



# PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps

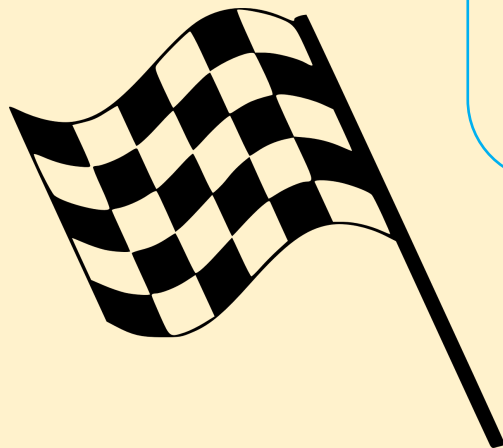
*Sebastian Zimmeck*

*Rafael Goldstein*

*David Baraka*

NDSS, February 24, 2021

Hmm, I wonder if I need a privacy policy for my app. Also, what should I write in there?  
I am lost ...



Privacy Policy

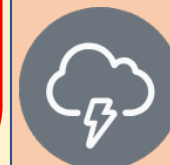
Questionnaire  
Wizard



```
22 var currentLoc : CLLocationCoordinate2D!  
23 let healthKitStore = HKHealthStore()  
24  
25  
26 override func viewDidLoad() {  
27     super.viewDidLoad()  
28  
29     workoutTable.backgroundColor = UIColor.lightGray  
30     workoutTable.separatorColor = UIColor.blue  
31  
32     // Ask for Authorization from the User.  
33     self.locationManager.requestAlwaysAuthorization()  
34  
35     // For use in foreground  
36     self.locationManager.requestWhenInUseAuthorization()  
37  
38     if CLLocationManager.locationServicesEnabled() {  
39         locationManager.delegate = self  
40         locationManager.desiredAccuracy = kCLLocationAccuracyNearestTenMeters  
41         locationManager.startUpdatingLocation()  
42     }  
43 }
```

Code Analysis

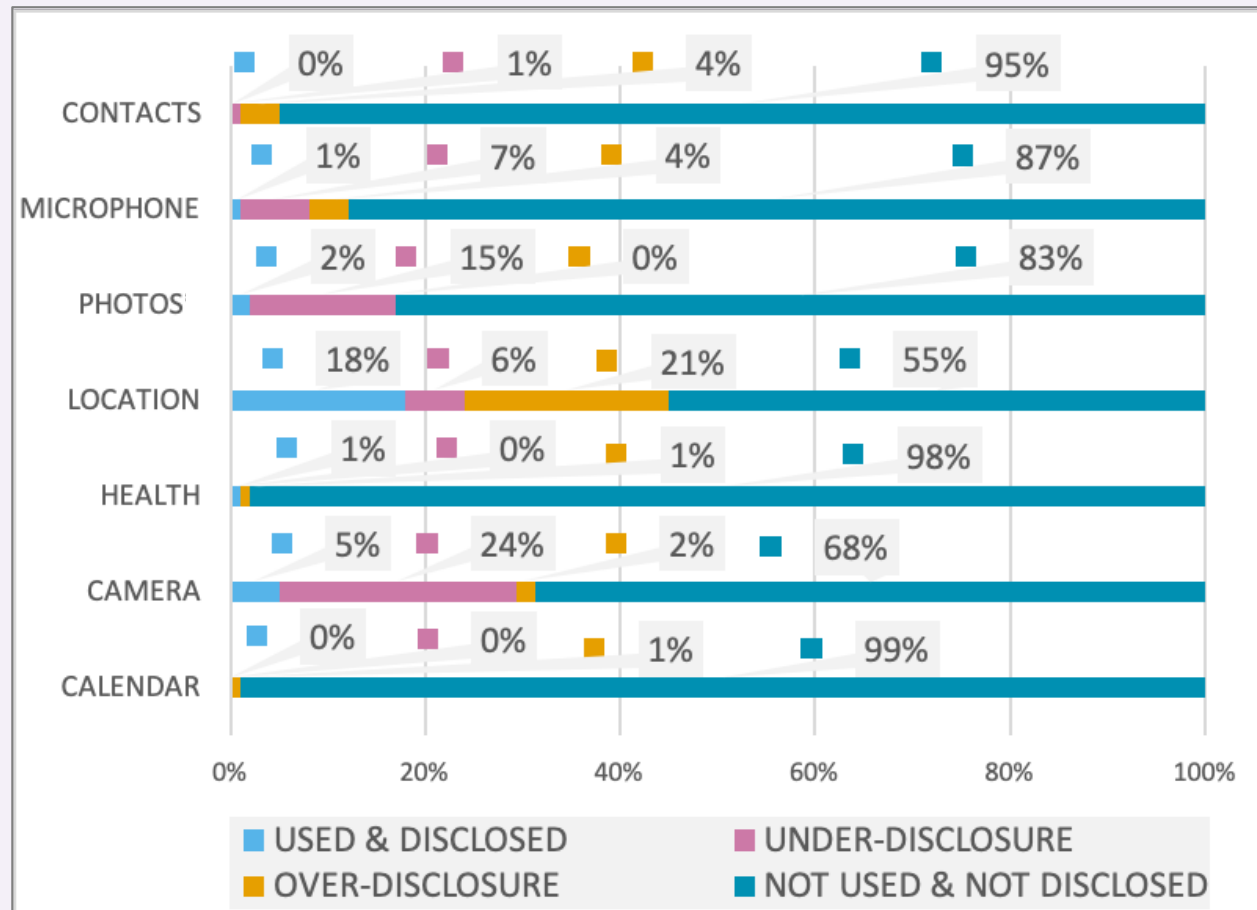
Don't worry! I got you covered. Here is the privacy analysis of your app.



**PrivacyFlash**  
**PRO**

# Current Policy Generators Could Do Better

- Iubenda, TermsFeed, Termly ...
- Completely questionnaire-based
- Generators' compliance with laws sometimes problematic
- Permission use not accurately reflected 🙅
- Library use not accurately reflected

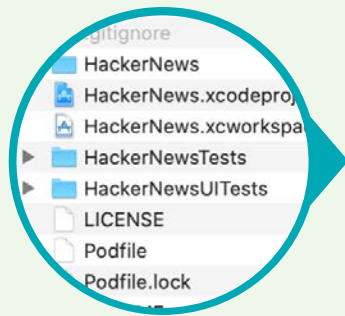


# PrivacyFlash Pro (PFP) Automates Policy Creation



## PrivacyFlash Pro

- Browser-based desktop app
- Python, JS, ...
- <https://github.com/privacy-tech-lab/privacyflash-pro>



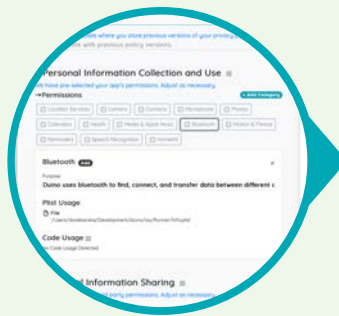
## Static Code Analysis

- Analyze Swift source code and (un)compiled third party libraries
- Data is processed locally



## API Identification

- Identifies privacy practices using PLIST permission strings and other evidence contained in spec



## Questionnaire Wizard

- Fine tune results in a guided wizard that automatically live updates policy as changes are made



## Privacy Policy

- Generates a privacy policy as html file adhering to accessibility requirements

# How Does PFP Work?

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>NSLocationWhenInUseUsageDescription</key>
6   <string>We are using your location to recommend a gym nearby.</string>
```

## A. iOS API Evidence Spec

(1) Plist Permission Strings★

(2) Framework Imports★

(3) Class Instantiations★

(4) Authorization Methods★

(5) Entitlements★  
(only for some privacy practices, e.g., Health)

★ Plist used by 1st and 3rd parties.  
★ Must be all in 1st party files for 1st party practices and in 3rd party files for 3rd party practices. But (6) Additional Evidence suffices in 3rd party files if an Authorization Method is in 1st party files (and vice versa).

```
1 import UIKit
2 import CoreLocation
3 import HealthKit
4 import HomeKit
5
6 class WorkoutViewController: UIViewController, CLLocationManagerDelegate,
7
8   @IBOutlet weak var gymDistance: UILabel!
9   @IBOutlet weak var recommendedGym: UILabel!
10  @IBOutlet weak var workoutTable: UITableView!
11  var workout = [String]()
12
13  let locationManager = CLLocationManager()
14  let healthKitStore = HKHealthStore()
15
16  let homeManager = HMHomeManager()
17  var homes: [HMHome] = []
18
19  override func viewDidLoad() {
20    super.viewDidLoad()
21
22    workoutTable.backgroundColor = UIColor.lightGray
23    workoutTable.separatorColor = UIColor.blue
24
25    self.locationManager.requestAlwaysAuthorization()
```

## B. Signature Detection in App and Library Files

## Privacy Policy for the Workout With Friends App

Last updated: 05/02/2020  
Previous [versions](#)

We are the developers of Workout With Friends. This privacy policy describes how we process your personal information and which privacy rights you have when you are using Workout With Friends. Please contact us at the contact information [below](#) if you have any questions or comments.

1. [Personal Information Collection and Use](#)
2. [Personal Information Sharing](#)
3. [Tracking Technologies](#)
4. [Social Logins](#)
5. [In-app Purchase Information](#)
6. [Children's Personal Information](#)
7. [How Long We Keep Your Personal Information](#)
8. [How We Protect Your Personal Information](#)
9. [Policy Changes](#)
10. [Accessibility](#)
11. [Contact Us](#)

## C. Privacy Policy Generation

### 1. Personal Information Collection and Use

If you grant Workout With Friends permission, we may collect and use personal information from you as follows.

#### • Location Services

Purpose: We are using your location to recommend a gym nearby.



# PFP is "awesome"

## Privacy Laws

PrivacyFlash Pro generates privacy policies based on the following laws.

- California Consumer Privacy Act (CCPA)
- California Online Privacy Protection Act (CalOPPA)
- Children Online Privacy Protection Act (COPPA)
- General Data Protection Regulation (GDPR)

### 1. Privacy Laws

#### California Consumer Privacy Act (CCPA)

Section 1798.110

a. A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

**ProTip:** Select tracking technologies, adjust as necessary.

Adjust your app's and third parties' use of tracking technologies and their purposes.\* Common tracking technologies are advertising identifiers, IP addresses, device identifiers (e.g., MAC addresses), cookies, and user agent strings (which can be used for device fingerprinting).

**Identifier For Advertising (IDFA)**  
In addition to the use of tracking technologies, this section of the policy should also clarify your app's response to Do-Not-Track (DNT) signals. The California Online Privacy Protection Act (CalOPPA) requires such statement. By default, native apps are not responsive to DNT signals.

- ☒ Tracking technology used in your app and included in the policy
- ☐ Tracking technology not used in your app and excluded from the policy

\* Purposes are required.

### 2. Tooltips

2. Personal Information Sharing

We have pre-selected third party permissions. Adjust as necessary.

→Third Parties

☒ AdColony

+ Add Third Party

→Permissions -- All Third Parties

☐ Location Services ☐ Camera ☐ Contacts ☐ Microphone ☐ Photos

☒ Calendars ☐ Health ☐ Media & Apple Music ☐ Bluetooth

☐ Motion & Fitness ☐ Reminders ☐ Speech Recognition ☐ HomeKit

3. Tracking Technologies

We have pre-selected tracking technologies. Adjust as necessary.

→Tracking Technologies

☒ Identifier For Advertising (IDFA) ☐ Cookies ☐ Device Identifier

+ Add Tracking Technology

Identifier For Advertising (IDFA)

First Party Usage **Add**

Purpose

We use this technology to...

Third Party Usage

You may add new third parties at the beginning of Section 2.

Dark Mode

New Analysis **Export Policy** **Privacy Laws** **1.**



*DEMO-TIME*



## 0. Let's Go ...

Firefox

[Firefox.com/previous-privacy-policy](https://www.firefox.com/previous-privacy-policy)

→Permissions

Location Services Camera Contacts Microphone **Photos**

Calendars Health Media & Apple Music Bluetooth

Motion & Fitness Reminders Speech Recognition HomeKit

→ Third Parties

☒ KIF
 ☒ A-Star
 ☒ SwiftKeychainWrapper
 ☒ GCDWebServer
 ☒ SwiftyJSON

1. Personal Information Collection and Use
2. Personal Information Sharing
3. Tracking Technologies
4. Social Logins
5. In-app Purchase Information
6. Privacy Rights of California Residents
7. Privacy Rights of Users in the European Economic Area
8. Children's Personal Information
9. How Long We Keep Your Personal Information
10. How We Protect Your Personal Information
11. Policy Changes

If you grant Firefox permission, we may collect and use personal information from you as follows.



# How Well Does PFP Work?

Permission Category	True Positives	False Positives	False Negatives
Bluetooth	2	0	0
Calendars	4	0	0
Camera	15	0	2
Contacts	3	0	1
Health	0	0	0
HomeKit	0	0	0
Location	21	0	0
Microphone	1	0	0
Motion & Fitness	0	0	0
Media & Apple Music	2	0	1
Photos	14	0	1
Reminders	0	0	1
Speech Recognition	0	0	0
Sum	62	0	6

TABLE V: Detection of permission uses for the 40 apps analyzed by the participants in our usability study (first and third party uses combined). With 62 true positives and 6 false negatives the analysis achieves a precision of 1 and recall of 0.91 for an F-1 score of 0.95.

Tested on:

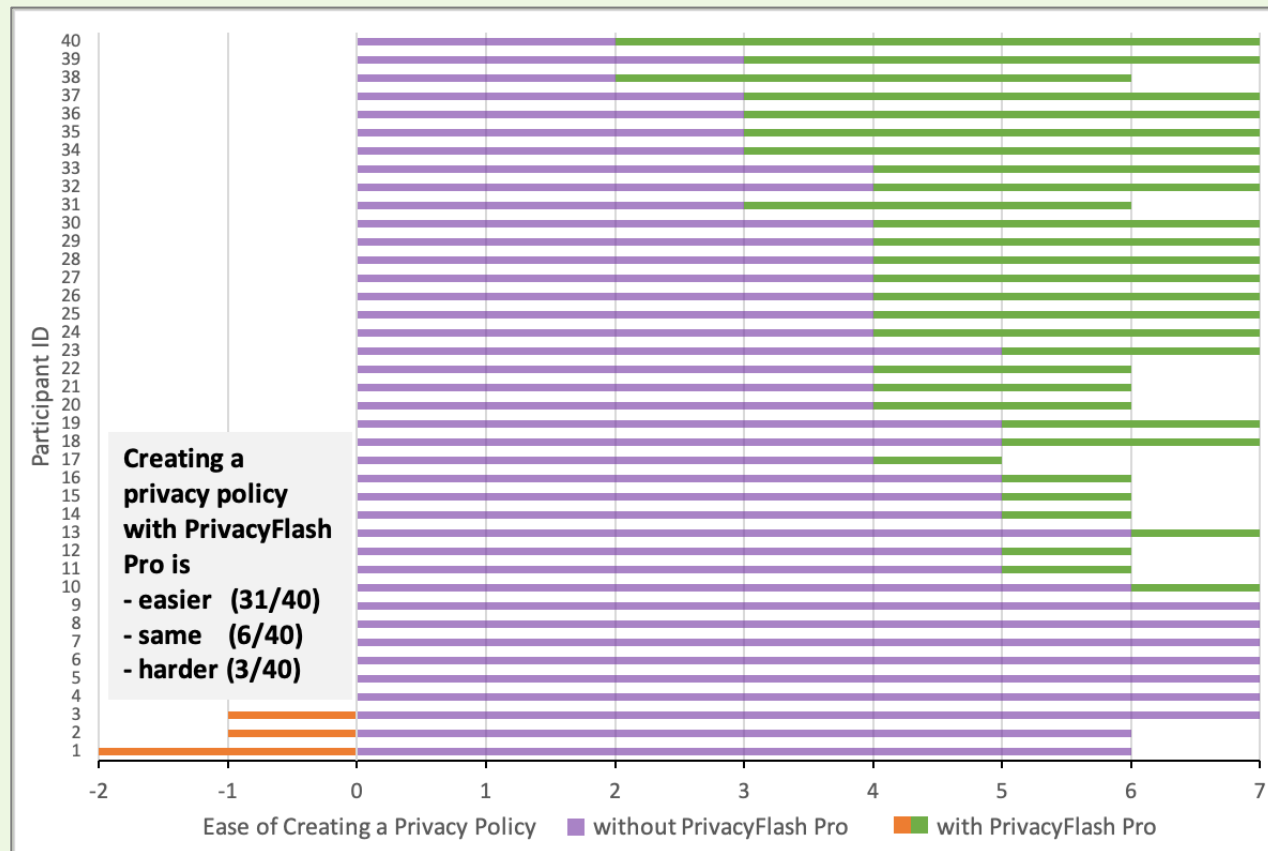
- Our own app
- 10 open source apps
- 40 apps from iOS developers who reported results to us (Tables V and VI)

Third Party Code	True Positives	False Positives	False Negatives
Libraries	525	0	1
Facebook Login	9	0	2
Google Login	6	0	3

TABLE VI: Detection of third party libraries, Facebook Login, and Google Login.

# Use by Developers

- Usability study with 40 iOS developers
- Most developers find creating a policy with PFP is easier compared to their previous method of creating a policy 🙌
- Net Promoter Score: “How likely is it that you would recommend PrivacyFlash Pro to a friend or colleague?” → 42.5



# The Big Picture

- The behavior of software has an impact in the real world  
→ privacy policies for transparency and as a legal safeguard
- How can developers become better at creating privacy policies? → establish policy generation as a native extension of the software development process



# Main Takeaways

- Automate privacy policy generation for iOS apps with PrivacyFlash Pro
  - Extension to other platforms beyond iOS and “nutrition labels”
  - Integrate privacy policy creation into software development
  - Thank you! Questions?
- 
- Our code: <https://github.com/privacy-tech-lab/privacyflash-pro>
  - Our lab: <https://www.privacytechlab.org/>

