Did I Agree to This? Silent Tracking Through Beacons

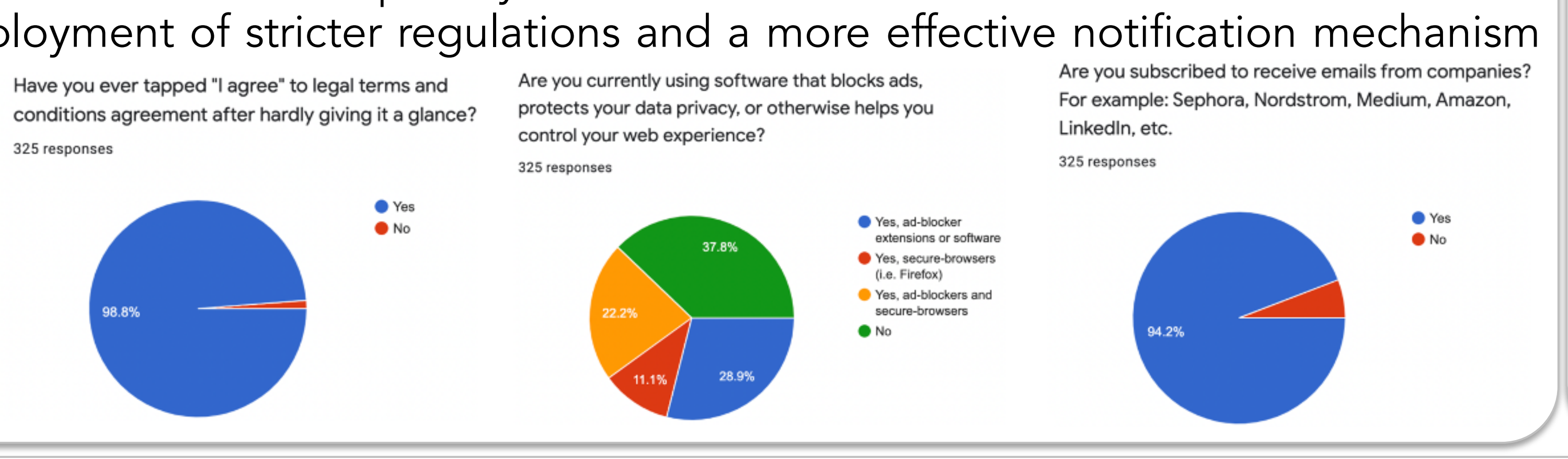
HOFSTRA UNIVERSITY

Edden Kashi

Fred DeMatties School of Engineering and Applied Science

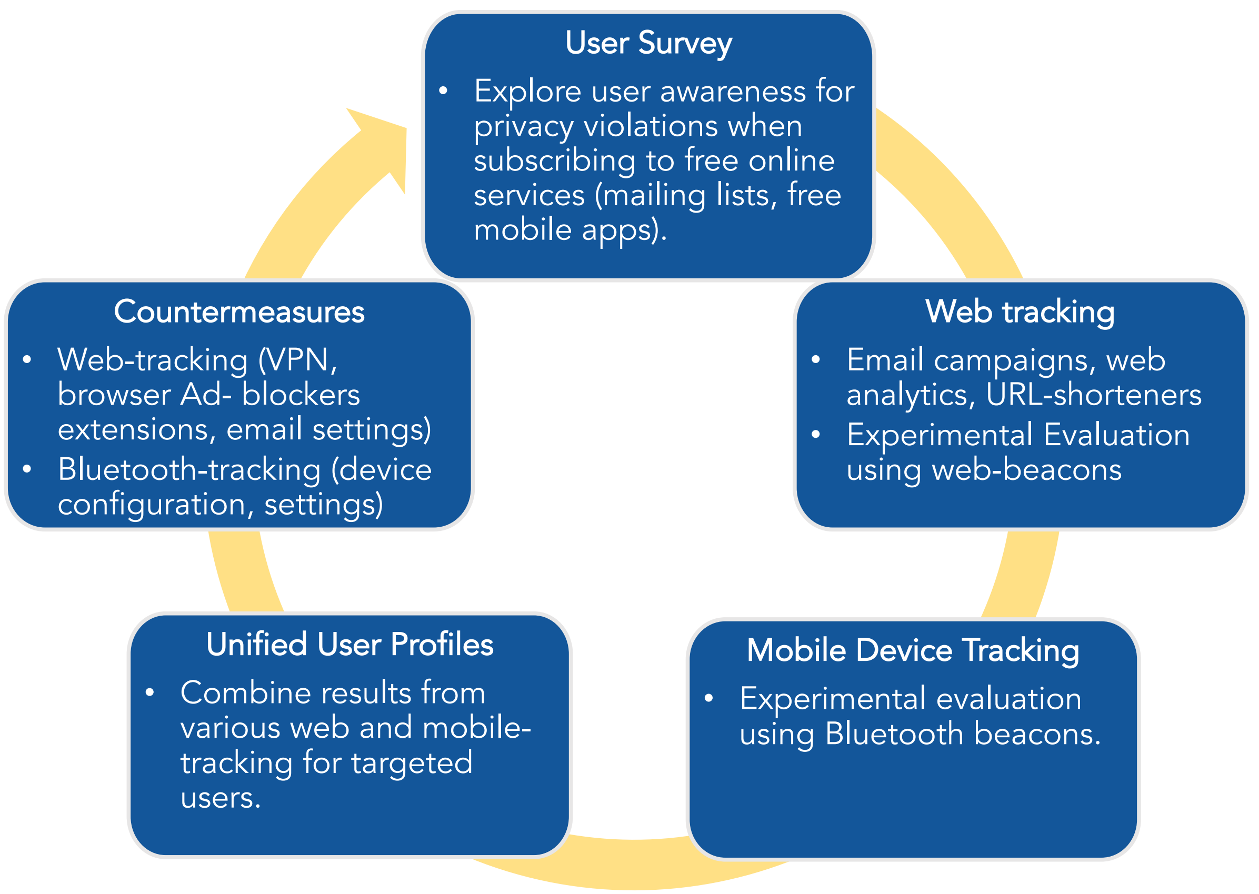
ABSTRACT

Users personally identifiable information (PII) collection is a primary revenue model for the app-economy. Therefore, **user tracking** has become increasingly invasive and ubiquitous. Smart and IoT devices provide even more access to users' personal information by utilizing their *exact location* and *default device settings*. Although users in most cases must grant permission before their personal data is collected and shared with third-parties, this is not the case when user tracking happens through email or just by owning and using Bluetooth dependent devices. In this project, we conducted an experimental evaluation of the most popular user tracking technologies for mobile devices and online user activity and were able to built **unified user profiles** for targeted users from our findings. We hope that our extensive analysis of beacon tracking will lead to greater awareness of the privacy risks involved with web beacons and Bluetooth tracking and motivate the deployment of stricter regulations and a more effective notification mechanism when such tracking is in place.



Figures 1,2,3.
User survey results
(325 participants)

PROJECT OVERVIEW



User Survey
- Explore user awareness for privacy violations when subscribing to free online services (mailing lists, free mobile apps).

Web tracking
- Email campaigns, web analytics, URL-shorteners
- Experimental Evaluation using web-beacons

Mobile Device Tracking
- Experimental evaluation using Bluetooth beacons.

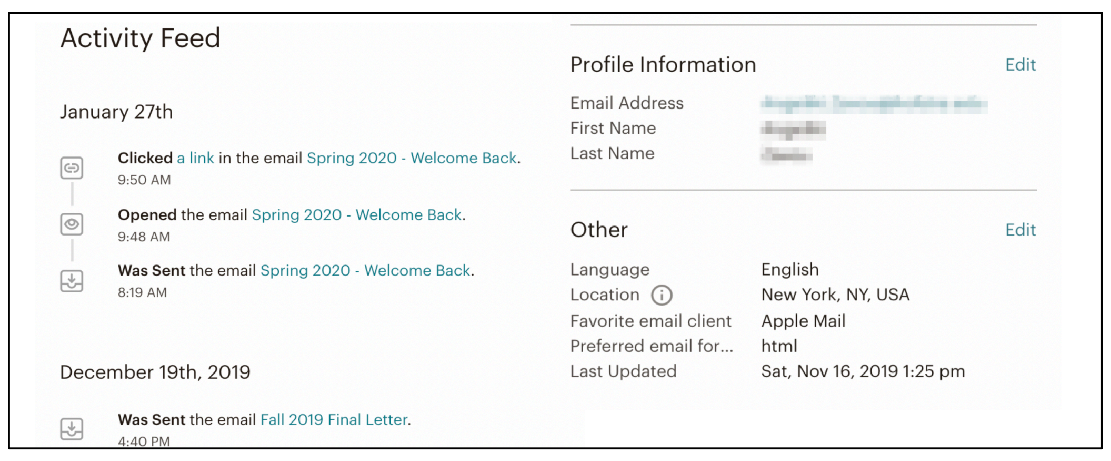
Unified User Profiles
- Combine results from various web and mobile-tracking for targeted users.

Countermeasures
- Web-tracking (VPN, browser Ad- blockers extensions, email settings)
- Bluetooth-tracking (device configuration, settings)

METHODOLOGIES

1. <u>Tracking with Web Beacons</u>
   a. **Email Tracking:** through email extensions (`Streak`, `ContactMonkey`) and CRMs tools (`Mailchimp`)
      - 27 email campaigns for a span of 4 months.
         - Recorded user *engagement* (*i.e.*, the view- and URL-click-rate)
         - Collected device *fingerprinting* data and retrieve the participants' most **frequent** *locations* (*see Figure 4*).

   b. ***URL Shorteners*** (`Grabify, Bitly`) ***& Web Analytics*** (`Google Analytics, StatCounter, Web-Stat`)*:*
      - URL click results in **device fingerprint**.
      - User is redirected to test website monitored by multiple web analytics services (*see Figure 5*).



Activity Feed

January 27th

Clicked a link in the email Spring 2020 - Welcome Back.
9:50 AM

Opened the email Spring 2020 - Welcome Back.
9:48 AM

Was Sent the email Spring 2020 - Welcome Back.
8:19 AM

December 19th, 2019

Was Sent the email Fall 2019 Final Letter.
4:40 PM

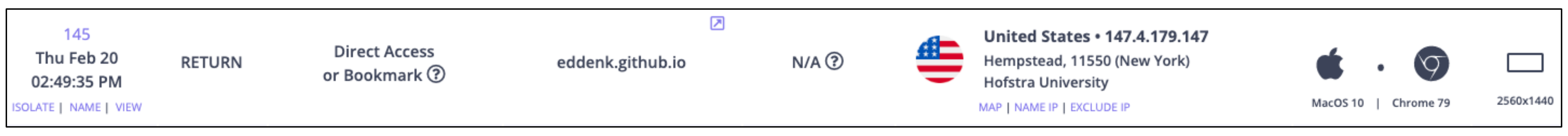
Profile Information Edit

Email Address [redacted]
First Name [redacted]
Last Name [redacted]

Other Edit

Language English
Location ⓘ New York, NY, USA
Favorite email client Apple Mail
Preferred email for... html
Last Updated Sat, Nov 16, 2019 1:25 pm

Figure 4. Mailchimp generated user profile



145
Thu Feb 20
02:49:35 PM
ISOLATE | NAME | VIEW

RETURN

Direct Access or Bookmark ⓘ

eddenk.github.io

N/A ⓘ

United States • 147.4.179.147
Hempstead, 11550 (New York)
Hofstra University
MAP | NAME IP | EXCLUDE IP

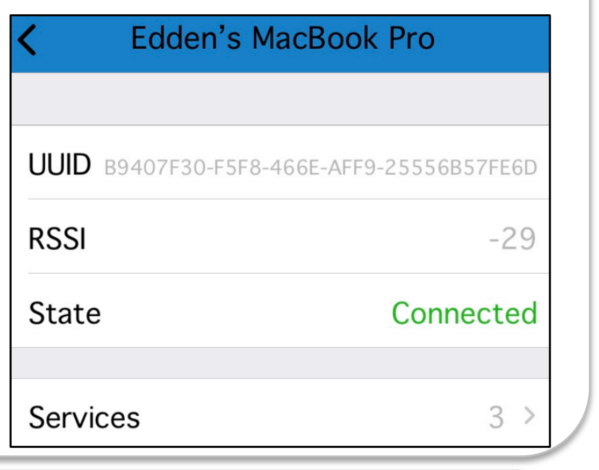
MacOS 10 | Chrome 79

2560x1440

Figure 5. Web-Stat Log

2. <u>Bluetooth Tracking</u>
   a. ***Bluetooth Tracking Applications*** (`BlueCap, NRFConnect`)
      - Identified nearby ***beacons*** and ***Bluetooth-enabled devices*** *(see Figure 6)*.
      - Simulated Bluetooth-enabled devices tracking using Bluetooth Beacons broadcasting our test website URL.

   b. Raspberry Pi Scanner
      - Simulated scanning app and created a ***permanent*** log of ***reoccurring* users**.
      - Identified nearby BLE-, Bluetooth-discoverable, and IoT devices (*i.e.*, fitness watches, wireless headphones, etc.)
         - Based on their ***MAC address** and **device name**,* created a permanent log of every physical appearance for targeted users.



Edden's MacBook Pro

UUID B9407F30-F5F8-466E-AFF9-25556B57FE6D

RSSI -29

State Connected

Services 3 >

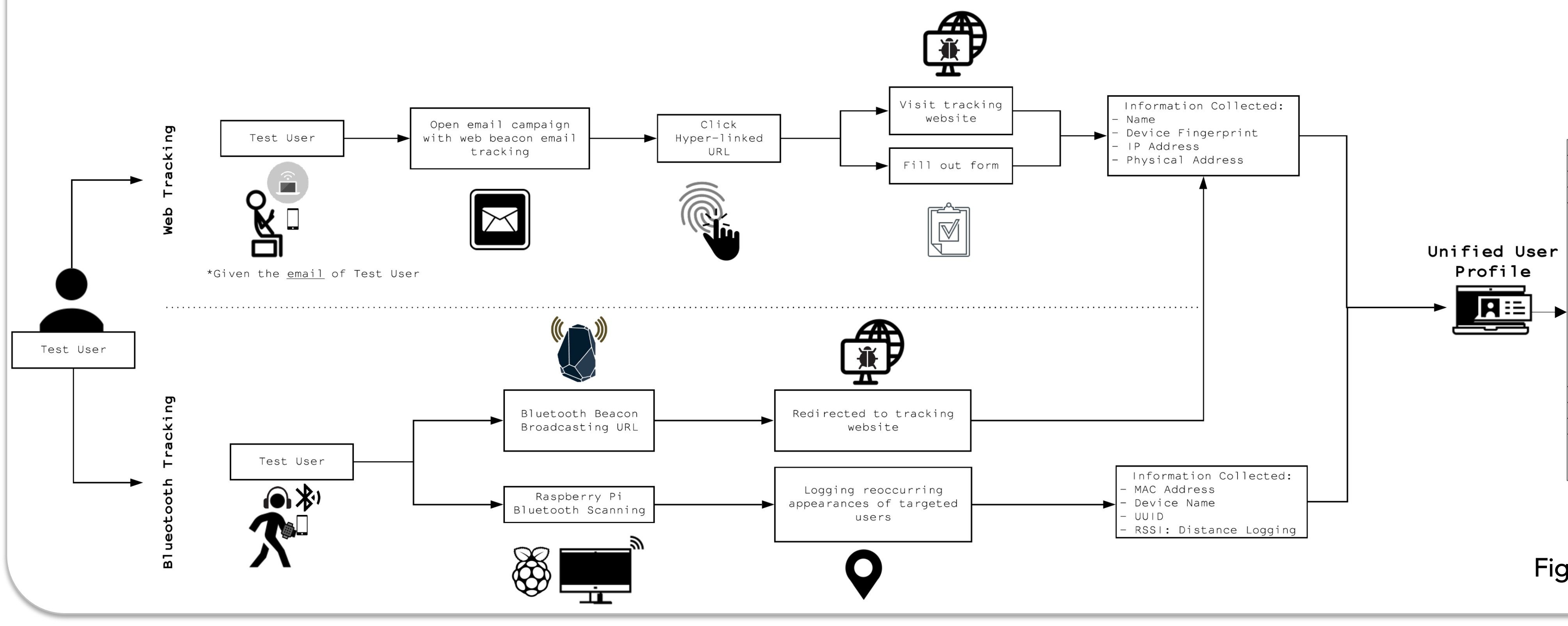
Figure 6.
Blue-Cap Scan

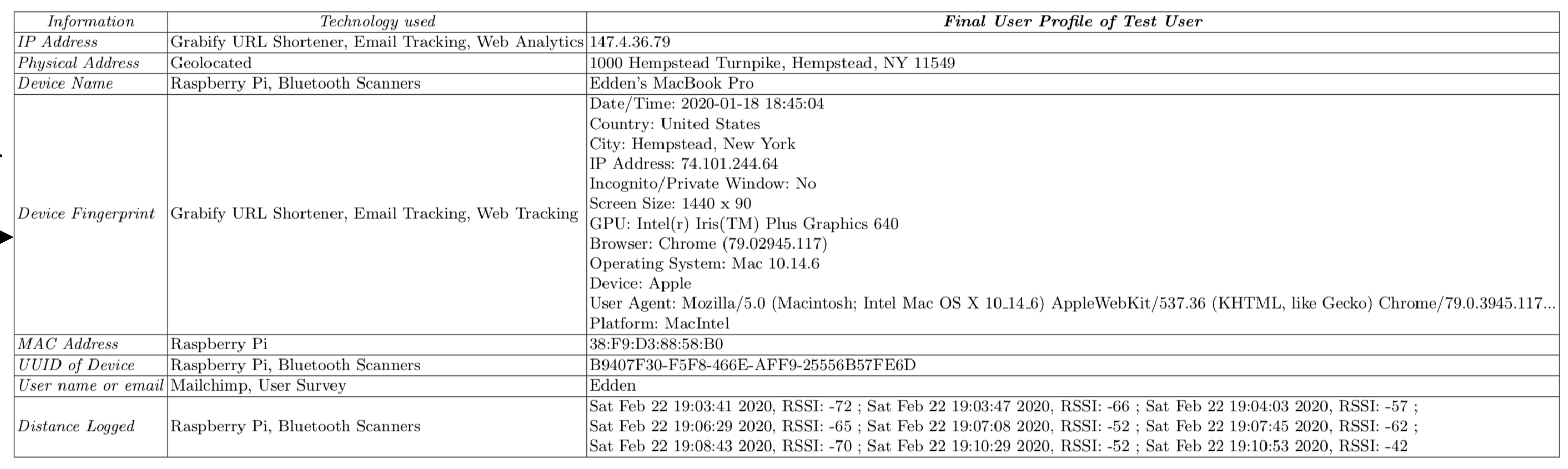
SYSTEM OVERVIEW & RESULTS

Unified User Profiles: built based on findings from the following tracking methods (*see Figure 7*):

1. *Using Web* - targeted users online by tracking the users' email address (subscribed to our mailing campaigns) and online activity.
   a. Tracked every campaign-email opening and conducted logs of targeted users' various devices and physical locations.
      - All 27 campaign emails included web beacons and hyperlinked content using URL-shortener loggers.
   b. Users had to either visit our tracking website or fill out one of the online forms (included in the tracked emails) with their personal information.

2. *Using Bluetooth-Discoverable Devices* - tracking of targeted users through their Bluetooth-enabled devices.
   a. Same result as web tracking through our beacons that are broadcasting our tracking website; so our targeted users don't need to be subscribed to email list.
   b. Kept logs of all **reoccurring appearances** and **timestamp** when the user, or their IoT devices, were within a certain range.





Information	*Technology used*	***Final User Profile of Test User***
IP Address	Grabify URL Shortener, Email Tracking, Web Analytics	147.4.36.79
Physical Address	Geolocated	1000 Hempstead Turnpike, Hempstead, NY 11549
Device Name	Raspberry Pi, Bluetooth Scanners	Edden's MacBook Pro
Device Fingerprint	Grabify URL Shortener, Email Tracking, Web Tracking	Date/Time: 2020-01-18 18:45:04 Country: United States City: Hempstead, New York IP Address: 74.101.244.64 Incognito/Private Window: No Screen Size: 1440 x 90 GPU: Intel(r) Iris(TM) Plus Graphics 640 Browser: Chrome (79.02945.117) Operating System: Mac 10.14.6 Device: Apple User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117... Platform: MacIntel
MAC Address	Raspberry Pi	38:F9:D3:88:58:B0
UUID of Device	Raspberry Pi, Bluetooth Scanners	B9407F30-F5F8-466E-AFF9-25556B57FE6D
User name or email	Mailchimp, User Survey	Edden
Distance Logged	Raspberry Pi, Bluetooth Scanners	Sat Feb 22 19:03:41 2020, RSSI: -72 ; Sat Feb 22 19:03:47 2020, RSSI: -66 ; Sat Feb 22 19:04:03 2020, RSSI: -57 ; Sat Feb 22 19:06:29 2020, RSSI: -65 ; Sat Feb 22 19:07:08 2020, RSSI: -52 ; Sat Feb 22 19:07:45 2020, RSSI: -62 ; Sat Feb 22 19:08:43 2020, RSSI: -70 ; Sat Feb 22 19:10:29 2020, RSSI: -52 ; Sat Feb 22 19:10:53 2020, RSSI: -42

Figures 7,8. Overview of the tracking system and the resulting unified user profile for a single test-subject.

COUNTERMEASURES

- <u>Limiting Web Beacon Tracking:</u>
   - **Block Image Loading**: the only ***permanent*** solution to end tracking via emails. Severely diminishes the quality of campaign emails that users have signed up for.
   - **Pixel Blocking:** web browser extensions (i.e., Trocker, UglyMail, PixelBlock), that **detect**, **notify**, and **block** tracking pixel within emails.
   - **VPN**: link-tracking was successfully bypassed, providing the VPN location, instead of the user location. However, device type, settings, timestamp and number of views were still accurate.
   - **Cookies:** blocking (third-party) cookies on `Google Chrome` and `Firefox`. Successful but unpopular choice by regular users.
   - **Ad-blockers:** Successful against ***widely known* web analytics** (i.e., `Google Analytics, StatCounter`). Unsuccessful against **email trackers**, **URL shorteners, and** `Web-Stat` web analytics platform.
- <u>Limiting Bluetooth Tracking:</u>
   - **Turn off Bluetooth: effective**, but, **unpopular** option for most users, that need Bluetooth for many of their devices (*i.e.*, keyboards, AirPods, …).
   - **Device Renaming**: protection against personal interest tracking. Masks *only* the owner's name.

CONCLUSIONS & FUTURE WORK

Web beacons are used in emails, webpages, and links to track users and retrieve Personally Identifiable Information (PII). Most times this tracking is happening without their knowledge or consent. Bluetooth signals from mobile and IoT devices are used to track and log user activity, like location and device type. In this project, we demonstrated how even *low-skilled* adversaries with inexpensive equipment can successfully achieve tracking of targeted users, violating end-users privacy. And although there are **countermeasures** to limit this constant and invasive tracking, the average end-user neither fully understands the consequences of such tracking, or knows how to activate the said countermeasures on their devices.

Our ***future work*** will focus on the development of user-friendly **notification mechanisms**, for email-campaign tracking, so that the regular user can easily be aware of the extent and the frequency of this tracking in their day-to-day communications. We also plan to build a mobile application for **logging** the use of the **Bluetooth-controller** on mobile-devices so that the privacy-aware owners of smartphones will be able to easily identify the installed applications that are sending out data over Bluetooth so that they can make informed decisions regarding the applications on their device.

ACKNOWLEDGEMENTS

Thank you to my advisor Dr. Angeliki Zavou and Hofstra University for allowing this research to continue!