

On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies

Workshop on Technology and Consumer Protection '19

Ehimare Okoyomon, **Nikita Samarin**, Primal Wijesekera, Amit Elazari Bar On,
Narseo Vallina-Rodriguez, Irwin Reyes, Álvaro Feal, Serge Egelman



Berkeley
UNIVERSITY OF CALIFORNIA



INTERNATIONAL
COMPUTER SCIENCE
INSTITUTE



institute
IMdea
networks



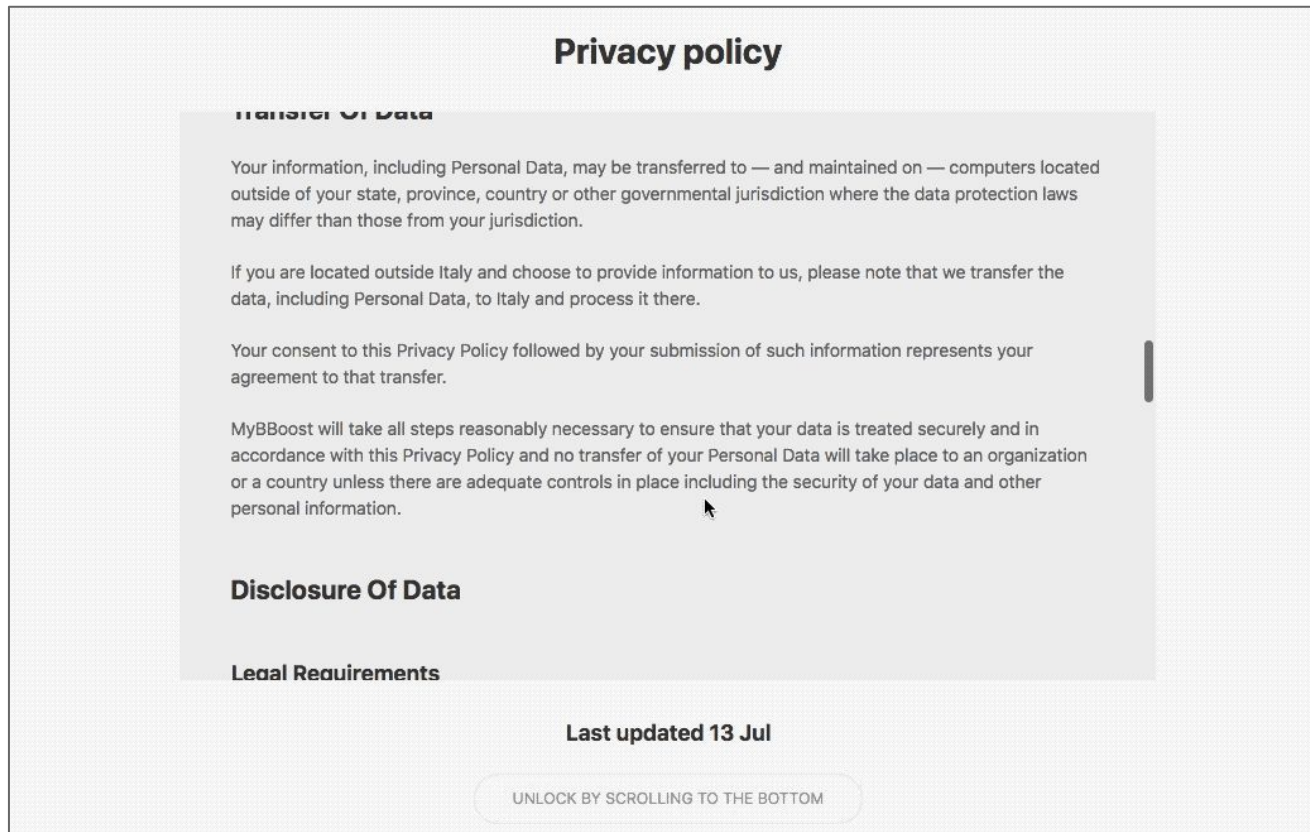
Universidad
Carlos III de Madrid

Notice and Consent

- Websites or mobile apps provide **notice** to users about their information collection practices and obtain their **consent** before collecting and sharing personal information

In practice, Notice and Consent Does Not Work

The hypothetical opportunity cost if each individual in the US started reading every encountered privacy policy is **781 BILLION US dollars!**



The image shows a screenshot of a privacy policy page. The page has a light gray background with a dark gray border. At the top, the title "Privacy policy" is centered in a bold, black font. Below the title, there are several sections of text, each with a bold heading: "Transfer Of Data", "Disclosure Of Data", and "Legal Requirements". The text under "Transfer Of Data" discusses data being transferred to computers outside the user's jurisdiction. The text under "Disclosure Of Data" mentions that data is transferred to Italy. The text under "Legal Requirements" states that MyBBoost will take steps to ensure data security. At the bottom of the page, there is a button that says "UNLOCK BY SCROLLING TO THE BOTTOM". The button is white with a dark gray border and is centered at the bottom of the page. A mouse cursor is visible over the text in the "Legal Requirements" section.

Privacy policy

Transfer Of Data

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside Italy and choose to provide information to us, please note that we transfer the data, including Personal Data, to Italy and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

MyBBoost will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Disclosure Of Data

Legal Requirements

Last updated 13 Jul

UNLOCK BY SCROLLING TO THE BOTTOM

Motivation

- Consumers do not read privacy policies...
- ... but even if they would, what difference would it make?
- **Can we be certain that disclosures made in privacy policies reflect actual data collection practices, at least in the context of mobile apps?**

What types of disclosures do we focus on?

1. Children's Privacy

Families and COPPA

Google Play offers a rich platform for developers to showcase trusted, high-quality and age appropriate content for the whole family. Before submitting an app to the Designed for Families program, ensure your app is appropriate for children and compliant with COPPA and other relevant laws.



2. Third-Party Data Collection

Art. 13 GDPR

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
 - (e) the recipients or categories of recipients of the personal data, if any;

3. Reasonable Security Measures



The image shows a screenshot of the Federal Trade Commission (FTC) website. At the top left is the FTC logo, which features a shield with a scale of justice and the text 'FEDERAL TRADE COMMISSION • UNITED STATES OF AMERICA'. To the right of the logo, the text 'FEDERAL TRADE COMMISSION' is displayed in large, bold, white letters, with 'PROTECTING AMERICA'S CONSUMERS' in smaller, light blue letters below it. Below the header is a dark blue navigation bar with four white text links: 'ABOUT THE FTC', 'NEWS & EVENTS', 'ENFORCEMENT', and 'POLICY'. Below the navigation bar is a white content area. At the top of this area is a breadcrumb trail: 'Home » Tips & Advice » Business Center » Guidance » App Developers: Start with Security'. Below the breadcrumb trail is the main title 'App Developers: Start with Security' in a large, dark blue font. At the bottom of the content area, there is a 'TAGS:' section with four links: 'Privacy and Security', 'Consumer Privacy', 'Data Security', and 'Tech', separated by vertical bars.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

[ABOUT THE FTC](#) | [NEWS & EVENTS](#) | [ENFORCEMENT](#) | [POLICY](#)

[Home](#) » [Tips & Advice](#) » [Business Center](#) » [Guidance](#) » [App Developers: Start with Security](#)

App Developers: Start with Security

TAGS: [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#) | [Tech](#)

3. Reasonable Security Measures

App Developers: Start with Security

Use transit encryption for usernames, passwords, and other important data.

To protect users, developers often deploy TLS in the form of HTTPS. Consider using HTTPS or another industry-standard method. There's no need to reinvent the wheel. If you use HTTPS, use a digital certificate and ensure your app checks it properly. A no-frills digital certificate from a reputable vendor is inexpensive and helps your customers ensure they're communicating with your servers, and not someone else's. But standards change, so keep an eye on current technologies, and make sure you're using the latest and greatest security features.

How do we compare disclosures in privacy policies to actual app behaviors?

The approach that we use



Database containing information about **68,051** Android apps' **runtime** and **network** behavior
(read more in [1])

Reddit Privacy Policy

Effective June 8, 2018. Last Revised May 25, 2018

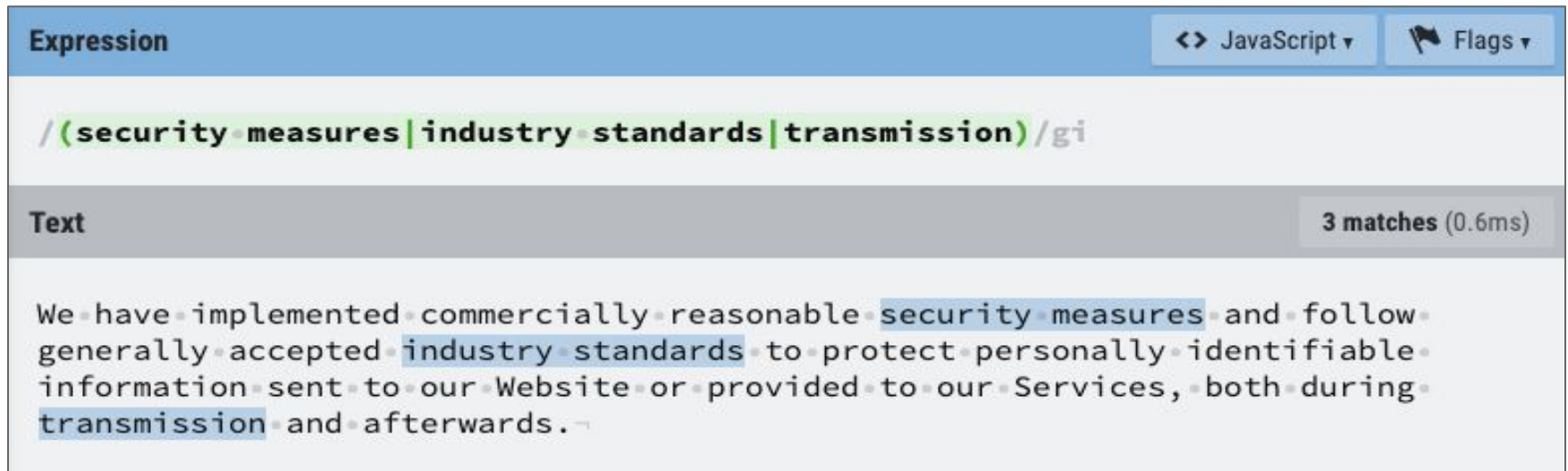
We want you to understand how and why Reddit, Inc. ("Reddit," "we" or "us") collects, uses, and shares information about you when you use our websites, mobile apps, widgets, and other online products and services (collectively, the "Services") or when you otherwise interact with us or receive a communication from us. This Privacy Policy applies to all of our Services including Reddit Gifts, which maintains a [separate privacy notice](#) that incorporates this Privacy Policy by reference.

Textual analysis of privacy policies to locate disclosures related to our problem domain
(this work)

[1] 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, 2018(3), pp.63-83.

Policy Text Analysis

String matching using regular expressions (“regex”) against known keywords and manual refinements



The screenshot shows a web-based regex testing interface. At the top, there is a header bar with the word "Expression" on the left, and two buttons on the right: a code editor icon labeled "JavaScript" and a flag icon labeled "Flags". Below the header, the search expression `/(security·measures|industry·standards|transmission)/gi` is entered. The expression is highlighted in green. Below the expression, there is a section labeled "Text" on the left, and a status indicator on the right that says "3 matches (0.6ms)". The text being searched is: "We·have·implemented·commercially·reasonable·security·measures·and·follow·generally·accepted·industry·standards·to·protect·personally·identifiable·information·sent·to·our·Website·or·provided·to·our·Services,·both·during·transmission·and·afterwards.↵". The words "security·measures", "industry·standards", and "transmission" are highlighted in blue, indicating they are matches for the regex.

What did we find for each category of misrepresentations?

Children's Privacy

- We analyzed privacy policies of 8,030 Android apps in DFF
- Out of these apps
 - **728 apps (9.1%) explicitly claim not to be directed at children**
 - **2,457 (30.6%) claim no knowledge of collecting any data from children under 13**



Smart Games for Kids for Free


DEVGAME KIDS Educational Education

★★★★★ 4,971

Everyone Ages 8 & Under

Contains Ads · Offers in-app purchases

⚠️ You don't have any devices.

 Add to Wishlist

 Install

Through these Services, DEVGAME does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to access those Services.

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20584

In the Matter of)
)
Request to Investigate Google's Unfair and)
Deceptive Practices in Marketing Apps for)
Children)
)
By

CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD (CCFC)
CENTER FOR DIGITAL DEMOCRACY (CDD)
BADASS TEACHERS ASSOCIATION
BERKELEY MEDIA STUDIES GROUP
COLOR OF CHANGE
CONSUMER ACTION
CONSUMER FEDERATION OF AMERICA
CONSUMER WATCHDOG
DEFENDING THE EARLY YEARS
ELECTRONIC PRIVACY INFORMATION CENTER
MEDIA EDUCATION FOUNDATION
NEW DREAM
OPEN MEDIA AND INFORMATION COMPANIES INITIATIVE (OPEN MIC)
PARENTS ACROSS AMERICA
PARENT COALITION FOR STUDENT PRIVACY
PARENTS TELEVISION COUNCIL
PEACE EDUCATORS ALLIED FOR CHILDREN EVERYWHERE (P.E.A.C.E.)
PRIVACY RIGHTS CLEARINGHOUSE
PUBLIC CITIZEN
STORY OF STUFF
TEACHERS RESISTING UNHEALTHY CHILDHOOD ENTERTAINMENT (TRUCE)
U.S. PIRG

DEVGAME KIDS (ages 6-8) transmitted a staggering 40 unencrypted device identifiers to third parties including Applovin and MoPub.⁹¹

Third-Party Data Sharing

- We analyzed the entire corpus of 68,051 apps
- We found that 22,856 apps do not mention third-party affiliates in their privacy policies, however, **7147 (31.3% of 22,856) still share user identifiers**
- Only **15,106 apps (22.2% of 68,051) explicitly name third-party affiliates**

Reasonable Security Practices

- We analyzed 9,424 apps that do not use TLS when transmitting personal identifiers over the network
- Out of these, **2,680 apps (28.4%) claim to take measures to secure user data**



The Perfect Date

iCandy Digital Puzzle

★★★★★ 195

Everyone

Contains ads

⚠ You don't have any devices.

Add to wishlist

Install

We also understand that it is important to keep your information safe and secure. Commercially reasonable security measures to safeguard and secure your information and to prevent the destruction, loss, misuse and alteration of information under our control have been implemented by us. We do not believe that there is any transmission method over website or Internet that is completely flawless, even though our commercially reasonable security measures have been put in place against possible breaches of our sites' security and our user records and databases. We are not liable for data loss, hacking, unauthorized access or other breaches in

Summary

- 9% of apps in the DFF program claim not to be directed at children
- 31% of apps that share user data with third-party service providers do not provide notice to users
- 28% of apps that do not encrypt data in-transit claim to take reasonable security measures

Takeaways

- We found contradictions between disclosures made in privacy policies and actual data collection practices for all three types of problem domains
- Even if consumers want to learn about data collection practices of mobile apps, they are unable to do so with the current quality of privacy disclosures

Third-Party Data Sharing

- We analyzed the entire corpus of **68,051 apps**
- We found that 22,856 apps do not mention third-party affiliates in their privacy policies, however, **7147 (31.3% of 22,856) still share user identifiers**
- Only **15,106 apps (22.2% of 68,051) explicitly name third-party affiliates**

Notice and Consent

- The dominant privacy framework in the context of online privacy
- Websites or mobile apps provide **notice** to users about their information collection practices and obtain their **consent** before collecting and sharing personal information
- In theory, users are expected to be aware of the privacy implications of consenting to the service provider's privacy policy...

Third-Party Data Sharing

Description	Observed App #	Sample Size
Mention third parties	45,195	68,051
Provide names of third parties explicitly	15,106 (33.4%)	45,195
Undisclosed sharing (third parties not mentioned)	7,147 (31.3%)	22,856

Children's Privacy

Description	Observed App #	Sample Size
Participate in DFF program	8,030	68,051
Claim not to target children	728 (9.1%)	8,030
Claim no knowledge of collecting children data	2,457 (30.6%)	8,030

Reasonable Security Practices

- We analyzed the entire corpus of **68,051 apps**
- Using the AppCensus dataset, we found that 9,424 apps (13.8% of 68,051) do not use TLS when transmitting personal identifiers over the network
- Out of these, **2,680 apps (28.4% of 9,424) claim to take measures to secure data transmission**

Reasonable Security Practices

Description	Observed App #	Sample Size
No encryption in-transit (i.e. no TLS)	9,424 (13.8%)	68,051
Claim to secure data transmission	2,680 (28.4%)	9,424