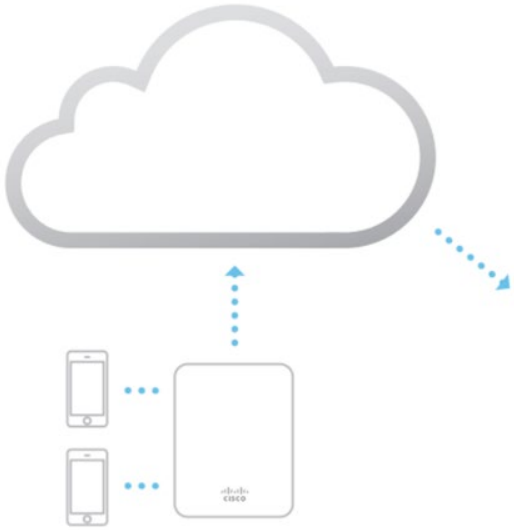
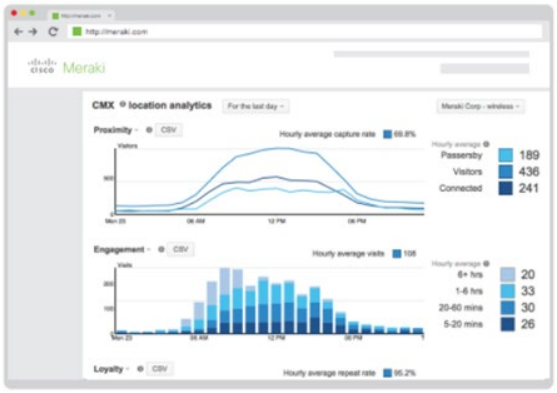
HOW DO LOCATION ANALYTICS WORK?



Probing and associated clients



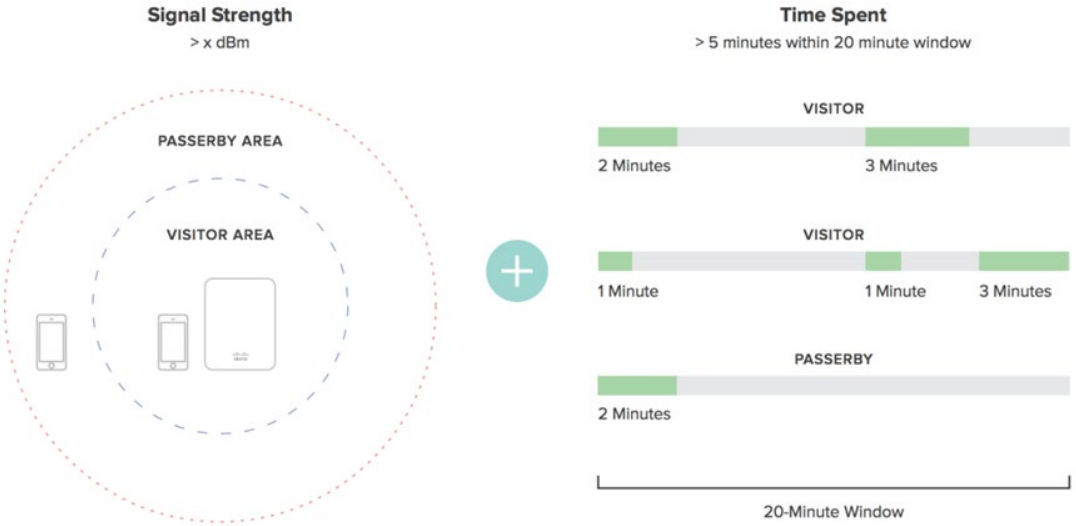
Meraki's CMX Location Analytics

Here is a basic explanation from Cisco:

Smartphones with WiFi can now be used as an indicator of customer presence thanks to a WiFi mechanism that is common across all such devices: **probe requests**. These 802.11 management frames are transmitted at regular intervals from WiFi devices such as smart phones.

The frames contain information that can be used to identify presence, time spent, and repeat visits within range of any WiFi access point. These devices can be detected by WiFi access points **irrespective** of its WiFi association state meaning that **even if a user does not connect his or her device to the wireless network**, the device's presence can still be detected while the device is within range of the network and the device's WiFi antenna is turned on.

Meraki uses probe requests, data frames, and Bluetooth beacon frames to locate and store client location.



What about privacy?

Because the location data contain raw MAC addresses, Meraki implemented a number of security mechanisms to anonymize the data in an irreversible fashion.

Using a unique Meraki algorithm, the Meraki cloud hashes, salts and truncates MAC addresses so that they are not identifiable. The Meraki cloud then stores only that hashed, salted and truncated version of the MAC address. This anonymization process is described in more detail in this document [link]

For more detail on this check out the full document on our website

Can people opt out?

Cisco Meraki's website offers a global opt-out feature that allows users to submit the MAC addresses of their devices, after which the Meraki cloud will no longer detect their MAC addresses either for its built-in Location Analytics views or for real-time export via the Scanning API.

Cisco Meraki also recommends that retailers and others using the Scanning API post notices on the availability of this global opt-out in prominent locations, preferably in the storefront or at building entrances where location detection is taking place.

Source: Cisco Meraki – Location Analytics

If you would like to learn more about Cisco Meraki's location analytics check out the recent webinar that SMART Towns hosted with Cisco on our Youtube channel and subscribe to our newsletter so that you don't miss out on the next session

How do we inform the general public?

While not yet a legal requirement, it is considered good practice to inform the public of any WiFi analytics processing that is happening in the area. Gwynedd and Anglesey use these stickers, which link to the data sharing platform, Patrwm, clearly showing the area covered with links to the privacy policy and terms and conditions. Being transparent about what data is being collected, by whom and for what purpose can help pre-empt citizens' concerns and can help tackle misinformation.

What else can we do to ease concerns?

It is important that information is readily available to members of the public who are concerned about data analytics, as incomplete or misguided information can cause unnecessary problems. Consider compiling a comprehensive list of FAQs for your town or county's digital developments, like this great example from Flintshire.

Community engagement can help ease concerns, this can be through workshops and presentations explaining the benefits of the data, or by distributing data reports to stakeholders.
Gaining the support of a local regeneration or business group can also help to distribute the information and gain support for the program.
If you would like any further advice or support in setting up a workshop get in touch with smarttowns@mentermon.com

What other documents/ policies should be in place?

DPIA: A data protection impact assessment is an essential document for the organisation that is controlling/ processing the data. An example of this document can be found here*
Terms and conditions: Examples of privacy policies and terms and conditions can be found here*

*please note that these examples are for reference and if in doubt you should seek professional advice.

What else do we need to consider?

In this short video from last year's Masterclass series, Ben Hawes, who used to be the Government's lead on Smart Cities, explores some of the responsibilities involved in collecting location data. Including data ethics.

Is this something you would like to discuss further? Is there other information which could be useful? Drop us an email at smarttowns@mentermon.com