# Toward a Better Privacy on Surfing in the Internet

**Department of Computer science, Kean University, Union, NJ**

**By Mohanapriya Logapriyan, Te Wei Lai, Daniel Pareja and Sean Sewell with Dr. Jing-Chiou Liou (Advisor)**

## Introduction

In this project we study current browsers on both standard and private browsing to summarize the difference between the two modes for each browser. Then, we will propose certain criteria and perform a comparison using the criteria on various browsers for private browsing.

## Scope

**Our Concern :**

To protect users from unintentionally revealing privacy information and to raise awareness of the privacey information being retrieved during their Internet surfing. Toward this end, we focus our study on computer browsers, especially on their private browsing feature.

**Browsers under study :**

- Chrome
- Mozilla FireFox
- Safari
- Microsoft Edge

## The Research Team

Sean Sewell, Te Wei Lai, Daniel Pareja, Dr.Jing-Chiou Liou, Mohanapriya Logapriyan

## Test Scenarios

1. Checking the accessibility of information entered on a web page in private mode but not submitted to that website.
2. Checking the accessibility of private browsing history with the help of proxy.
3. Checking the fact of identity tracking by a service provider via Apple ID while using Iphone/Ipad.
4. Checking the image of Hard Drive for sensitive data after private browsing.
5. Checking the Auto-filling feature of private browsing for listing sensitive data like Account Number, Routing Number etc..
6. Checking the functionality of HSTS cookies towards privacy.

## Approach

1. Sensitive Information is entered in the commercial websites in day to day use but the web page is left without actually submitting the information. Examination on the input data whether it could be captured by the website though it is not actually submitted.
2. Setting up a proxy to investigate the range of accessibility in case of private browsing mode.
3. Browsing commercial websites and viewing the products offered without any purchase or adding it to cart. Examining the way of capturing our interested products and tracking the way of respective personalization emails. Thereby concluding whether our Apple Identity is used for the same/not.
4. Investigation is to be carried on with the forensic tool, OSForensics over the hard-drive image acquired after private browsing.
5. Fake website is designed spoofing the sensitive information like credit-card details or personal identification information entered in today's commercial and non-commercial website. Checking whether the data entered in original websites are listed as auto-fill options for this fake site. If so, first case comes into picture, where data might be captured by a (fake or original) website without actually being submitted.
6. Hidden input tags, each containing a single value, one value set by browser's dimension to pixel ratio, another by browser version, etc. are considered. These bit values within the HTML become a fingerprint unique to that user. The server can successfully track user through website. We attempt to defeat this by having Javascript locate these HSTS bits, reassign them with random values each time, thus "corrupting" fingerprints.

## Status of our work

Carrying out the above mentioned approach to investigate the behavior of each type of browser in the identified test scenarios.

Brainstorming for better and smart work towards better privacy.