main dependent variable. The average number of pieces of sensitive data required by an app is 0.586. We also construct a dummy variable *Prob Sensitive Data* measuring whether the app requests at least one piece

[8] The law requires verifiable parental consent for the collection, use, and disclosure of personal information on children aged under 13. This information is not available to the researchers: only developers and users who actually use the app have access to this information. Thus, we are only able to measure the type of permissions required by each app. The complete list of children's personal data is available in FTC rulemaking regulatory reform proceedings (`https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule`). Last accessed, January 8, 2018.

of sensitive data; 32.8% of apps belong to this category.

3.3 Developer Size

Conceptually, developer size could affect the likelihood of sensitive data collection through channels, through compliance costs, and through shaping underlying demand for sensitive data. In terms of compliance costs, on the one hand, larger developers may find it easier to internalize compliance costs and therefore may have lower marginal costs of collecting more sensitive data. The fixed cost of compliance may be substantial. In 2013 (when COPPA was lastly revised), the estimated average cost of compliance according to TechFreedom (working on behalf of the FTC) was around $6,200 per year but up to $18,670 a year for newly created companies.[9] On the other hand, smaller developers may be more likely to take a less risk-averse approach, a non-robust approach to compliance, and consequently have lower compliance costs for collecting more sensitive data. There is substantial legal risk from collecting sensitive data. Recent FTC and state cases show that the FTC imposes high settlements on firms that do not comply with the COPPA as shown in Table 10 Appendix C.1.

In terms of underlying demand, larger developers may find it desirable to collect more data because their scale of operations and data-sophistication means they can extract the most value from it. Smaller developers may find it desirable to collect more data because ultimately the incremental value of data is larger for smaller firms, given that data is often duplicative.

We use several metrics to measure developer size.

3.3.1 Number of Apps by Developer

We capture developer size by counting the number of apps available for each developer each week: *Nb of Apps by Developer*. The average developer size is 18.03 apps. The marginal effect of producing one more app may impact small and larger developers differently. To account for this effect, we split the continuous variable *Nb of Apps by Developer* into five categories ranging from 1 app to over 46 apps using the 25th, 50th, 75th and 90th percentile distribution

[9] These figures do not include additional costs and reduced revenue from ads. `https://www.lexology.com/library/detail.aspx?g=0b6d68a9-5d17-4d52-9b30-54d356ddb08a`. Last accessed, May 31, 2020.

in order to highlight any threshold effects. *1 App* indicates that at time t developer has only one app, *2-4 Apps* indicates that developer has between 2 and 4 apps, *5-18 Apps* indicates that developer has between 5 and 18 apps, *19-45 Apps* indicates that developer has between 19 and 45 apps and *46+ Apps* indicates that developer has more than 46 apps (top decile). Table 3 presents the average number of types of sensitive data collected by developer size. We find that 41.4% of apps produced by small developers request at least one type of sensitive data, but that percentage drops to 17.7% for larger developers. In all rows, the amount of sensitive data collected declines as the developer size increases.

Table 3: **Sensitive Data Collected by Developer Size**

	1 App (1)	2-4 Apps (2)	5-18 Apps (3)	19-45 Apps (4)	46+ Apps (5)
Sensitive Data	0.872	0.663	0.447	0.388	0.251
Sharing	0.142	0.095	0.054	0.030	0.019
Location Data	0.312	0.224	0.119	0.108	0.050
Identity Information	0.328	0.289	0.260	0.241	0.178
User Surveillance	0.089	0.056	0.014	0.008	0.004
Prob Sensitive data	0.414	0.346	0.302	0.280	0.177
# Distinct Apps	11,096	9,354	9,413	5,541	2,980
# Distinct Developers	10,557	3,193	922	170	34
Observations	428,240	330,317	378,257	223,806	150,125

Notes: Average pieces of sensitive data collected by developer size.

3.3.2 Alternative Measures of Developer Size

The literature on big data suggests that data performance does not depend linearly on the amount of data collected (Tucker, 2019). We want to investigate whether developers with a large number of installs experience increasing returns to data collection. In this section, we use several metrics to capture alternative measures of developer size, based on the number of consumers (downloads) and new products (new apps). The number of downloads is another important measure of developer size which is also considered by competition authorities in the recent cases.[10] We construct the binary variable *Large # Installs* which takes value 1 if the developer has at least one app with more than 5 million downloads. This market is

[10] `https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf` Last accessed, June 5, 2019.

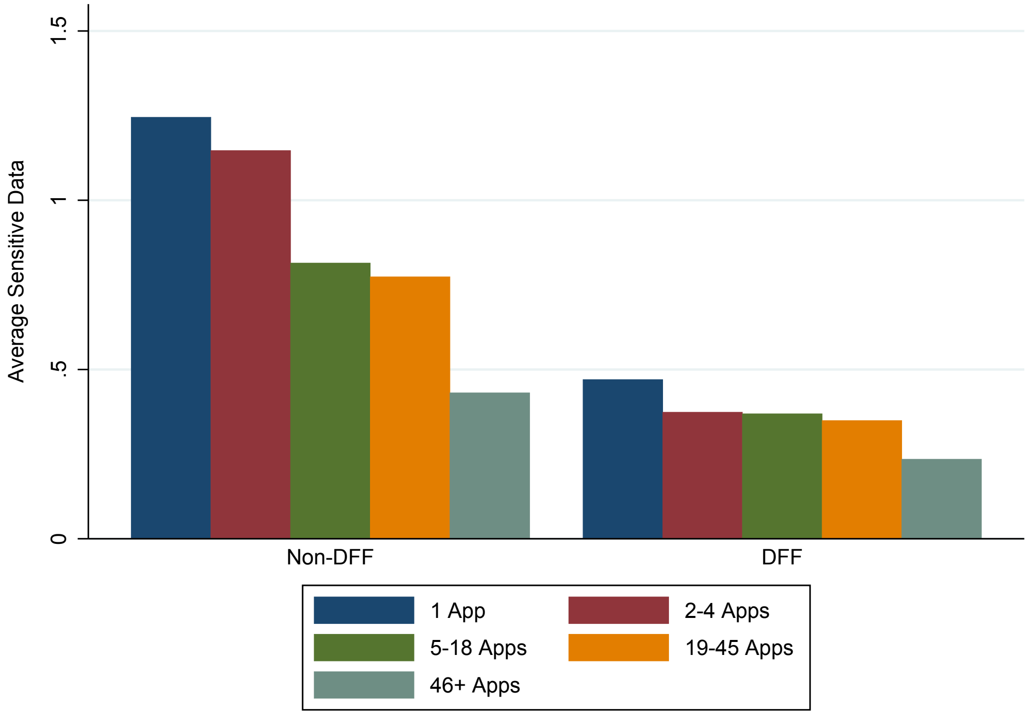
characterized by a high degree of skew in the size distribution of app demand (Bresnahan *et al.*, 2014a). In addition to our main explanatory variable for developer size, we also measure the newly created apps for each developer. The variable *Nb of New Apps by Developer* accounts for new apps introduced in the market after September 2017 by a given developer. In our sample, there are 11,974 new apps which represents 43.1% of apps. This allows us to capture recently produced apps that might did not appear immediately in the Google Play Store at the beginning of our data collection. We split this variable into four categories reflecting percentile distributions ranging from zero to more than 11 new apps, using the 50th, 75th and 90th percentiles of the distribution of size measure. *0 New App* indicates that at time t developer has no new app created after September 2017. *1-3 New Apps* indicates that developer has between 1 and 3 new apps. *4-10 New Apps* indicates that developer has between 4 and 10 new apps. *11+ New Apps* that developer has more than 11 new apps (top decile). The variable *New App* is a binary variable indicating whether an app is introduced in the market after September 2017.

3.4 Self-certification Regime: DFF

A developer's decision to self-certify through the DFF is a strategic choice about customers and competitors (Ershov, 2020). Developers that include apps in the DFF self-declare that their apps comply with the COPPA rules and content is rated "Everyone" or "Everyone 10+" (or equivalent) according to the Entertainment Software Rating Board (ESRB) definition. We use the variable *DFF* to identify whether the app belongs to the DFF.

Figure 1 shows that overall, apps that opt in in the DFF are less likely to request sensitive data compared to apps outside the DFF. Regardless of certification, larger developers request less sensitive data than smaller developers. It suggests that DFF likely complements the stringency of US legislation. What is striking is the strong decrease in data collection related to increase in developer size for apps outside of DFF. Apps in DFF more consistently collect less sensitive data across all sizes of developers.

Figure 1: **Sensitive Data by Developer Size and DFF Self-Certification**



Notes: The y-axis indicates the average number of sensitive data collected.

3.5 Developer's Country and National Privacy Regime

We study children's apps published in the US Google Play Store, but which have been developed worldwide. In our dataset, developers originate from 127 countries. We exploit geographical information disclosed by each developer to identify developer's country. Overall, a plurality of the apps in the US market are produced by US developers (31.7% of the sample). After the US, the largest producers of children's apps are India (with 8.15%), and the United Kingdom (6.29%) (Table 12 Appendix C).

Privacy regulation rules vary across countries, and we exploit this variation to characterize national privacy policies. A developer's privacy strategy might be associated with the home institutional framework. To assess differences in national regulatory frameworks, we augment our data with a vector of the institutional framework measures associated with the developer's address. In the context of privacy regulation, in 1980 the OECD was one of the first international organizations to provide privacy guidelines which were reformed in 2013 (OECD, 2013). Thus, it is reasonable to believe that developers in the OECD have longstanding traditions related to privacy issues. To capture this effect, we create the binary variable *OECD* which identifies developers located in OECD countries.

Table 4 presents detailed descriptive evidence on the rate of growth of new app numbers and data collection intensity by country groups based on production in an OECD country or a non-OECD country.

Columns (1) and (2) respectively present the number of apps and the percentage of apps in each country group. Column (3) presents the number of new apps. Column (4) indicates the rate of growth of new app creation since September 2017. One important descriptive trend that we observe is that the new apps targeted at children are produced largely in non-OECD countries, with a growth rate of 106.61%.[11] The lowest rates of growth of new apps is in the OECD and EU member countries despite a smaller app baseline compared to non-OECD countries. This reflects a potential dampening effect of regulation on the development of apps for children. The stringency of the privacy protection applying to children may have increased the reluctance of local developers in the US to develop apps targeted at the child market, and reduced the relative market shares of domestic to international firms. Column (5) shows the average number of apps that collect at least one piece of sensitive data by country group. Column (6) indicates the average number of apps produced by larger developers requesting at least one piece of sensitive data. On average, 23% of apps produced by larger developers in the Non-OECD country group request at least one piece of sensitive data. Column (7) indicates the average number of new apps produced by larger developers requesting at least one piece of sensitive data.

[11] Apps growth rate = $[(T1 - T0)/T0] * 100$ where $T0$ is the total number of apps present in the sample in September 2017 and $T1$ is the total number of apps including those newly created during the four years observation period.

Table 4: **Apps Growth Rates and Privacy Regime**

	# Apps	% Apps	# New Apps	% Growth New Apps	Prob Sensitive Data	Prob Sensitive Data 46+ Apps	Prob Sensitive Data 11+ New Apps
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
US	6,444	23.19	2,361	57.83	0.34	0.07	0.13
OECD	14,461	52.05	5,099	54.46	0.32	0.13	0.10
EU	7,940	28.58	2,773	53.67	0.29	0.14	0.15
Non-OECD	13,324	47.95	6,875	106.61	0.34	0.23	0.23

Notes: Column (1) indicates the total number of apps in each group of countries. Column (2) shows the overall percentage of apps. Column (3) shows the number of new apps created since September 2017. Column (4) illustrates growth rates of the number of apps created after September 2017. Column (5) shows the percentage of apps requesting at least one piece of sensitive data. Column (6) indicates the percentage of apps produced by larger developers requesting at least one piece of sensitive data. Column (7) indicates the percentage of apps produced by larger developers of new apps requesting at least one piece of sensitive data. Appendix C Table 12 shows growth rates by the top country.

4 Results from Panel Data: Sensitive Data Collection from Children

4.1 Developer Size and DFF

Table 5 presents our initial results when we examine how data collection is affected by developer size as well as the effects of self-certification program offered by the platform.

We first examine each key variable separately, namely developer size and the decision to opt in to the self-certification program, before estimating our main model. Table 5 incrementally builds up to the final specification, Equation (1), in column (3). In each case, the specification includes the variable *Contains Ad* to reflect the app's business model and a vector of dummy variables measuring download intensity. We also include app fixed effects to account for cross-app heterogeneity and week fixed effects for the week the data was scraped.

Column (1) investigates the effect of developer size as measured by the number of apps produced by each developer over time. This measure allows us to determine whether the behaviors of large professional developers and small developers differ. Larger developers (*46+ Apps*) are less likely to collect sensitive data compared to small developers. This result is negative and significant across all specifications. The estimate for the variable *46+ Apps* implies an average decrease of 0.085 in the number of types of sensitive data collected. This corresponds to a 6.82% reduction,[12] considering as baseline a small developer with one

[12] This corresponds to 0.085/1.245, where 1.245 is the average data collection by small developers with 1 app that do not belong to the DFF.

app not in the DFF. There are many potential explanations for this finding. One is the theoretical findings in Campbell *et al.* (2015) that privacy regulation imposes costs on all firms, but larger firms are more likely to internalize these costs. For example, larger firms can benefit from economics of scale on the fixed compliance costs. In this case, regulation might distort competition against small companies. Another possibility is that companies may benefit from having large quantities of data but with diminishing return to scale (Bajari *et al.*, 2019). Another concern is that larger developers might collect less sensitive data on single user account than a one-app developer as larger developers can collect different pieces of sensitive data for each single apps. To address this, Figure 4 in Appendix F shows the average types of pieces of sensitive data requested by each developer. While smaller developers request different types of sensitive data, larger developers request on average the same pieces of sensitive data than incremental data.

Column (2) shows that apps that opt in to the Google self-certification program (DFF) are less likely to collect child data. If this reflects the ability of platform self-certification initiatives to influence developer behavior, then this program can help with adherence to local (US) laws. While apps in DFF are not subject to strong enforcement, the platform reminds developers of COPPA legislation requirements (see Figure 3 in the Appendix B). In the app market, there is fierce competition across all app categories for consumer attention (Bresnahan *et al.*, 2014a). The increased visibility in the market for children's apps conferred by DFF certification might compensate for these developers' regulatory compliance costs.

Column (3) of Table 5 reports the main estimates in which we study the effects of developer size and DFF in a single model. This result highlights that both self-certification and developer size reduce sensitive data collection. This finding is important from a privacy policy perspective, showing that self-certification is not the only instrument to reduce data collection and might not be sufficient on its own.

When we look at the coefficient of the vector of downloads reported in Table 14 Appendix D, the estimates are reasonably consistent. Apps with less than 500 thousand downloads are more likely to collect sensitive data. We check the validity of these results in multiple ways. These estimates are presented in Appendix E. Table 15 reports data collection by advertising business model. Table 16 shows robustness of our results to different functional forms. Table 17 shows robustness of our results when we consider alternative dependent variables.

Table 5: **OLS Estimates: Drivers of Requests for Sensitive Data**

Sensitive Data as Dependent Variable	Developer Size (1)	DFF (2)	Main Specification (3)
2-4 Apps	-0.003		-0.001
	(0.010)		(0.010)
5-18 Apps	-0.001		0.003
	(0.014)		(0.013)
19-45 Apps	-0.021		-0.016
	(0.016)		(0.016)
46+ Apps	-0.085***		-0.078***
	(0.025)		(0.025)
DFF		-0.050***	-0.050***
		(0.007)	(0.007)
Constant	0.566***	0.597***	0.605***
	(0.014)	(0.013)	(0.015)
Downloads	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes
Week FE	Yes	Yes	Yes
App FE	Yes	Yes	Yes
Observations	1,510,745	1,510,745	1,510,745
Number of groups	27,785	27,785	27,785
Adjusted R2	0.942	0.942	0.942

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. The omitted size category is a developer with one app. Robust standard errors are clustered at app level and reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

4.1.1 Alternative Measures of Developer Size

We also assess the robustness of our results to three alternative measures of developer size. Table 6 reports the main estimates. This robustness check is independently interesting because it shows that apps produced by larger developers are less likely to collect sensitive data. Overall, the results are consistent with the main estimates in Table 5.

Column (1) includes the continuous measure of developer size. We corroborate previous results regarding the effect of developer size. This suggests that non-linearity of developer size is not driving our results. To address concern on the heterogeneity of developer size in data collection, column (2) includes the variable *84+ Apps* to measure the size of very large developers. Very large developers with more than 84 apps are likely to collect less sensitive data. This corresponds to an 11.16% reduction, considering as the baseline a small developer with one App not being in the DFF.

Column (3) and column (4) of Table 6 include the binary variable *Large # Installs* to investigate whether developers who have access to a large number of users are less likely to collect sensitive data. The coefficient of the variable *Large # Installs* is negative and statistically significant suggesting that developers with at least one app with a large number of users are less likely to collect sensitive data. This pattern suggests decreasing returns to data, as previously shown in the literature by Chiou and Tucker (2017); Bajari *et al.* (2019); Claussen *et al.* (2019); Farboodi *et al.* (2019). This result challenges the recent approach of different competition authorities of targeting larger firms.

To address concerns that the reduction in sensitive data collection is merely driven by older developers who no longer produce new apps, column (4) and column (5) consider as a measure of developer size the newly created apps over the period of the time we study. The omitted category is the variable *0 New App*. The coefficient of the variable *11+ New Apps* is negative and statistically significant, suggesting that even recently active larger developers in our sample are less likely to collect sensitive data.

Overall, our results are robust to these alternative measures of developer size. The pattern that larger developers are less likely to request sensitive data is replicated across these estimates.

Table 6: **Alternative Measures of Developer Size**

Sensitive Data as Dependent Variable	Continuous Developer Size	Very Large Developer Size	Large Installs		New Apps
	(1)	(2)	(3)	(4)	(5)
Nb of Apps by Developer	-0.001***				
	(0.000)				
2-4 Apps		-0.002	-0.001		
		(0.010)	(0.010)		
5-18 Apps		0.002	0.003		
		(0.013)	(0.013)		
19-45 Apps		-0.017	-0.016		
		(0.016)	(0.016)		
46+ Apps			-0.078***		
			(0.025)		
46-83 Apps		-0.076***			
		(0.024)			
84+ Apps		-0.139***			
		(0.038)			
1-3 New Apps				-0.002	-0.001
				(0.006)	(0.006)
4-10 New Apps				-0.009	-0.007
				(0.008)	(0.009)
11 + New Apps				-0.091***	-0.088***
				(0.013)	(0.013)
Large # installs			-0.060***	-0.051**	
			(0.020)	(0.020)	
DFF	-0.048***	-0.048***	-0.050***	-0.050***	-0.049***
	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)
Constant	0.615***	0.608***	0.630***	0.633***	0.603***
	(0.014)	(0.015)	(0.012)	(0.008)	(0.013)
Downloads	Yes	Yes	No	No	Yes
Contains Ad	Yes	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes	Yes
Observations	1,510,745	1,510,745	1,510,745	1,510,745	1,510,745
Number of groups	27,785	27,785	27,785	27,785	27,785
Adjusted R2	0.942	0.942	0.942	0.942	0.942

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. The omitted size category is a developer with one app in column (2) and (3). The omitted category in the estimates reported in column (4) and (5) is developers producing any new apps after September 2017. Robust standard errors are clustered at app level and reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

4.2 Privacy Regulation Regimes

National privacy regime variation across countries is extensive and leads to a wide range of country heterogeneity. We use variation in privacy legislation across countries to estimate the developer size effect within different level of privacy laws. To explore this effect, we split the sample into groups of countries according to stringency of privacy regulation regime.

To account for the heterogeneity of countries in term of privacy regulation, we use the international measure of national privacy regime constructed by the French Privacy Regulation Authority (CNIL).[13] They categorize countries according to their level of compliance with EU privacy legislation (comparable to the US COPPA legislation). Table 11 in the Appendix C presents countries categorized according to their level of compliance with EU privacy legislation. The dummy variable *EU* identifies the developer country as part of the European Economic Area (EEA). The dummy variable *Recognized by the EU* indicates that the country's privacy laws are compatible with EU legislation and thus equally stringent as COPPA. The binary variable *With Legislation* indicates that the country has some level of privacy legislation. The binary variable *Independent Authority* indicates the existence of an independent authority regulating privacy. The dummy variable *No Privacy Law* indicates absence of privacy laws in the developer's country.

The baseline specification for different sub-samples are reported in Table 7. We use the continuous measures of developer size to have consistent estimates for each sub-group of countries. To facilitate the interpretation of the estimates, we report the mean value of the dependent variable *Sensitive data*. Column (1) explores what happens when we restrict our sample to apps produced in the OECD. The larger developers are less likely to collect sensitive data. Apps that opt in the DFF are likely to reduce data requests. The results in column (2) show the regression on the subsample of apps produced in non-OECD member countries. Developer size is negatively and significantly related to sensitive data collection and being in the DFF tends to decrease the pieces of sensitive data collected.

Column (3) displays the results of the sub-sample of apps produced by US developers. Apps commercialized by developers in the US that opt in to DFF are less likely to request sensitive data. The coefficient associated with *DFF* is substantially larger for apps produced in the US compared to other estimates. This provides suggestive evidence that self-certification is more efficient when driven by home regulation.

[13] CNIL, "La protection des données dans le monde". `https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde`. Last accessed, January 8, 2018.

Column (4) explores what happens when we restrict our sample to apps produced in EU which has a children's privacy protection regime comparable to COPPA. While developer size is not significantly related to sensitive data collection, the estimate shows that only the self-certification regime is likely to affect the pieces of sensitive data requested by European developers.

In the sub-sample of apps produced in countries with a privacy legislation recognized by the EU (Column (5)), we see similar estimates as in column (3). Column (6) shows the estimates on a sub-sample of apps produced in countries with an independent privacy authority. We show that the main effects of developer size on sensitive data collection are larger when we focus on countries with laxer privacy regimes.

Columns (7) and (8) show respectively that the apps produced by larger developers in countries with privacy legislation (*With Legislation*) and without any privacy legislation (*No privacy regime*) are less likely to collect sensitive data. The coefficient associated with *Nb of Apps by Developer* is larger for apps produced in countries with laxer privacy legislation compared to other estimates. The estimates show that apps in DFF are less likely to request sensitive data. This suggests that conditional on already having a strong privacy regulatory regime relating to children's data (US and country with legislation recognized by the EU), consumer protections may be more effectively improved by influencing digital platform global policies towards children rather than changing the regulatory regime within a single country.

Table 7: **Intensity of Data Collection and Privacy Regimes**

Sensitive Data as	OECD vs. Non-OECD		US	Privacy Regime				
Dependent Variable	OECD (1)	Non-OECD (2)	US (3)	EU (4)	Rec. EU (5)	Ind. Aut (6)	With leg (7)	No Privacy (8)
Nb of Apps by Developer	-0.001***	-0.002***	-0.001**	-0.000	-0.001***	-0.003**	-0.003***	-0.004***
	(0.000)	(0.000)	(0.000)	(0.001)	(0.000)	(0.001)	(0.001)	(0.001)
DFF	-0.048***	-0.050***	-0.093***	-0.023**	-0.076***	0.008	-0.066***	-0.059**
	(0.009)	(0.010)	(0.017)	(0.010)	(0.014)	(0.017)	(0.016)	(0.026)
Constant	0.573***	0.633***	0.699***	0.481***	0.642***	0.718***	0.614***	0.805***
	(0.017)	(0.022)	(0.028)	(0.026)	(0.023)	(0.046)	(0.028)	(0.056)
Downloads	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dep. var. mean	0.578	0.597	0.685	0.508	0.647	0.638	0.558	0.706
Observations	844,467	666,278	376,697	456,275	480,159	142,378	353,547	78,386
Number of groups	14,461	13,324	6,444	7,940	8,190	2,573	7,048	2,034
Adjusted R2	0.954	0.926	0.962	0.942	0.959	0.921	0.920	0.942

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. Column (1) shows the estimates within the sub-sample of apps produced in OECD member countries. Column (2) shows the estimates within the sub-sample of apps produced in non-OECD member countries. Column (3) reports the estimates of the sub-sample of apps produced in the US. Column (4) reports the estimates of the sub-sample of apps produced in the EU. Column (5) reports the estimates of the sub-sample of apps produced in countries with a privacy regulation regime recognized by EU. Column (6) shows the estimates within the sub-sample of apps produced in countries with an independent privacy authority. Column (7) shows the estimates of apps produced in countries with a privacy legislation. Column (8) shows the estimates of apps produced in countries with no privacy legislation. Robust standard errors are clustered at app level and reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

4.3 Privacy Protection: New Apps and New Entrants

Privacy protection is designed to protect consumers. This can impact the dynamics of market entry, adversely affecting new entrants and raising concerns about competition, but it can also encourage the creation of privacy-oriented apps. To address these issues, we investigate data collection by new apps introduced into the market and whether new developers are more likely to collect sensitive data. We introduce the binary variable *New Single App Developer* which measures new single app developer that enters in the market after September 2017. This variable measures the effect of the first app created by a new developer. Column (1) of Table 8 reports the estimates when we investigate whether new apps produced by larger developers are less likely to collect sensitive data. These sets of interaction terms capture the incremental effect of producing a new app for each group of developer size. The results suggest that new apps produced by medium and larger developers are less likely to collect sensitive data compared to smaller developers. Column (2) presents the estimates of the interaction terms *New App* × *DFF*. We find a negative and statistically significant effect. This result underlines that the new apps commercialized in the DFF are less likely to collect sensitive data. Our results might be driven by a new developer complying with children data regulation. To address this concerns, Column (3) includes in the estimate the variable *New Single App Developer* which is positive and significant. This shows that new smaller developers are more likely to collect sensitive data. The interaction term *New Single App Developer* × *DFF* is not significant. New smaller developers entering the market collect more sensitive data, while new apps produced by larger developers are less intrusive. This suggests that new apps are less intrusive only if they are produced by larger developers.

We also checked whether our results are driven by developer experience (in Appendix E.4.1, Table 18). We find suggestive evidence that the size effects we measure is driven partially by developers that enter the market after the creation of the DFF. Apps included in the DFF created after the beginning of this program are less likely to collect sensitive data. Finally, we investigate developer experience and the intensity of the privacy regime. Table 19 and 20 in Appendix E.4.2 present the estimates. The results provide suggestive evidences that apps produced by developers from laxer privacy legislation regimes that enter the market before the creation of DFF are likely to continue to collect data. This suggests that privacy legislation is needed to legislate earlier rather than later.

Table 8: **New Apps and New Developer Entry**

Sensitive data as	New App		New Single Developer	
Dependent Variable	Size	DFF	New	DFF
	(1)	(2)	(3)	(4)
2-4 Apps	0.009			
	(0.013)			
5-18 Apps	0.021			
	(0.017)			
19-45 Apps	0.011			
	(0.021)			
46+ Apps	-0.050*			
	(0.030)			
2-4 Apps × New App	-0.035*			
	(0.018)			
5-18 Apps × New App	-0.066**			
	(0.026)			
19-45 Apps × New App	-0.095***			
	(0.032)			
46+ Apps × New App	-0.095*			
	(0.051)			
Nb of App by Developer		-0.001***	-0.001***	-0.001***
		(0.000)	(0.000)	(0.000)
DFF × New App		-0.055***		
		(0.014)		
New Single App Developer			0.026**	0.036**
			(0.013)	(0.018)
DFF × New Single App Developer				-0.013
				(0.015)
DFF	-0.050***	-0.029***	-0.048***	-0.046***
	(0.007)	(0.009)	(0.007)	(0.007)
Constant	0.601***	0.620***	0.611***	0.611***
	(0.015)	(0.014)	(0.014)	(0.014)
Downloads	Yes	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes
Observations	1,510,745	1,510,745	1,510,745	1,510,745
Number of groups	27,785	27,785	27,785	27,785
Adjusted R2	0.942	0.942	0.942	0.942

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. The omitted size category is a developer with one app for column (1). Robust standard errors are clustered at app level and reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

5 Conclusion

This paper provides empirical evidence that an app produced by a smaller developer is more likely to collect sensitive data from young children who use it, than an app produced by a larger developer. This is an important empirical regularity to document, given that conceptually it is not clear whether apps produced by larger or smaller developers would collect more sensitive data. We present evidence that shows that this is particularly driven by smaller developers in countries with lax privacy regimes. The question then becomes how best to protect child privacy. Using panel data variation, we show that Google's self-certification program that allows developers to opt in to self-certify, can help to protect children's privacy.

These results have several implications. First, many theories of competitive harm by large digital platforms is based on the idea that their size allows them to collect more sensitive data. But we see no evidence of such a pattern in our data.

Second, our results support the view that regulatory interventions should be imposed not only on larger companies but should encourage compliance by small companies. Third, our results suggest also that the high standards imposed by regulation can create market distortions by affecting developers in different ways depending on their capacity to comply with the regulation. The platform self-certification regime seems to encourage US developers to comply with COPPA regulation. This finding is aligned with the aim of the platform to encourage compliance with COPPA legislation.

Further research is needed to investigate the extent to which privacy protection is also associated with better content for children. A potential limitation of our findings is that we have no information on the objectives of data collection beyond content improvement and expected users behavior. However, this study provides a first attempt to understand the complexity of the child apps market and how national privacy regulation affects firms' decisions worldwide.

References

Acquisti, A., Taylor, C. and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*. 54(2), 442–92.

Adjerid, I., Acquisti, A., Telang, R., Padman, R. and Adler-Milstein, J. (2015). The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science*. 62(4), 1042–1063.

Athey, S. (2015). Information, privacy, and the Internet. *CPB Lecture, CPB Netherlands Bureau for Economic Policy Analysis*.

Bajari, P., Chernozhukov, V., Hortaçsu, A. and Suzuki, J. (2019). The impact of big data on firm performance: An empirical investigation. *AEA Papers and Proceedings*. 109, 33–37.

Bian, B., Ma, X. and Tang, H. (2021). The supply and demand for data privacy: Evidence from mobile apps. *Available at SSRN*.

Bleier, A., Goldfarb, A. and Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*. 37(3), 466–480.

Bresnahan, T., Davis, J. P. and Yin, P.-L. (2014a). Economic value creation in mobile applications. In *The changing frontier: Rethinking science and innovation policy*. (pp. 233–286). University of Chicago Press.

Bresnahan, T., Orsini, J. and Yin, P.-L. (2014b). *Platform choice by mobile app developers*. Technical report. National Bureau of Economic Research.

Brill, J. (2011). The intersection of consumer protection and competition in the new world of privacy. *Competition Policy International*. 7(1), 7–23.

Campbell, J., Goldfarb, A. and Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy*. 24(1), 47–73.

Chiou, L. and Tucker, C. (2017). *Search engines and data retention: Implications for privacy and antitrust*. Technical report. National Bureau of Economic Research.

Claussen, J., Peukert, C. and Sen, A. (2019). *The editor vs. the algorithm: Economic returns to data and externalities in online news*. CESifo Working Paper.

Comino, S., Manenti, F. M. and Mariuzzo, F. (2019). Updates management in mobile applications: iTunes versus Google Play. *Journal of Economics & Management Strategy*. 28(3), 392–419.

de Cornière, A. and Taylor, G. (2021). *Data and competition: A general framework with applications to mergers, market structure, and privacy policy*. Working Paper n. 20-1076, Toulouse School of Economics, France.

Deng, Y., Lambrecht, A. and Liu, Y. (2022). *Spillover effects and freemium strategy in the mobile app market*. Working Paper SSRN.

Ershov, D. (2020). *Competing with superstars in the mobile app market*. Working Paper #18-02, NET Institute, USA.

Ershov, D. (2021). *Consumer product discovery costs, entry, quality and congestion in online markets*. Working Paper, Toulouse School of Economics, France.

Farboodi, M., Mihet, R., Philippon, T. and Veldkamp, L. (2019). Big data and firm dynamics. *AEA Papers and Proceedings*. 109, 38–42.

Fuller, C. S. (2017). The perils of privacy regulation. *The Review of Austrian Economics*. 30(2), 193–214.

Ghose, P. and Han, S. P. (2014). Estimating demand for mobile applications in the new economy. *Management Science*. 60(6), 1470–1488.

Goldfarb, A. and Tucker, C. (2012). Privacy and innovation. *Innovation policy and the economy*. 12(1), 65–90.

Goldfarb, A. and Tucker, C. E. (2011). Privacy regulation and online advertising. *Management science*. 57(1), 57–71.

Jia, J., Jin, G. Z. and Wagman, L. (2020). GDPR and the localness of venture investment. *Available at SSRN 3436535*.

Jia, J., Jin, G. Z. and Wagman, L. (2021). The short-run effects of GDPR on technology venture investment. *Marketing Science*. 40(4), 661–684.

Johnson, G. A., Shriver, S. K. and Du, S. (2020). Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science*. 39(1), 33–51.

Kesler, R., Kummer, M. E. and Schulte, P. (2017). *Mobile applications and access to private data: The supply side of the Android ecosystem*. ZEW - Centre for European Economic Research, Discussion Paper # 17-075.

Kummer, M. and Schulte, P. (2019). When private information settles the bill: Money and privacy in Google's market for smartphone applications. *Management Science*. 65(8), 3470–3494.

Leyden, B. T. (2021). *Platform design and innovation incentives: Evidence from the product ratings system on Apple's App Store*. CESifo Working Paper # 9113.

Liu, M., Wang, H., Guo, Y. and Hong, J. (2016). Identifying and analyzing the privacy of apps for kids. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. February. ACM, 105–110.

Livingstone, S., Stoilova, M. and Nandagiri, R. (2019). *Children's data and privacy online: growing up in a digital age: an evidence review*. Technical report. London School of Economics and Political Science.

Marthews, A. and Tucker, C. (2019). Privacy policy and competition. *Brookings Paper*. Last accessed December, 2019.

Miller, A. R. and Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. *Management Science*. 55(7), 1077–1093.

Miller, A. R. and Tucker, C. (2011). Can health care information technology save babies? *Journal of Political Economy*. 119(2), 289–324.

Miller, A. R. and Tucker, C. (2017). Privacy protection, personalized medicine, and genetic testing. *Management Science*. 64(10), 4648–4668.

Montes, R., Sand-Zantman, W. and Valletti, T. (2019). The value of personal information in online markets with endogenous privacy. *Management Science*. 65(3), 1342–1362.

Nielsen (2017). *Mobile kids: the parent, the child and the smartphone*. Technical report. Last accessed January, 2017.

OECD (2013). *Privacy expert group report on the review of the 1980 OECD privacy guidelines*. Technical Report 229.

Peukert, C., Bechtold, S., Batikas, M. and Kretschmer, T. (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*.

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N. and Egelman, S. (2018). Won't somebody think of the children? Examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies*, 63–83.

Rochelandet, F. and Tai, S. H. T. (2016). Do privacy laws affect the location decisions of internet firms? Evidence for privacy havens. *European Journal of Law and Economics*. 42(2).

Tucker, C. (2019). Digital data, platforms and the usual [antitrust] suspects: Network effects, switching costs, essential facility. *Review of Industrial Organization*. 54(4).

Yin, P. L., Davis, J. P. and Muzyrya, Y. (2014). Entrepreneurial innovation: Killer apps in the iPhone ecosystem. *American Economic Review*. 104(5), 255–59.

Supplementary Appendix A: The Dependent Variable

A.1 Descriptive Statistics of Permissions and Interactive Elements Used to Construct Sensitive Data

Sensitive Data is the major dependent variable because it aggregates all types of COPPA-designated categories of sensitive data. It includes four subsets of sensitive data measures: *Sharing*, *Location Data*, *Identity Information* and *User Surveillance*. Table 9 presents the detailed descriptive statistics of each piece of sensitive data used to construct the dependent variable. It also provides detailed statistics by developer location.

The variable *Sharing* takes value 1 if the app requests at least one of the interactive elements allowing apps to share users' personal data with other apps and third parties; this includes *Share Location*, *Share Info* and *Users Interact*. In 2015, the Google Play Store announced the presence of interactive elements to inform consumers on what information the app has access to. The binary variable *Users Interact* measures if the app exchanges sensitive data between users. This feature allows the app to be exposed to unfiltered/uncensored user-generated content including user-to-user communications and media sharing via social media and networks. *Share Info* measures whether the app shares users' personal information with third-parties such as Instagram, Viber and other social networks. *Share Location* equals 1 if the app shares users' locations to other users of social network likes Facebook and Snapchat.[14]

We identify four permissions that request users' location data to construct the binary variable *Location Data*. *ALEC* (Access Location Extra Commands) indicates whether an app collects user's locations based on various device capabilities, and *ANBL* (Approximate Network Based Location) is used to access approximate location derived from network location sources such as cell towers and Wi-Fi. *MLST* (Mock Location Sources for Testing) is used to facilitate developer access to users' locations, and *Precise GPS Location* provides accurate location data.

The binary variable *Identity Information* includes two permissions to identify unique

[14] See esrb.org. Last accessed, July 21, 2020.

individual identity. The permission *Read Phone Status and Identity* allows developers to identify a smartphone's unique IMEI (International Mobile Equipment Identity) which is considered a persistent unique identifier by COPPA and GDPR (Reyes *et al.*, 2018). The IMEI can be used to recognize a user over time and across different online services,[15] and it could be used to log all kinds of personal data and target the consumer. The IMEI number also permits developers to know which advertising is already seen by a user. A child's voice can be captured via the permissions *Record Audio*.

User surveillance is a binary variable that measures whether at least one permission allows access to user activity and contact information. *Read Your Own Contact Card* allows developers to access users' contact cards and associate users' phone numbers with their names. *RCEPCI* (Read Calendar Events Plus Confidential Information) is used to read information stored on users' phones including those of friends. *Read Your Contacts* indicates whether the app reads users' contacts stored including the frequency with which the user communicates with a given individual. The permission *Read Call Log* allows the app to access data about incoming and outgoing calls. *Read Your Browser History and Bookmarks* gives access to web browser information including internet account information.

[15] Complying with COPPA: Frequently Asked Questions. Last accessed, September 3, 2020.

Table 9: **List of Permissions and Interactive Elements Used to Construct the Dependent Variable *Sensitive Data***

	Overall (1)	US (2)	EU (3)	OECD (4)	Non-OECD (5)
Sharing	0.081	0.104	0.082	0.090	0.070
Share Location	0.014	0.020	0.013	0.014	0.013
Share Info	0.013	0.013	0.018	0.015	0.011
Users Interact	0.054	0.071	0.051	0.061	0.047
Location data	0.188	0.220	0.155	0.175	0.205
ALEC[a]	0.003	0.004	0.003	0.003	0.003
ANBL[b]	0.096	0.111	0.075	0.089	0.106
MLST[c]	0.001	0.000	0.001	0.000	0.001
Precise GPS Location	0.088	0.105	0.076	0.083	0.095
Identity Information	0.275	0.296	0.238	0.267	0.284
Read Phone Status And Identity	0.199	0.198	0.166	0.180	0.222
Record Audio	0.076	0.097	0.072	0.087	0.062
User Surveillance	0.042	0.065	0.033	0.046	0.038
Read Your Own Contact Card	0.005	0.009	0.002	0.005	0.004
RCEPCI[d]	0.007	0.007	0.005	0.006	0.008
Read Your Contacts	0.022	0.036	0.018	0.025	0.018
Read Call Log	0.005	0.007	0.005	0.006	0.004
Read Your Browser History and Bookmarks	0.004	0.006	0.003	0.004	0.004

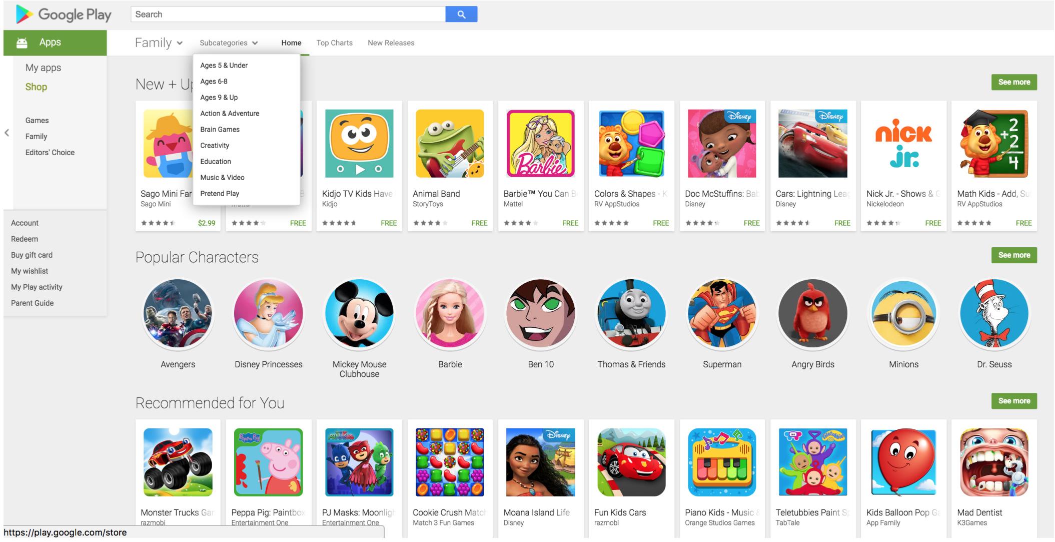
Notes: This table depicts the summary statistics of the permissions and interactive elements used to construct the main dependent variable *Sensitive Data*. Column (1) presents the overall mean. Column (2) presents the mean for sensitive data requested by apps produced in the US. Column (3) presents the mean for sensitive data requested by apps produced in the EU. Column (4) presents the mean for sensitive data requested by apps produced in the OECD countries. Column (5) presents the mean for sensitive data requested by apps produced in the non-OECD countries.

[a] ALEC: Access Location Extra Commands.
[b] ANBL: Approximate Network Based Location.
[c] MLST: Mock Location Sources for Testing.
[d] RCEPCI: Read Calendar Events Plus Confidential Information.

Supplementary Appendix B:
Design for Families Program

DFF was launched in May 2015. Registration in the Google Play Store requires the app developer to pay a one-time fee of $25. There are no additional fees associated with registering for this program. Before Google, the iOS App Store introduced the “Kid category” (Apple’s 2013 Keynote) to target children under the age of 13. Google Play Store provides to developers a detailed documentation on app eligibility criteria to belong to this program.[16]

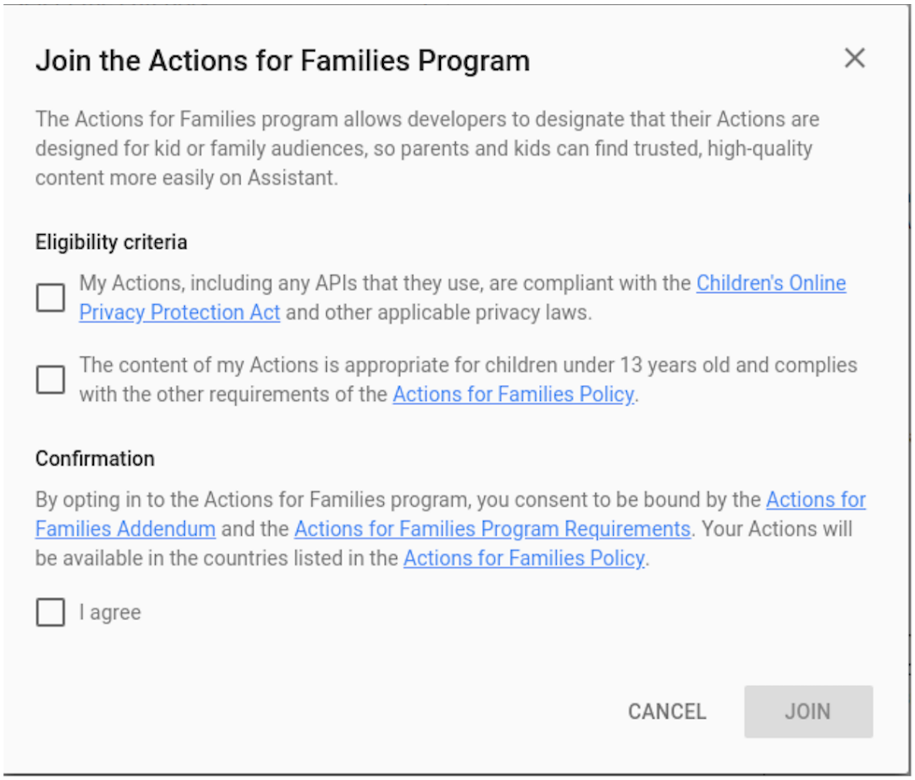
Figure 2: **Screenshot of Google Play Store: Designed for Families Category**



Notes: The figure show the DFF category of the Goolge Playstore.

[16] https://developer.android.com/google-play/guides/families. Last accessed, July 21, 2020.

Figure 3: **Join the Actions for Families Program**



Join the Actions for Families Program

The Actions for Families program allows developers to designate that their Actions are designed for kid or family audiences, so parents and kids can find trusted, high-quality content more easily on Assistant.

Eligibility criteria

□ My Actions, including any APIs that they use, are compliant with the Children's Online Privacy Protection Act and other applicable privacy laws.

□ The content of my Actions is appropriate for children under 13 years old and complies with the other requirements of the Actions for Families Policy.

Confirmation

By opting in to the Actions for Families program, you consent to be bound by the Actions for Families Addendum and the Actions for Families Program Requirements. Your Actions will be available in the countries listed in the Actions for Families Policy.

□ I agree

Notes: Eligibility criteria that developers should opt in when joining the DFF.

Supplementary Appendix C:
COPPA Regulation Enforcement and Developer Location

C.1 COPPA Regulations Enforcement

The FTC ensures compliance with COPPA legislation in the US and in other countries. Since COPPA was implemented, the FTC has investigated more than 30 cases. Table 10 presents some recent cases. Some of these cases involve the app developer directly. The FTC imposes strong requirements regarding the type of data that companies can collect, and how they should protect children's personal information.[17]

Table 10: **COPPA Regulations Enforcement**

Firms	Date	Settlement	Country	Mobile Apps
WW International, Inc.	2022	$1,500,000	US	Yes
OpenX Technologies, Inc.	2021	$2,000,000	US	No
Recolor	2021	$3,000,000	US/ Finland	Yes
TikTok	2019	$5,700,000	China	Yes
HyperBeard	2019	$150,000	US	Yes
YouTube[a]	2019	$170,000,000	US	-
Inmobi	2016	$950,000	Singapore	Yes
LAI Systems	2015	$60,000	US	Yes
Retro Dreamer	2015	$300,000	US	Yes
TinyCo, Inc.	2014	$300,000	US	Yes
Path, Inc	2013	$800,000	US	Yes
Artist Arena LLC	2012	$1,000,000	US	No
RockYou, Inc.	2012	$250,000	US	No
Broken Thumbs	2011	$50,000	US	Yes
Playdom, Inc.	2011	$3,000,000	US	No
Skidekids.com	2011	$100,000	US	No
Iconix Brand Group	2009	$250,000	US	No
Imbee.com	2008	$130,000	US	No
Sony Music Song BMG	2008	$1,000,000	US	No
Xanga.com	2006	$1,000,000	US	No
Ms. Fields Famous Brands	2003	$100,000	US	No

Notes: The table illustrates the amount of settlements imposed by FTC under COPPA rules. All cases can be find on the FTC website.

[a] https://www.ftc.gov/system/files/documents/cases/youtube_complaint.pdf. Last accessed, May 31, 2020.

[17] https://www.ftc.gov/news-events/blogs/business-blog/2018/10/happy-20th-birthday-coppa. Last accessed, July 21, 2020.

C.2 Developer Location

To explore US regulation spillovers to other countries, we retrieve geographical information disclosed by developers of apps available in the Google Play Store. Although the FTC requires that firms collecting or maintaining sensitive data from children should indicate in their online notices or information practices their name, address, telephone and email address, several developers fail to provide a geographical address.[18]

To retrieve developers' countries, we use different strategies. First, we use Maps APIs to collect the latitudes and longitudes of the given address to identify the country. Second, we used a Python library (Libpostal)[19] to search for a country name in the developer's address. Third, we check the match between the location identified using the Google Maps APIs and the country name identified via Libpostal. Fourth, among the subset of apps without any developer's address, we identify their location using the email extension. Using this procedure, we identify the origin countries of 310 apps. Finally, we manually check for certain addresses. We delete apps produced by developers which did not indicate their geographical location since this did not allow us to identify country of origin. To summarize, 19.22% of the initial sample fall into this category.

[18] `https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312`. Last accessed March 2, 2022.

[19] `https://github.com/openvenues/pypostal`. Last accessed, February 13, 2020.

Table 11: **Privacy Regime Based on EU Privacy Regulation: List of Countries Presented in Our Sample**

EU	Recognized by EU	Independent Authority	With Legislation	No Privacy Law
Austria	Andorra	Albania	Angola	Afghanistan
Belgium	Argentina	Australia	Armenia	Algeria
Bulgaria	Canada	Bosnia and Herzegovina	Azerbaijan	Bahrain
Croatia	Israel	Colombia	Brazil	Bangladesh
Cyprus	New Zealand	Costa Rica	Chile	Barbados
Czech Republic	Switzerland	Gabon	China	Belarus
Denmark	US[a]	Ghana	India	Bolivia
Estonia	Uruguay	Hong Kong	Indonesia	Cambodia
Finland		Korea, Rep.	Japan	Congo, Rep.
France		Kosovo	Kazakhstan	Cuba
Germany		Macedonia, FYR	Kyrgyz Republic	Dominican Republic
Greece		Mexico	Malaysia	Ecuador
Hungary		Moldova	Montenegro	Egypt, Arab Rep.
Iceland		Morocco	Nepal	El Salvador
Ireland		Senegal	Nicaragua	Ethiopia
Italy		Serbia	Philippines	Guatemala
Latvia		Tunisia	Qatar	Honduras
Lithuania		Ukraine	Russian Federation	Iran, Islamic Rep.
Luxembourg			Seychelles	Iraq
Malta			Singapore	Jamaica
Netherlands			South Africa	Jordan
Norway			Taiwan, China	Kenya
Poland			Thailand	Kuwait
Portugal			Turkey	Lao PDR
Romania			Vietnam	Lebanon
Slovak Republic			Yemen, Rep.	Mongolia
Slovenia			Zimbabwe	Mozambique
Spain				Myanmar
Sweden				Nigeria
United Kingdom				Oman
				Pakistan
				Palau
				Palestine
				Panama
				Peru
				Puerto Rico
				Samoa
				Saudi Arabia
				Sri Lanka
				Tanzania
				Uganda
				United Arab Emirates
				Uzbekistan
				Venezuela, RB

Notes: This table presents countries categorized according to their level of compliance with EU Privacy legislation.

[a] In July 2020, the EU Court of Justice invalidated the the EU-U.S. Privacy Shield Framework. We consider that US belongs to the category *Recognized by the EU*. From July 2020, US does not belong anymore to this category.

C.3 Where Apps Targeted at Young Children are Produced?

Developers of children's apps are located across the world. Column (1) of Table 12 depicts the distribution of the 10 largest countries in our database. Column (2) indicates the percentage of apps produced by each country. Column (3) shows the sub-sample of new apps which enter the Google Play Store since September 2017.

Column (4) shows the growth rate of new apps by country. It shows that after the

Pakistan (338.46% of the sub-sample of new apps), China (119.53%) and India (101.69%) are the largest producers of new apps in the market followed by the Russian Federation and Hong Kong. Column (5) indicates the average of the variable *Prob Sensitive Data*. Column (6) presents the average data collection on the subsample of apps produced by larger developers. Column (7) presents the average data collection on the subsample of new apps produced by larger developers.

Table 12: **Top 10 Countries in term of Number of Apps in our Sample**

	# Apps	% Apps	# New Apps	% Growth New Apps	Prob Sensitive Data	Prob Sensitive Data 46+ Apps	Prob Sensitive Data 11+New Apps
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
US	6,444	23.19	2,361	57.83	0.34	0.07	0.13
India	2,265	8.15	1,142	101.69	0.39	0.46	0.27
United Kingdom	1,747	6.29	599	52.18	0.26	0.09	0.15
Pakistan	1,140	4.10	880	338.46	0.36	0.06	0.22
Russian Federation	940	3.38	456	94.21	0.25	.	0.04
Germany	914	3.29	254	38.48	0.25	0.02	.
Hong Kong SAR, China	874	3.15	345	65.22	0.55	0.33	0.38
Spain	815	2.93	301	58.56	0.27	0.01	0.01
Israel	756	2.72	272	56.20	0.23	0.12	0.09
China	652	2.35	355	119.53	0.48	0.32	0.23

Notes: The table indicates the top 10 countries in term of number of apps in our sample. Column (1) indicates the total number of apps in each group of countries. Column (2) shows the overall percentage of apps. Column (3) shows the number of new apps created since September 2017. Column (4) illustrates growth rates of the number of apps created after September 2017. Column (5) shows the percentage of apps requesting at least one piece of sensitive data. Column (6) presents the percentage of apps produced by larger developers requesting at least one piece of sensitive data. Column (7) indicates the percentage of apps produced by larger developers of new apps requesting at least one piece of sensitive data.

Supplementary Appendix D:
Size of Apps and Downloads

To measure the market size of a given app, we use the download category provided by Google Play Store that includes 21 distinct groups. The number of downloads are presented in Table 13 and range from 0 to over five billion downloads. It shows the mean of apps across download intervals.

Table 13: **Summary Statistics: Distribution of Downloads**

	Mean	Min	Max
Downloads 0	0.001	0	1
Downloads 1	0.014	0	1
Downloads 5	0.013	0	1
Downloads 10	0.059	0	1
Downloads 50	0.035	0	1
Downloads 100	0.099	0	1
Downloads 500	0.047	0	1
Downloads 1k	0.114	0	1
Downloads 5k	0.050	0	1
Downloads 10k	0.112	0	1
Downloads 50k	0.052	0	1
Downloads 100k	0.136	0	1
Downloads 500k	0.063	0	1
Downloads 1000k	0.124	0	1
Downloads 5000k	0.033	0	1
Downloads 10000k	0.034	0	1
Downloads 50000k	0.005	0	1
Downloads 100000k	0.005	0	1
Downloads 500000k	0.0008	0	1
Downloads 1000000k	0.0008	0	1
Downloads 5000000k	0.0001	0	1

Notes: The table illustrates the distribution of apps per download range and it indicates the lower range.

D.1 Coefficients of Download Dummies Associated to the Main Estimates

Table 14 reports the estimates of download intensity measures. We check whether our result holds for a different potential measure of size. It appears that indeed apps with small number of downloads are more likely to collect sensitive data.

Table 14: **Child Sensitive Data Collection Download Dummies**

Sensitive Data as	Developer Size	DFF	Main Specification
Dependent Variable	(1)	(2)	(3)
Downloads 50	0.012**	0.012**	0.011**
	(0.005)	(0.005)	(0.005)
Downloads 100	0.027***	0.025***	0.025***
	(0.007)	(0.007)	(0.007)
Downloads 500	0.034***	0.032***	0.031***
	(0.009)	(0.009)	(0.009)
Downloads 1k	0.041***	0.037***	0.037***
	(0.010)	(0.010)	(0.010)
Downloads 5k	0.039***	0.033***	0.033***
	(0.011)	(0.011)	(0.011)
Downloads 10k	0.041***	0.034***	0.035***
	(0.013)	(0.013)	(0.013)
Downloads 50k	0.043***	0.034**	0.036**
	(0.015)	(0.015)	(0.015)
Downloads 100k	0.047***	0.036**	0.038**
	(0.017)	(0.017)	(0.017)
Downloads 500k	0.050**	0.037*	0.040**
	(0.020)	(0.020)	(0.020)
Downloads 1000k	0.029	0.016	0.019
	(0.022)	(0.021)	(0.022)
Downloads 5000k	-0.016	-0.029	-0.027
	(0.029)	(0.029)	(0.029)
Downloads 10000k	-0.081**	-0.096***	-0.093**
	(0.037)	(0.037)	(0.037)
Downloads 50000k	-0.098	-0.114	-0.111
	(0.070)	(0.070)	(0.070)
Downloads 100000k	-0.138	-0.151	-0.149
	(0.102)	(0.101)	(0.101)
Downloads 500000k	-0.121	-0.131	-0.130
	(0.162)	(0.162)	(0.162)
Downloads 1000000k	-0.492*	-0.498*	-0.498*
	(0.264)	(0.263)	(0.263)
Downloads 5000000k	-0.413	-0.417	-0.416
	(0.371)	(0.371)	(0.371)
Contains Ad	0.013	0.011	0.011
	(0.009)	(0.009)	(0.009)
Downloads	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes
Week FE	Yes	Yes	Yes
App FE	Yes	Yes	Yes
Observations	1,510,745	1,510,745	1,510,745
Number of groups	27,785	27,785	27,785
Adjusted R2	0.942	0.942	0.942

Notes: The table reports the coefficients of each dummy variable indicating the lower range of downloads which are estimated in the main regression presented in Table 5. *Sensitive Data* is the dependent variable. The omitted category is the downloads category with less than 50 downloads. Robust standard errors clustered at app level are reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

Supplementary Appendix E:
Robustness Check

E.1 Apps Offering Advertising

The main finding suggests that larger developers are likely to collect less data. The major focus of this paper is also to understand why developers collect children's sensitive data. The literature suggests that personal data can improve targeted ads. Therefore, data collection can be correlated with advertising business model.[20] The tag "Contains Ad" notifies prospective users that ads are used in the app prior to installation. We exploit this information to measure if the apps provide advertising. We create the binary variable *Contains Ad* which takes the value 1 if the app displays advertisements to users. Overall, 53.4% of apps use ads.

We split the sample into apps not using ads and those that do. We present the estimates in Table 15. We use two measures of developer size to test whether size is correlated with collection of sensitive data for apps using ads. The second set of regressions includes the variable *Large # installs* to measure whether developers with many users rely on data collection. We see that our main results hold for apps that contains ads. Larger developers have the competencies to offer ads without relying on user data collection.

[20] We do not provide specific information on freemium; it applies to 10.09% of the apps in the sample.

Table 15: **Data Collection by Advertising Business Model**

Sensitive Data	With Downloads		With Large Installs	
as Dependent Variable	Contains Ad=0	Contains Ad=1	Contains Ad=0	Contains Ad=1
	(1)	(2)	(3)	(4)
2-4 Apps	-0.016	0.013	-0.015	0.012
	(0.012)	(0.015)	(0.012)	(0.015)
5-18 Apps	-0.002	0.012	0.000	0.010
	(0.015)	(0.021)	(0.015)	(0.021)
19-45 Apps	0.009	-0.032	0.011	-0.034
	(0.018)	(0.026)	(0.018)	(0.025)
46+ Apps	-0.043	-0.075**	-0.040	-0.078**
	(0.034)	(0.034)	(0.034)	(0.033)
DFF	-0.007	-0.072***	-0.007	-0.071***
	(0.009)	(0.009)	(0.009)	(0.009)
Large # installs			0.032	-0.055***
			(0.064)	(0.021)
Constant	0.560***	0.647***	0.595***	0.651***
	(0.016)	(0.022)	(0.012)	(0.017)
Downloads	Yes	Yes	No	No
Contains Ad	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes
Observations	703,977	806,453	703,977	806,453
Number of groups	20,990	16,902	20,990	16,902
Adjusted R2	0.965	0.922	0.965	0.922

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. Omitted size category is developer with one app. 25 observations are dropped as they do not vary in the sub-samples. Robust standard errors clustered at app level reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

E.2 Alternative Functional Forms

We report our main estimates from models with different functional forms, including probit and poisson. Table 16 shows the robustness of the results to different functional forms. Column (1) shows the estimates of a probit estimation. We use the dependent variable *Prob Sensitive Data*. The sample size is smaller because some observations are dropped for lack of variation in the outcome, but the pattern of results matches the OLS estimates. Column (2) shows the results of the Poisson functional form that accounts for the number of pieces of sensitive data collected. Larger developers are less likely to collect sensitive data. DFF certification is negatively associated with data collection. Overall, the main results hold.

Table 16: **Robustness Check with Different Functional Forms**

Dependent Variable:	*Prob Sensitive Data*	*Sensitive Data*
	Probit	Poisson
	(1)	(2)
2-4 Apps	-0.150***	-0.178***
	(0.022)	(0.029)
5-18 Apps	-0.189***	-0.382***
	(0.023)	(0.028)
19-45 Apps	-0.235***	-0.456***
	(0.027)	(0.035)
46+ Apps	-0.671***	-0.910***
	(0.033)	(0.048)
DFF	-0.442***	-0.785***
	(0.018)	(0.024)
Constant	-0.212***	-0.161***
	(0.035)	(0.050)
Downloads	Yes	Yes
Contains Ad	Yes	Yes
Week FE	Yes	Yes
App FE	No	No
Observations	1,510,604	1,510,745
Number of groups	27,785	27,785
Wald chi2	3052.122	5083.501

Notes: Probit and Poisson estimates with random effects. Omitted size category is developer with one app. Column (1) uses as dependent variable the binary variable *Prob Sensitive data*. 141 observations are dropped because of perfect predict. Column (2) uses *Sensitive Data* as the dependent variable. Robust standard errors clustered at app level are reported in parentheses. Significance levels: $*p < .10$, $**\,p < .05$, $***p < .01$

E.3 Estimates with Alternative Measures of Sensitive Data

We check whether our result holds for different measures of sensitive data. One potential critique is that our main dependent variable includes a broad definition of sensitive data. We check whether a given set of sensitive data is driving our results. Table 17 shows the estimates in each column. We consider the main measure of sensitive data excluding one category of sensitive data. Column (1) excludes the set of data *Sharing* and column (2) excludes *Location Data.* Column (3) reports the estimates when the dependent variable is the main dependent variable excluding *Identity Information.* The estimates show that medium and large size developers are less likely to collect more sensitive data. Column (4) estimates the main dependent variable excluding *User Surveillance.* Overall, we find that larger developers collect less data. Apps that belong to DFF might be more careful to share and collect information from this vulnerable audience.

Table 17: **Alternative Dependent Variables**

	Excluding Each of These Sets of Sensitive Data			
	Sharing	Location Data	Identity Information	User Surveillance
	(1)	(2)	(3)	(4)
2-4 Apps	0.003	-0.004	-0.000	-0.003
	(0.010)	(0.007)	(0.008)	(0.009)
5-18 Apps	0.011	0.001	-0.005	0.002
	(0.013)	(0.009)	(0.010)	(0.013)
19-45 Apps	-0.009	0.003	-0.026**	-0.017
	(0.016)	(0.011)	(0.012)	(0.016)
46+ Apps	-0.066***	-0.028**	-0.043***	-0.095***
	(0.024)	(0.014)	(0.017)	(0.024)
DFF	-0.033***	-0.029***	-0.050***	-0.037***
	(0.006)	(0.005)	(0.005)	(0.007)
Constant	0.507***	0.379***	0.369***	0.560***
	(0.014)	(0.011)	(0.011)	(0.015)
Downloads	Yes	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes
Observations	1,510,745	1,510,745	1,510,745	1,510,745
Number of groups	27,785	27,785	27,785	27,785
Adjusted R2	0.930	0.937	0.947	0.934

Notes: OLS with app and week fixed effects. Dependent variable is as noted. Omitted size category is developer with one app. Robust standard errors clustered at app level reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

E.4 Developer Size and Experience

E.4.1 Do Experienced Developers Collect less Sensitive Data?

In this section, we check whether a developer's experience as well as the pattern of entry in the market might affect the negative relationship between developer size and sensitive data collection. Given the work of Kummer and Schulte (2019) who find a pattern of developer app experience correlates with requests for more data, it is important to understand how this might influence our results.

We use the continuous measures of developer size to have consistent estimates for each sub-group of countries. We estimate two sets of regressions, dividing the sample according to the year in which the developer enters the Google Play Store. We consider two distinct groups of developers: those that enter the Google Play Store before the creation of the DFF (May 2015) and those who enter after. We also consider whether each app was created before or after May 2015. Columns (1) and (2) of Table 18 show the estimates of the main equation when we restrict to the sub-sample of apps produced by developers that enter the Google Play Store before May 2015. Column (1) includes only apps created before the creation of the DFF. Column (2) estimates the main equation with the sub-sample of apps created after the creation of the DFF.

Column (3) explores what happens when we restrict our sample to sub-samples of apps produced by developers that enter the market after the creation of the DFF (and therefore apps created after May 2015). It shows that the increase of the size of developers is negatively associated with sensitive data collection. This estimate provides suggestive evidence that the size effects we measure are driven partially by developers that enter the market after the creation of the DFF.

Table 18: **Developer Entry Before and After DFF**

Sensitive Data as	Developer Entry Before DFF		Developer Entry After DFF
Dependent Variable	App Created Before DFF	App Created After DFF	App Created After DFF
	(1)	(2)	(3)
Nb of Apps by Developer	-0.000*	-0.000	-0.007***
	(0.000)	(0.000)	(0.001)
DFF	-0.041***	-0.087***	-0.028***
	(0.014)	(0.014)	(0.010)
Constant	0.726***	0.519***	0.601***
	(0.057)	(0.025)	(0.018)
Downloads	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes
Week FE	Yes	Yes	Yes
App FE	Yes	Yes	Yes
Dep. var. mean	0.703	0.463	0.580
Observations	488,932	431,407	590,404
Number of groups	7,181	7,163	13,589
Adjusted R2	0.958	0.919	0.936

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. Two singleton observations are dropped. Robust standard errors are clustered at app level. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

E.4.2 Privacy Regime and Developer's Experience

In this section, we used two sources of heterogeneity to test the robustness and explore the underlining mechanisms of our results, the developer creation date and national privacy regime of developer. We split the sample into developers that enter the market before and after the creation of the DFF and we estimate a separate regression for each privacy regulation regime. App privacy strategies of developers who enter before the DFF was launched may differ from those who enter afterwards. Table 19 presents the estimates for the subsample of apps produced by developers that enter the market before the creation of the DFF. Columns (1)-(6) present the estimates on the subsample of apps created before the DFF. Columns (7)-(12) present the estimates on the subsample of apps created after the DFF by more experienced developers. A pattern emerges when we split the sample into apps produced before DFF (see Columns (1)-(6) of Table 19) and apps produced after DFF (see Columns (7)-(12) of Table 19). This subsample split meant to capture how developers' size and self-certification influence data collection for apps produced before and after the implementation of the self-certification by experienced developers. Columns (1)-(6) show that for apps produced before the DFF by large existing developers there is no effect of size on the collection of sensitive data. The estimates in Column (6) of Table 19 shows that apps produced before the creation of the DFF by larger developers in countries with no legislation (*No privacy regime*) were more likely to collect sensitive data.

Columns (7)-(12) of Table 19 show that the pattern that larger developers are less likely to request data is replicated in apps produced in: the US, countries with an independent authority and countries with privacy legislation. The effect of developer size is positive for apps produced in European countries and countries with no privacy regime. However, at the same time, the effect of DFF is negative and significant for apps produced in EU.

Table 19: **Stratification by Privacy Regime: Developer Entry before Creation of the DFF**

	Developers enter Before DFF											
		App Created Before DFF						App Created After DFF				
Sensitive Data as	US	Privacy Regime					US	Privacy Regime				
Dependant Variable	US (1)	EU (2)	Rec. EU (3)	Ind. Aut (4)	With leg (5)	No Privacy (6)	US (7)	EU (8)	Rec. EU (9)	Ind. Aut (10)	With leg (11)	No Privacy (12)
Nb of Apps by Developer	-0.000	-0.000	-0.000	0.001	-0.001	0.009***	-0.002*	0.001**	-0.000	-0.006***	-0.002***	0.008***
	(0.000)	(0.000)	(0.000)	(0.002)	(0.001)	(0.003)	(0.001)	(0.000)	(0.000)	(0.002)	(0.001)	(0.002)
DFF	-0.012	-0.005	-0.015	0.031	-0.131***	-0.050	-0.154***	-0.044**	-0.114***	-0.049	-0.084***	-0.155
	(0.026)	(0.020)	(0.023)	(0.034)	(0.042)	(0.085)	(0.037)	(0.019)	(0.027)	(0.047)	(0.027)	(0.103)
Constant	0.827***	0.595***	0.789***	1.025***	0.404***	-0.290	0.727***	0.402***	0.599***	0.801***	0.463***	0.450***
	(0.079)	(0.103)	(0.074)	(0.105)	(0.151)	(0.368)	(0.053)	(0.045)	(0.040)	(0.090)	(0.057)	(0.154)
Downloads	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dep. var. mean	0.812	0.599	0.796	0.766	0.667	0.586	0.605	0.421	0.530	0.496	0.410	0.636
Observations	164,710	164,767	200,329	36,469	79,134	8,233	96,477	155,407	130,662	40,578	96,114	8,646
Number of groups	2,316	2,459	2,839	555	1,184	144	1,565	2,593	2,107	650	1,645	168
Adjusted R2	0.970	0.958	0.967	0.947	0.933	0.944	0.940	0.925	0.940	0.921	0.877	0.940

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. This table shows the estimates of sub-samples of developers enter before the DFF was enacted. Columns (1) and (7) report the estimates of the sub-sample of apps produced in the US respectively for apps created before the DFF and after the DFF. Columns (2) and (8) report the estimates of the sub-sample of apps produced in the EU respectively for apps created before the DFF and after the DFF. Column (3) and (9) report the estimates of the sub-sample of apps produced in countries with a privacy regulation regime recognized by the EU respectively for apps created before the DFF and after the DFF. Column (4) and (10) show the estimates within the sub-sample of apps produced in countries with an independent privacy authority respectively for apps created before the DFF and after the DFF. Column (5) and (11) show the estimates of apps produced in countries with a privacy legislation for apps created before the DFF and after the DFF. Columns (6) and (12) show the estimates of apps produced in countries with no privacy legislation for apps created before the DFF and after the DFF. Robust standard errors are clustered at app level and reported in parentheses. Significance levels: $*p < .10$, $**p < .05$, $***p < .01$

We explore what happens when we restrict our sample to developers who enter after the creation of the DFF. Columns (1)-(6) of Table 20 present the estimates. The estimates show that both developer size and self-certification regime are likely to affect the pieces of sensitive data requested. They also show that apps created after the DFF are less likely to request sensitive data. Column (6) suggests that developers' size is negative and statistical significant for apps produced in no privacy law countries. In the previous estimates of Table 19, developer size was positive and significant.

Table 20: **Stratification by Privacy Regime: Developer Entry after Creation of DFF**

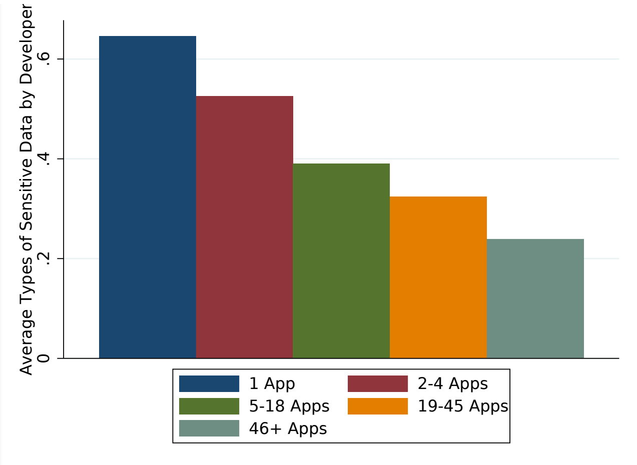
		Developers Enter After DFF				
Sensitive Data as	US	Privacy Regime				
Dependant Variable	US (1)	EU (2)	Rec. EU (3)	Ind. Aut (4)	With leg (5)	No Privacy (6)
Nb of App by Developer	-0.004	-0.010***	-0.012***	0.000	-0.002	-0.005***
	(0.003)	(0.002)	(0.003)	(0.002)	(0.002)	(0.001)
DFF	-0.111***	0.008	-0.087***	-0.020	-0.020	-0.072***
	(0.027)	(0.014)	(0.023)	(0.023)	(0.022)	(0.028)
Constant	0.651***	0.575***	0.599***	0.462***	0.604***	0.831***
	(0.029)	(0.034)	(0.027)	(0.055)	(0.033)	(0.060)
Downloads	Yes	Yes	Yes	Yes	Yes	Yes
Contains Ad	Yes	Yes	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes	Yes	Yes
App FE	Yes	Yes	Yes	Yes	Yes	Yes
Dep. var. mean	0.570	0.498	0.550	0.654	0.589	0.732
Observations	115,510	136,101	149,168	65,331	178,297	61,507
Number of groups	2,572	2,955	3,255	1,375	4,280	1,724
Adjusted R2	0.957	0.937	0.952	0.903	0.929	0.945

Notes: OLS with app and week fixed effects. *Sensitive Data* is the dependent variable. This table reports the estimates of by apps produced by developers who enter the market after the creation of the DFF. Column (1) reports the estimates of the sub-sample of apps produced in the US. Column (2) reports the estimates of the sub-sample of apps produced in the EU. Column (3) reports the estimates of the sub-sample of apps produced in countries with a privacy regulation regime recognized by EU. Column (4) shows the estimates within the sub-sample of apps produced in countries with an independent privacy authority. Column (5) shows the estimates of apps produced in countries with a privacy legislation. Column (6) shows the estimates of apps produced in countries with no privacy legislation. Robust standard errors are clustered at app level and reported in parentheses. Significance levels: $*p < .10$, $**\,p < .05$, $***p < .01$

Supplementary Appendix F:
Developers Level

Figure 4 shows the average types of sensitive data requested by developer size. The summary statistic points out that while smaller developers collect different types of data, developers with multiple apps request on average the same pieces of sensitive data rather than incremental data.

Figure 4: **Average Types of Sensitive Data at the Developer Level**



Notes: The y-axis indicates the average number of types of sensitive data collected by developer.