Developing and Implementing a Privacy Protection Protocol for Mobile Devices

Valentino Calderon[1], Manjap Singh[2], Nathaniel Good[3], Ashkan Soltani[3], Adam Miller[3]
[1]Berkeley City College, [2]University of California Berkeley, [3]California Department of Justice
2013 Transfer-to-Excellence Research Experiences for Undergraduates Program (TTE REU Program)

Abstract

Governmental regulation of an industry is needed to mitigate fraud and manipulation within a business. In the mobile device industry, data collection, or collecting personal information on a user, plays a major role in the online economy. Given the potential privacy issues of data collection, the California Department of Justice has been placing mobile app developers under scrutiny. In order to enforce federal and state privacy polices, a man-in-the-middle proxy is used to intercept and record the data collected from mobile app developers.

Background

Mobile Applications and Advertisements:

Direct Purchases: Making a purchase directly through an internet advertisement.
Impressions: Exposure to an internet advertisement that influences our behavior over time.
Data Collection: Collecting personal information on a user to establish a distinctive advertising profile for personalized advertising or advertising analytics.

Federal and State Policies:

Children's Online Privacy Protection Act: A Federal Policy that pertains to the online collecting of personal information from persons under the age of thirteen.
•Requires Parental Consent
•Must provide a notice disclosing: (1) All collecting entities (2) Types of information collected (3) How the information is used

California Online Privacy Protection Act: A State Policy that requires online services that collect personal information from California residents to conspicuously post and comply with their privacy policy.

Types of Personally Identifiable Information:
•First & last name
•Physical address
•E-mail address
•Telephone number
•Social Security Number
•Information maintained in a personally identifiable form
- Geo-location
- Facebook IDs
- Device Identifiers (UDID, ODIN, MAC Address, etc.)

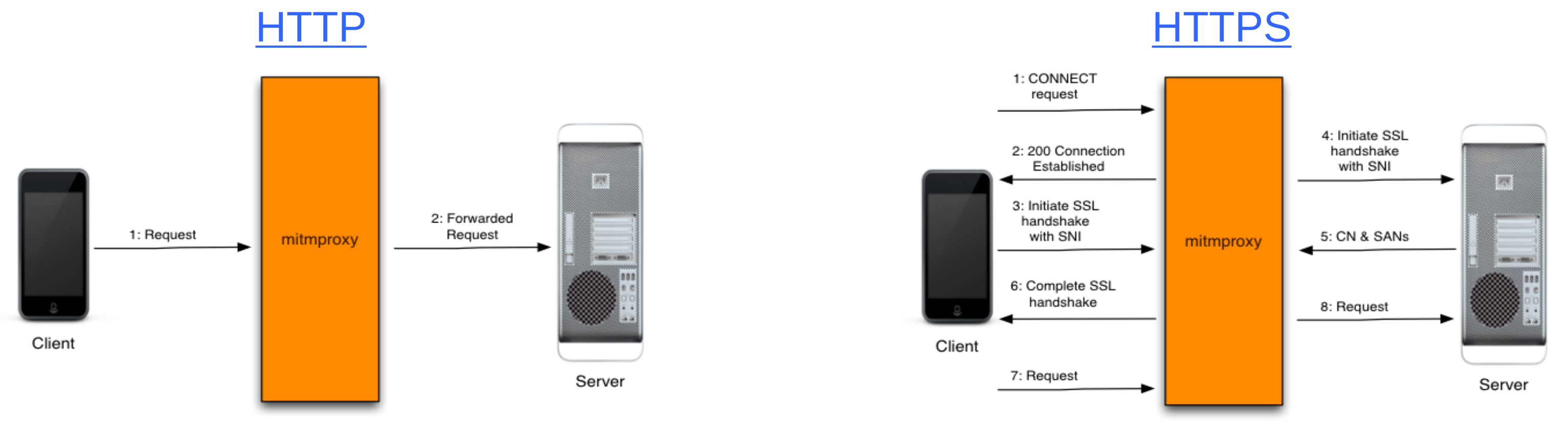
Objective

The objective of my research is to develop and implement a protocol to intercept and record data collected from mobile app developers, and then compare that information with the company's privacy policy.

Tools

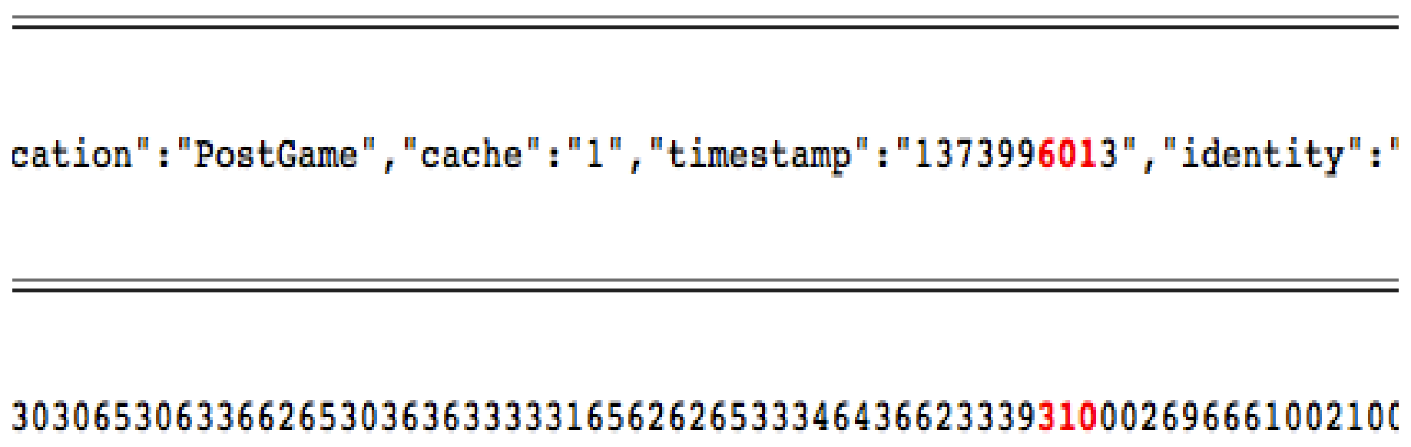
MITM Proxy: An interactive, SSL-capable man-in-the-middle proxy for HTTP with a console interface.

Features:
•Intercept HTTP requests and responses (with the ability to modify them on the fly).
•Save complete HTTP conversations and save them for later replay and analysis.
•Generate SSL certificates on the fly.



Canaries: Variables set equal to potential PII, Personally Identifiable information, to flag personal information going over the wire

Optimization:
•Refining the set of canaries through trial-and-error to produce less false positives
•Determining the proper syntax to identify specific pieces of information
- Date-of-Birth Example: *yyyymmdd* vs. *mmddyy* vs. Epoch Time



```
cation":"PostGame","cache":"1","timestamp":"1373996013","identity":"
```

```
303065306336626530363633333165626265333464366233393100026966610021OC
```

Stages of Testing

Pre-Testing:

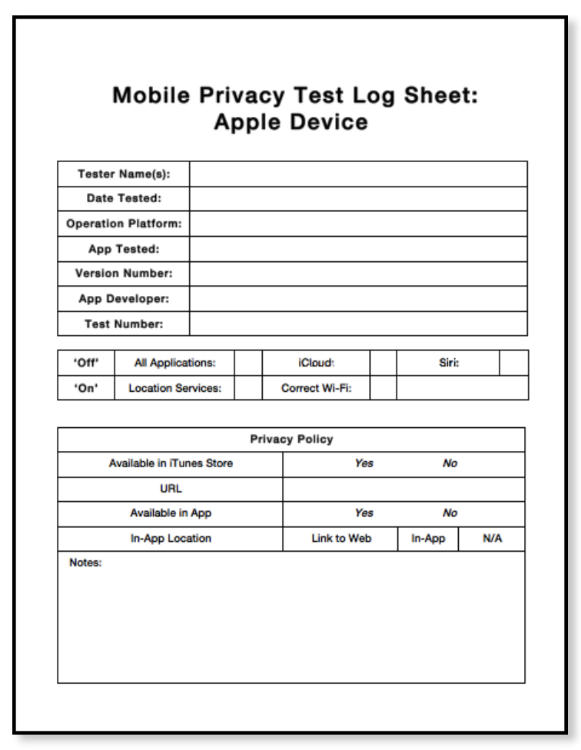
- Note the status and location of the app developer's privacy policy, both in-store and in-app.
- Isolate the intercepted traffic flow by shutting down the programs running down in the background.
- Establish a strong connection between a computer providing a Wi-Fi airport and the mobile testing device.

Pre-Testing Alterations

- Discontinued logging the test on a physical copy

Pros:
- Provided additional copies
- Easier notes & organization

Cons:
- Significantly slowed down the testing process



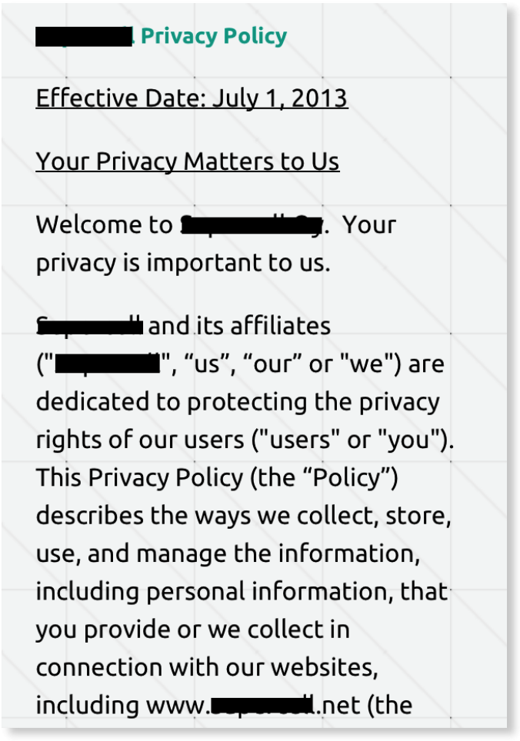
Mobile Privacy Test Log Sheet: Apple Device

Tester Name(s):	
Date Tested:	
Operation Platform:	
App Tested:	
Version Number:	
App Developer:	
Test Number:	

'Off'	All Applications:		iCloud:		Siri:		
'On'	Location Services:		Correct Wi-Fi:				

Privacy Policy			
Available in iTunes Store	*Yes*	*No*	
URL			
Available in App	*Yes*	*No*	
In-App Location	Link to Web	In-App	N/A

Notes:



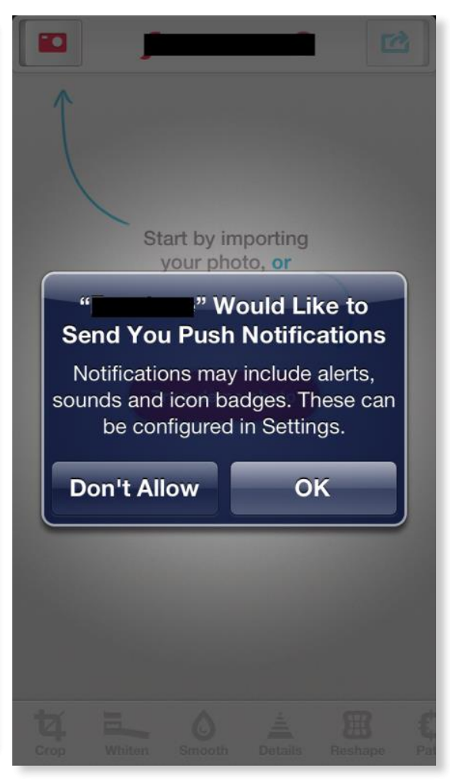
[redacted] Privacy Policy

Effective Date: July 1, 2013

Your Privacy Matters to Us

Welcome to [redacted]. Your privacy is important to us.

[redacted] and its affiliates ("[redacted]", "us", "our" or "we") are dedicated to protecting the privacy rights of our users ("users" or "you"). This Privacy Policy (the "Policy") describes the ways we collect, store, use, and manage the information, including personal information, that you provide or we collect in connection with our websites, including www.[redacted].net (the



[redacted]

Start by importing your photo, or

"[redacted]" Would Like to Send You Push Notifications

Notifications may include alerts, sounds and icon badges. These can be configured in Settings.

Testing:

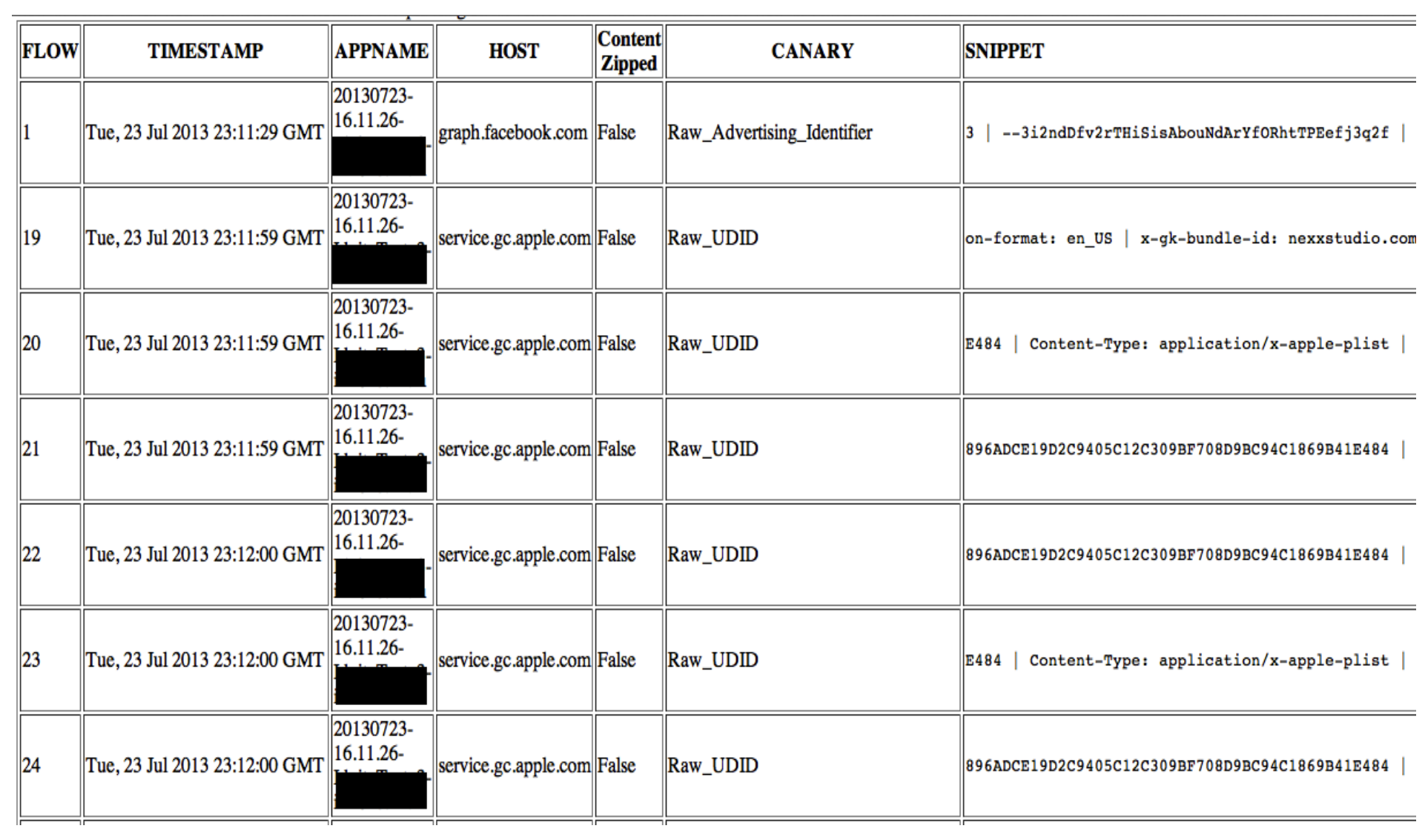
- Run the capture program on the computer, and then start the desired mobile application.
- Accept and screenshot all "Allow Access" queries from the mobile application.
- Explore all accessible pages on the application.

Testing Issues

- Not pragmatic to run tests over extended periods of time
- Does not catch all traffic going over the wire

Post-Testing:

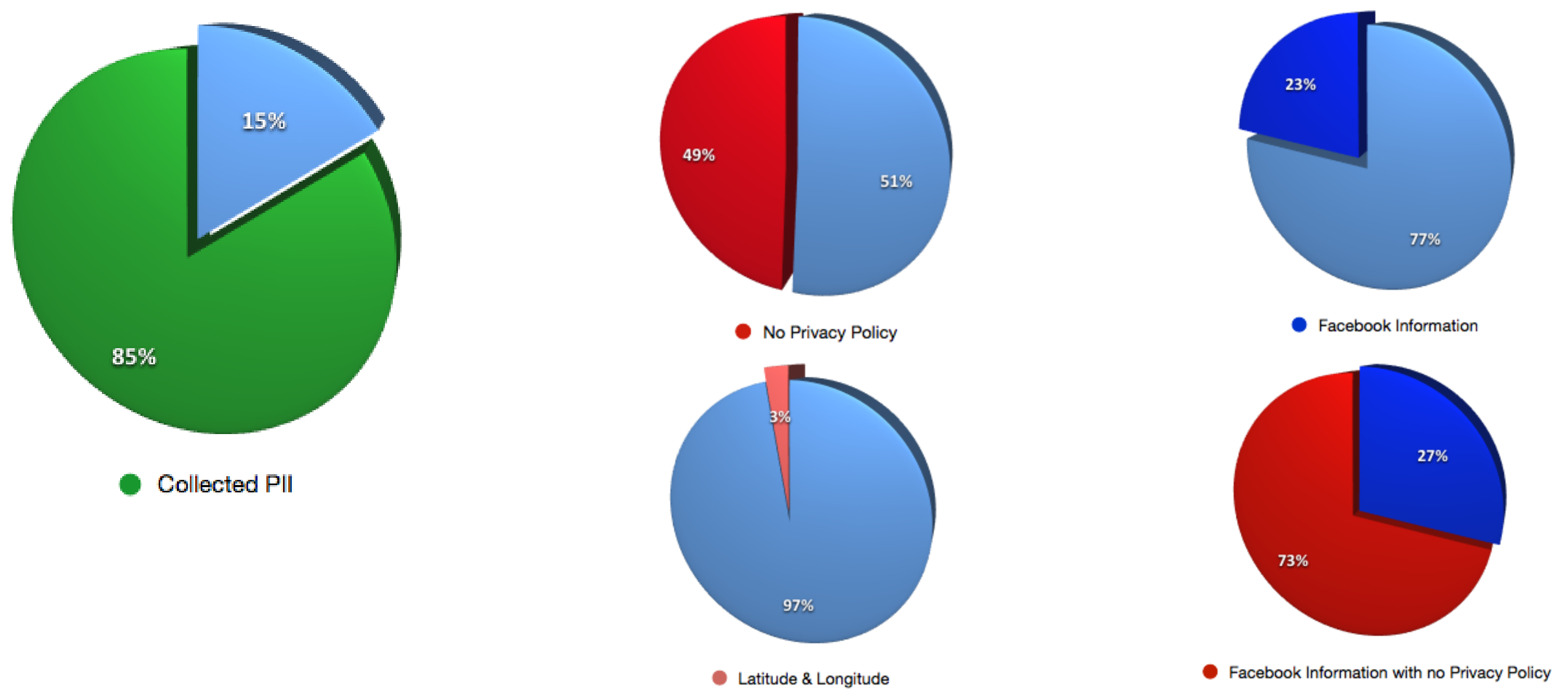
- Log all information into a secure database.
- Generate an HTML file that formats the canaries into a readable structure.
- Compare the data gathered 'over the wire' with the app developer's privacy policy claims.
- If the developer is violating any federal or state privacy laws, take appropriate action.



FLOW	TIMESTAMP	APPNAME	HOST	Content Zipped	CANARY	SNIPPET
1	Tue, 23 Jul 2013 23:11:29 GMT	20130723-16.11.26-[redacted]	graph.facebook.com	False	Raw_Advertising_Identifier	3 | --3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f |
19	Tue, 23 Jul 2013 23:11:59 GMT	20130723-16.11.26-[redacted]	service.gc.apple.com	False	Raw_UDID	on-format: en_US | x-gk-bundle-id: nexxstudio.com
20	Tue, 23 Jul 2013 23:11:59 GMT	20130723-16.11.26-[redacted]	service.gc.apple.com	False	Raw_UDID	E484 | Content-Type: application/x-apple-plist |
21	Tue, 23 Jul 2013 23:11:59 GMT	20130723-16.11.26-[redacted]	service.gc.apple.com	False	Raw_UDID	896ADCE19D2C9405C12C309BF708D9BC94C1869B41E484 |
22	Tue, 23 Jul 2013 23:12:00 GMT	20130723-16.11.26-[redacted]	service.gc.apple.com	False	Raw_UDID	896ADCE19D2C9405C12C309BF708D9BC94C1869B41E484 |
23	Tue, 23 Jul 2013 23:12:00 GMT	20130723-16.11.26-[redacted]	service.gc.apple.com	False	Raw_UDID	E484 | Content-Type: application/x-apple-plist |
24	Tue, 23 Jul 2013 23:12:00 GMT	20130723-16.11.26-[redacted]	service.gc.apple.com	False	Raw_UDID	896ADCE19D2C9405C12C309BF708D9BC94C1869B41E484 |

Data

Due to proprietary reasons, I am not legally allowed to disclose all of the data and results acquired from implementing this procedure



Acknowledgements

I would like acknowledge my supervisor, Adam Miller, my two mentors, Ashakan Soltani and Nathaniel Good, for providing me with the necessary support and structure to develop this protocol, and Sharnnia Artis and Aimee Tabor for giving me this opportunity to have a research experience.

Contact Information

valentino.a.calderon@gmail.com
+1 (714) 330 8801

Support Information

This work was funded by National Science Foundation Award ECCS-0939514 & ECCS-1157089.