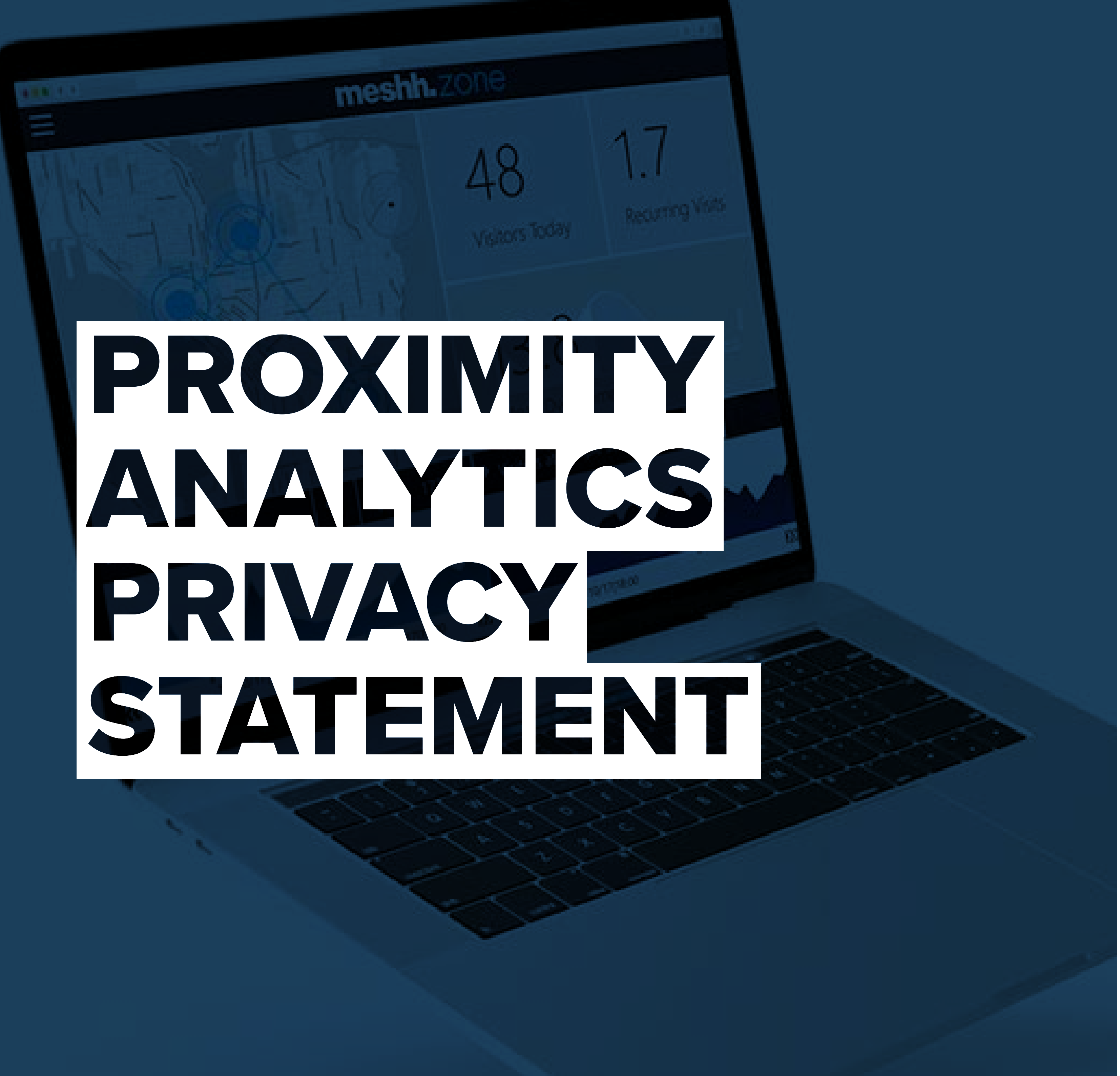
meshh.



PROXIMITY ANALYTICS PRIVACY STATEMENT

Overview

Introduction

Meshh gathers and uses certain limited data about mobile devices.

This process aggregates, processes, stores and analyzes information and shares reports generated out of such analysis with clients to recognize and use consumer behavior and trends in such outlets and locations to make them more consumer centric;

This process involves capturing some data sent by a WiFi enabled device as it probes for available WiFi networks.

This policy describes how this data is collected, handled and processed to meet the company's data protection standards — and where applicable to comply with the law.

We aim to be proactive rather than preventative regarding privacy risks with automatic measures in place that do not require being enabled.

Why this policy exists

This policy ensures Meshh:

- Complies with any relevant data protection law and follows good privacy and security practices
- Protects the rights of customers and partners
- Is open about how it stores and processes device data

Policy scope

This policy applies to:

- Meshh's Proximity Analytics product
- Edge devices using to capture device data
- Cloud based applications that handle or process device data

Meshh Sensors

Meshh uses small portable devices known as Meshh Sensors. These devices can be placed in a space and can see data that is transmitted by WiFi enabled devices when they probe for available WiFi networks.

Please see our Server Security Policy for further details.

Meshh Dashboard

No PII is passed back to the cloud hosted database. All data is aggregated and anonymous, we cannot derive any personal information from the information stored in the Meshh data repository.

Please see our Server Security Policy for further details.

MAC Address Anonymization

A key part of the data transmitted by a mobile device is its MAC Address. When a Meshh sensor sees a device, it carries out the following actions to ensure that the MAC Address is quickly forgotten and removed from the data we collect.

The process can be summarised as:

1. WiFi data, including MAC Address is captured
2. The MAC Address is then immediately one-way hashed
3. The hash is used to replace the MAC Address
4. The MAC Address is discarded and forgotten
5. The WiFi data is then encrypted
6. The encrypted and hashed data is then transmitted to a cloud based application for processing

This whole process takes place in less than a second. It is computationally infeasible to obtain the original data from hashed data and Meshh does not attempt to do so.

The following diagram shows the anonymization process:

WiFi Anonymised Device Tracking

Captured	Anonymised	Encrypted	Received
Type: 80 SensorMAC: a8f7e0009f02 OUI: 34e6ad WLANBSSID: 30b5c2a02de4 WlanSRC: 30b5c2a02de4 MobileDevice MAC: 34e6ade0e03e Signal(HEX): 42 Channel(HEX): 2 SSID(HEX): 67656d61726f6d3130	Type: 80 SensorMAC: a8f7e0009f02 OUI: 34e6ad WLANBSSID: 30b5c2a02de4 WlanSRC: 30b5c2a02de4 MobileDevice MAC: 3a49d-fe94d3c756054f8741581ec-c4b726c4b726c4b8b-5d236d1831921f7f66cc58699 Signal(HEX): 42 Channel(HEX): 2 SSID(HEX): 67656d61726f6d3130	80a8f7e0009f0234e6ad30b5c2a62de430b5c2a62de4349dfe94d3c756054f8741581ecc4b726c4b8b5d236d1831921f7f66cc5869944267656d61726f6d3130	8063c68ba30abe6f0707a7b160edf9f04fe012b3236d55843cc1b701771a7a2fa23f3026135a8e3252968d200fc1677c6c4eac4838bb6ba776b18d2ced182a8a340228b8151166a9c7676780e78ba20ca1c612e3cde0949610f56b9071a99b05dfd9ce8319b0213ff6c02557fe9cce00719cc6e7190bd78caa44158b54401167e3af9147ec0219b8f269417961eda4c8e6409a84da4c9edad1b1be681367bc0
Remove PII (Personal Identifiable Information)		Tamper protection	Secure transmission

Disclosure of data

Meshh will not use/disseminate/disclose such information/data except as outlined in this policy.

Meshh may disclose such data under mandate of law for the purpose of verification of identity or for prevention, detection and investigation including cyber incidents, prosecution and punishment of offences.

Meshh may generate and share publicly periodic reports about consumer trends using aggregated, non-personal data collected by Meshh.

Meshh provides only non-personal data to its clients.

Meshh does not provide identifiable device-specific data to its clients or any third party.

Privacy, Security and Responsibilities

Privacy

MAC Address data is anonymized on our Meshh Sensors, in situ on the client's premises, or at an event. No PII (Personal Identifiable Information) is stored or transmitted.

The anonymized WiFi data is only passed back to Meshh's cloud based applications once it has been fully encrypted.

Meshh's cloud based applications never see any PII data or any MAC Addresses. Only the hashed data is processed and stored.

Meshh provides an opt out form on its website this can be found here – http://meshh.com/optout.html

This form and its functionality can also be incorporated into any 3rd party website or application if requested.

Security

Security has been designed into Meshh's Proximity Analytics as a core component. Please see our Server Security Policy for further details.

MAC Addresses are anonymized in under a second and the remaining data is then immediately encrypted, both when at rest and during transmission.

Responsibilities

Everyone who works for or with Meshh has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.