Retail Analytics Buyer's Guide

The 7 questions to ask every provider of smartphone-based retail analytics.

To find out more visit www.getblix.com

Brought to you by BLIX

INTRODUCTION

Retail Analytics Buyer's Guide

The 7 questions to ask every provider of smartphone-based retail analytics.

Collecting data from smartphones to measure customer traffic and deliver world-class retail analytics may seem complicated. There are many ways to collect the data, to manage it and report on it - all of which have their pros and cons.

Without needing extensive technical knowledge, this document will help you make sense of how different solutions compare and will quickly assist you to work out what is fact or fiction.

Cut through the tech jargon to easily understand the most important differences between solution providers.

THE QUESTIONS

1. What technology is being used to detect and track smartphones (e.g. WiFi, Bluetooth, Cellular, 3G, 4G, GPS etc.)?
2. If using WiFi, how is MAC randomisation dealt with?
3. Is the positioning of sensors important to data integrity?
4. Is it possible to calibrate a sensor to only measure a particular space or direction?
5. What are the technical specifications of the hardware (e.g. make, model & components)?
6. What are the specifications of the antenna used to collect data (range/power) and is it directional?
7. What monitoring and notifications are provided when a sensor goes offline, and what data is lost?

01 What technology is being used to detect and track smartphones (e.g. WiFi, Bluetooth, Cellular, 4G, GPS etc.)?

WHY IS THIS IMPORTANT

There are several ways to collect data from smartphones in order to provide retail analytics and customer behaviour data - each of which has different accuracy, privacy and legal implications.

To ensure that your company is not on the wrong side of the law and isn't the next feature story on A Current Affair, it's important that you know what technology your solution provider is using and how that technology is viewed by privacy and legal experts.

> **Your business cannot afford to be on the wrong side of privacy and data collection laws.**

TECHNOLOGIES USED TO TRACK SMARTPHONES

Bluetooth

Tracking devices via Bluetooth provides very little value as phones only transmit data in response to 'accepted' devices that have previously been paired.

Summary

- Data quality: very low
- Legality: legal
- Privacy: not PII
- Encryption: low
- **Sample size: 1-5%**
- Cost: <$500/unit

GPS

Involves accessing GPS data from apps installed on the user's phone. Accuracy varies considerably based on source and data is not useful for indoor applications.

Summary

- Data quality: high outdoors, low indoors
- Legality: legal
- Privacy: PII, but opt-in
- Encryption: none
- **Sample size: ~1-20%**
- Cost: $/thousand records

01 What technology is being used to detect and track smartphones (e.g. WiFi, Bluetooth, Cellular, 4G, GPS etc.)?

TECHNOLOGIES USED TO TRACK SMARTPHONES

Passive Cellular, 3G, 4G

Passively 'sniffing' cell phone traffic requires very expensive hardware ($2k-$10k per unit) that can intercept data between the phone and cell tower.

Summary

- Data quality: low
- **Legality: questionable**
- **Privacy: not PII however considered very poor practice by the Office of Australian Information Commissioner**
- Encryption: heavy
- Sample size: 10-20%
- Cost: $2k-$10k/unit

WiFi is by far the best solution for retail analytics - it's legal, doesn't breach privacy and +95% of people have location services or WiFi turned on.

Active Cellular, 3G, 4G

Actively tracking cellular signals involves eavesdropping on mobile phone data (voice, calls, sms etc.) and 'pretending' to be a cell tower.

Summary

- Data quality: very high
- **Legality: requires warrant**
- Privacy: deemed PII
- Encryption: heavy
- Sample size: very low (this method is typically used to target specific devices eg. by AFP/FBI)
- Cost: $2k-$10k/unit

WiFi

Involves 'sniffing' WiFi probes sent by smartphones for location services & WiFi connectivity. MAC randomisation makes this method more challenging.

Summary

- Data quality: high
- Legality: legal
- Privacy: not PII
- Encryption: high
- Sample size: +95%
- Cost: <$1k/unit

02 If using WiFi, how is MAC randomisation dealt with?

WHY THIS IS IMPORTANT

WiFi-based retail analytics solutions cannot ignore MAC randomisation. More than 80% of all WiFi data collected from smartphones has randomised MAC addresses. That means that if 10 customers spend 10 minutes in your store, it is likely that the data collected will have approximately 10 real MAC addresses and 40 fake ones.

Now the question is - do those 40 fake MAC addresses represent 40 smartphones, or do they in fact belong to the original 10 smartphones and customers?

Solution providers will have different solutions to this and results may vary. The most common solution is to simply use the data that contains real MAC addresses as a sample and extrapolate the data from that sample.

> **It is impossible to provide accurate analytics from WiFi without a solution to MAC randomisation.**

MAC RANDOMISATION EXPLAINED

In the last two years, both the Apple iOS and Android operating systems have changed the way smartphones probe in search of WiFi. There are two key changes.

Firstly, the MAC address is often randomised. This means that a single smartphone may send probes with different MAC addresses on a regular basis, making it more difficult to know whether this is a single phone or multiple phones.

Secondly, due to the fact that Apple and Android use WiFi most commonly to locate you (via location services) the probe frequency has increased substantially. This means there is a lot more probe activity over the WiFi radio channels, which is both good (more opportunities to capture data) and bad (more noise).

83.7%

As of October 2019, 83.7% of all WiFi probe data contains a randomised MAC address.

02 If using WiFi, how is MAC randomisation dealt with?

BLIX DELIVERS UNPARALLELED ACCURACY WITH COUNTSMART®

Blix has spent two years developing our proprietary technology, CountSmart®. This new approach to WiFi analytics performs a deep analysis of every packet of smartphone data, irrespective of randomisation and encryption, allowing Blix to make use of 100% of available smartphone data.

In addition to this, AI-based CountSmart® algorithms are able to leverage the Blix Traffic database of more than three billion smartphone interactions to generate a unique identifier for every phone, all while providing complete privacy for the smartphone owner. This ensures we're compliant with all privacy legislation, including GDPR.

The result? Blix Traffic, powered by CountSmart®, is able to provide highly accurate analytics data, which you can confidently use to improve your retail operations.

> **Blix Traffic powered by CountSmart® delivers more accurate analytics.**

Retail CIO Outlook TOP 10 RETAIL ANALYTICS SOLUTION PROVIDERS IN APAC - 2019

In October 2019, Blix was recognised as a Top 10 Retail Analytics Solution Provider by CIO Outlook.

"To scale up the sales in bricks and mortar stores, retailers must master the art of making data-driven decisions… this is where Melbourne-based Blix wields its expertise in the retail sector through and through.

Blixs' proprietary CountSmart® technology delivers the highest level of smartphone tracking accuracy on the market today."

03 Is the positioning of sensors important to data integrity?

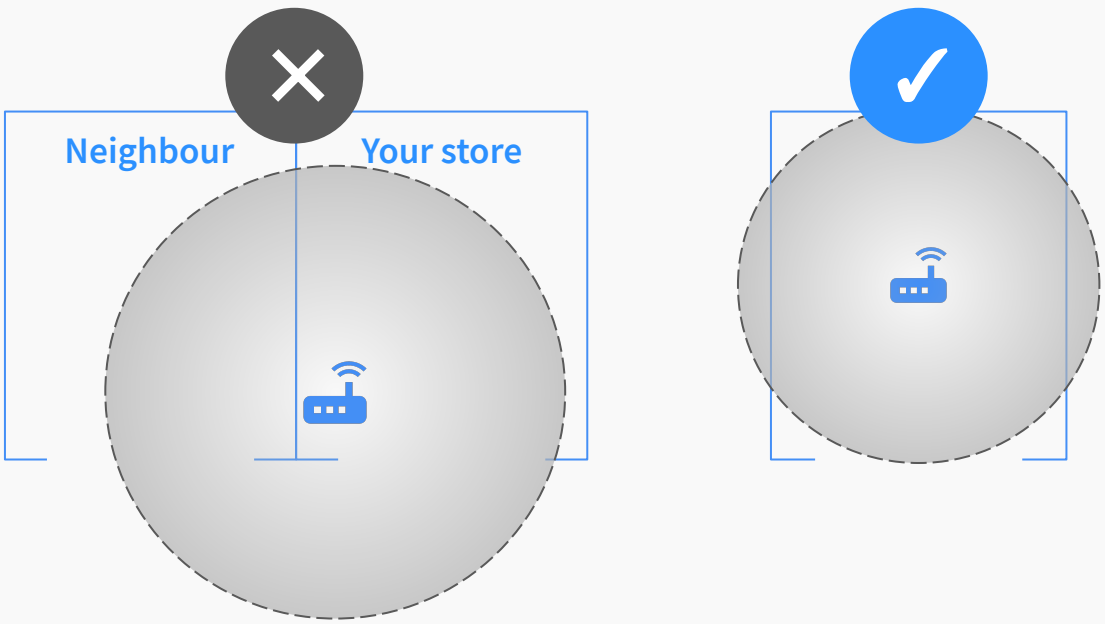
WHY THIS IS IMPORTANT

As explained in question #4, it is not possible to only capture data from one side of the sensor or antenna. WiFi antennas (and all radio-based communication antennas) emit a circular signal around the antenna and device. As such, placement is critical. Installing a sensor on the sidewall of a store will measure the neighbouring store. Likewise, installing the sensor near the front of the store will result in outside traffic being included in store traffic counts.

All radio frequency antennas emit a circular signal which means sensors must be located centrally to avoid measuring the neighbouring store's traffic.

BLIX SENSOR PLACEMENT

Blix uses electricians to install sensors in the centre of the store (this usually requires a ceiling installation) to ensure we only measure customers inside your stores, not the neighbouring stores. This also ensures the devices are not unplugged.

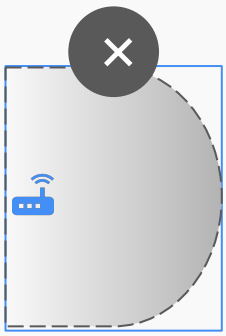


04 Is it possible to calibrate a sensor to only measure a particular space or direction?

WHY THIS IS IMPORTANT

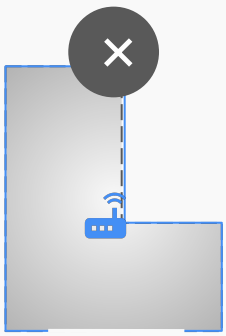
Whilst the capabilities of all sensors and technologies are different, all radio-based frequencies operate in the same way. Understanding what is, and isn't possible with sensor calibration is very important as this will guide your implementation plan in terms of the number of sensors you need and where they should be located.

> **It is not possible to calibrate out the limitations of radio frequency signals and whilst WiFi is amazing at measuring a large space, it cannot accurately measure a very small space such as a change room.**



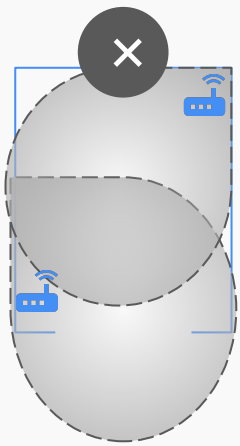
RADIO SIGNALS & CALIBRATION

Further reinforcing why installing sensors in the middle of the store is so critical, it is important to understand the limitations of radio signal (WiFi, Bluetooth, Cellular, 3G, 4G etc.) calibration. Please see Appendix C for more details.



It is not possible to:

- Bend the signal around corners
- Only capture data on one side of a sensor
- Only capture data within one-three metres of a sensor
- Use two sensors installed front and back to accurately measure a store
- Produce heat maps with less than four sensors.



> **The only way to accurately measure a space is to place the sensor in the middle of that space and measure 360° around the sensor.**

05 What are the technical specifications of the hardware (e.g. make, model & components)?

WHY THIS IS IMPORTANT

Regardless of the data being collected (ie. cellular or WiFi) the sensor hardware is how all data is collected, and as such, the quality of hardware and components directly impacts service levels and data quality.

Knowing that your solution provider uses the best possible hardware which is reliable, collects high quality data and provides a very high level of security is paramount.

Cheap hardware and components will collect less data, experience more outages and data losses and require more maintenance.

> **Hardware quality and security will directly impact system stability, data integrity and security.**

BLIX HARDWARE SPECIFICATIONS

Blix hardware is purpose-built by a leading global WiFi hardware manufacturer with quality components, leading chipsets and powerful antennas. The results:

- Reliable hardware (Blix can offer a lifetime warranty!)
- Less sensors needed per store (antenna range is 130m)
- More data captured (powerful antenna and CPU)

All of this adds up to more accurate analytics, more reliable hardware, less outages and happier clients! For detailed specs on the Blix hardware, see Appendix B.

Blix offers the only lifetime warranty on hardware in the industry.

06 What are the technical specifications of the antenna used to collect data (range/power) and is it directional?

WHY THIS IS IMPORTANT

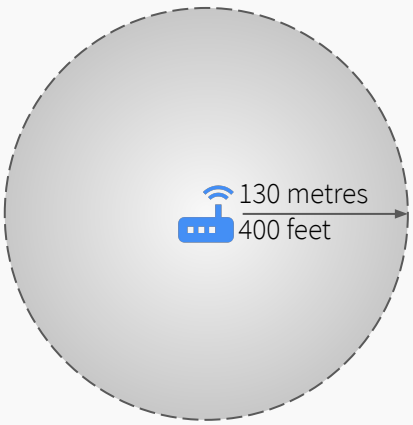
The size, range and power of the antenna directly impact the quality and quantity of data collected, making it paramount that a high quality antenna is used.

A larger (more surface area) antenna will collect more data and provide better analytics, and conversely, a smaller antenna will collect less data and produce lower quality analytics.

The antenna directly impacts how many sensors are needed per store and the quality and quantity of data collected.

THE BLIX ANTENNA

The Blix antenna is approximately 15cm high and has a range of 130m. It will not only measure more of the space outside your store (essential outside traffic trends), but will capture more data overall - this means more accurate analytics all round.



Directional antennas are designed to extend signals large distances and as such do not work in a retail environment.

DIRECTIONAL ANTENNAS

In theory it is possible to use a directional antenna to limit data capture in one direction. In practice however, this does not work because a directional antenna is designed to extend signals in a particular direction, not limit signals in a particular direction entirely (not to mention they are very large and unsightly!).

07 What monitoring and notifications are provided when a sensor goes offline, and what data is lost?

WHY THIS IS IMPORTANT

Sensor outages will happen. The key is minimising the number of outages and their duration. If a sensor goes offline for an hour or two, that isn't likely to have a big impact on reporting. However, if sensors go offline for days at a time, this will impact how teams can use the data operationally and will also result in blanks in year-on-year data.

A system that triggers automated alerts to users will ensure that sensors are back online much faster. Additionally, this kind of system is less likely to engage in the practice of hiding data losses.

> **Automated alerts are essential to reduce the duration of outages and minimise the impact of data losses.**

BLIX OUTAGE & ALERTS SYSTEM

Blix does everything possible to avoid having sensor outages, but they still happen. The most common outages are caused by a 4G outage or a software/firmware issue. In the event of an outage, Blix will adjust the L4L reporting and acknowledge the outage.

Blix provides the following:

- Backup storage - every Blix sensor is capable of storing +two weeks worth of data on the sensor in the event of a 4G outage. When the internet connection is re-established, the sensor simply pushes all the data to the Cloud and there is no reporting data loss.
- Automated alerts - every customer can nominate people to receive alerts of sensor outages via email.

> **Some solution providers will hide data losses by using historical data to fill in the blanks.**

APPENDIX

Let’s get technical

The following appendices provide technical details for your IT team to review.

Some of the answers provided within this document can be further explained and supported with technical information as follows.

Question 1: greater in-depth information about cellular (3G, 4G LTE, GPRS) tracking and how it works.

Question 4: the technical reasons why it’s not possible to accurately measure very small spaces such as change rooms or bargain bins.

Question 5: the technical specifications of the Blix hardware.

Give the following pages to your IT team and feel free to request more details from Blix.

APPENDIX A

CELLULAR TRACKING IN MORE DETAIL

Passive Cellular, 3G, 4G tracking

Passively 'sniffing' cell phone traffic (3G, 4G LTE, GPRS, GSM, voice, SMS and data) involves using a specialised piece of hardware with a software defined antenna which can tune into the correct channels to capture the packets of data flowing between phones and cell towers.

This data is heavily encrypted and can travel over any of 40 radio channels, making it impossible to capture meaningful data because the hardware can only monitor one channel at a time (unless you install 40 hardware units each with their own antenna).

Additionally, the unique identifiers (IMSI/TMSI) are heavily encrypted and rotated, which makes it impossible to know whether the traffic is from one device or many.

Whilst not illegal, this method of tracking is heavily frowned upon by privacy, legal and law enforcement as it involves intercepting sensitive information such as your phone calls and data.

Active Cellular, 3G, 4G tracking

Active cellular tracking (3G, 4G LTE, GPRS, GSM, voice, SMS and data) involves using hardware (e.g. Stingray) that pretends to be a cell tower and essentially 'tricks' smartphones into connecting to it, instead of an actual tower.

This method of tracking is illegal in most countries and is mostly used by government and security agencies to intercept mobile signals for listening and locating. In Australia and the United States, a warrant is required to actively track cellular signals.

More information

Here are some helpful links for more information on cellular tracking: IMSI-catcher on Wikipedia, IMSI treated as 'personal information' by Australian Privacy Commissioner.

APPENDIX B

BLIX HARDWARE SPECIFICATIONS

Blix hardware is purpose-built by a leading global WiFi hardware manufacturer with quality components, leading chipsets and powerful antennas. The results:

- Reliable hardware (Blix can offer a lifetime warranty!)
- Less sensors needed per store (antenna range is 130m)
- More data captured (powerful antenna and CPU)

All of this adds up to more accurate analytics, more reliable hardware, less outages and happier clients!

CPU	Atheros AR9331, @400MHz
Memory / Storage	DDR 64MB / FLASH 16MG
Interfaces	1 WAN, 1 LAN, 1 USB 2.0, 1 micro USB (power), SIM card slot, MicroSD card slot, Antenna SAM mount holes
Frequency	2.4GHz
Transmission Rate	150Mbps
Max Tx Power	18dBm
Protocol	801.11 b/g/n
Power	Input 5V/2A, Consumption <3W
Dimension, Weight	105mm x 72mm x 27mm, 170g
SSID	N/A
Mode	Monitor Mode Only - RFMON
Firmware	Hardened OpenWRT (non-essential services disabled). Egress local firewall - accepts no inbound connections.
Data Transmission	HTTPS utilising secure versions of TLS over a 4G connection
File Verification	MD5 Hash checksum
Device Authentication	S3 Secret to establish identify and SSL connection
Server Encryption	AWS S3 Server-side encryption enabled
MAC Hash	MD5 with salting

APPENDIX C

RADIO SIGNALS & CALIBRATION LIMITATIONS

Using radio frequency signals (i.e. WiFi, Bluetooth, Cellular, 3G, 4G etc.) to measure very small spaces presents a number of challenges. Passively tracking cellular, 3G and 4G via intercepting phone signals as they move to the cell tower simply isn't accurate enough to measure small spaces such as a retail store because the cell towers may be many kilometres away.

WiFi also presents challenges, outlined below. Bluetooth is the only technology which is capable of measuring very small spaces, however, unless your customers all have your mobile app installed on their phone, the sample size of customers will be less than 5%.

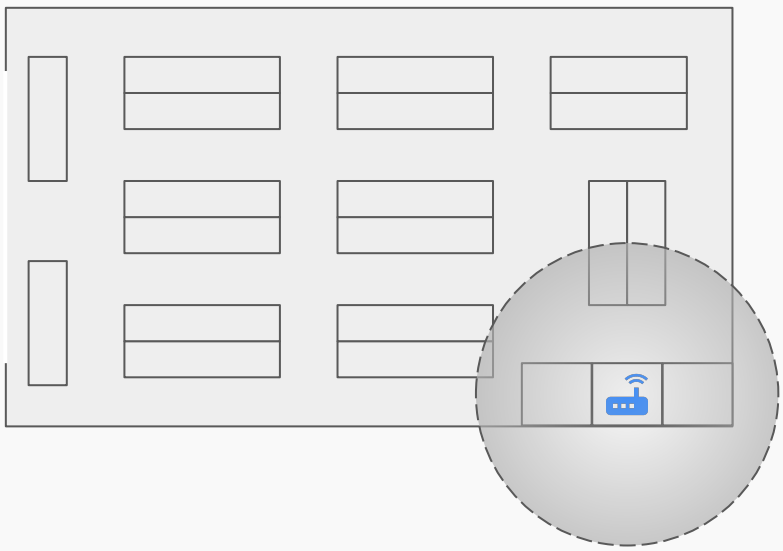
The only technology that can accurately measure a very small space is Bluetooth.

MEASURING SMALL SPACES SUCH AS CHANGE ROOMS

WiFi is amazing at measuring a large space (depending on the power of the antenna), however it cannot accurately measure a very small space such as a change room.

The reason is a technical one. WiFi uses the signal strength of a smartphone to determine its distance from a sensor. Once a phone is within 5m of a WiFi sensor, the signal strength reading does not change very much. Therefore, even if you place a sensor in the middle of the changerooms, you will still be measuring a much bigger space, including the neighbouring store as shown in the image below.

Blix only recommends measuring changeroom conversion when you have a reasonably large changeroom area, otherwise the data will be inaccurate.



ABOUT BLIX

Leading the way in retail analytics

Founded in 2013, Blix was born out of the realisation that bricks and mortar retailers needed greater insight into customer behaviour - simple counts through a door were not enough to compete with the online world.

Visit: **www.getblix.com**

Email: **hello@getblix.com**

Retail CIO Outlook TOP 10 RETAIL ANALYTICS SOLUTION PROVIDERS IN APAC - 2019

MARKETSANDMARKETS

Blix recognised as the most 'Dynamic Differentiator" in the 2019 Global WiFi Analytics Report.