# MEXIA Interactive
# Privacy Policy/Protocols
# Data Collection/Algorithm Process

Mexia Interactive has taken the industry of people counting to a new, higher level. We have done this by replacing what has been done for years through door cameras, video cameras, IR devices and other ways to provide retailers and other companies with information about how many people visit a location and when, with a technology platform that provides better insight for companies, and better experiences for consumers.

Although some media reports have stated that companies such as Mexia and our clients are 'spying' on consumers, nothing could be further from what the reality is. Although is creates great headlines, the substance of the story is not based on complete information, complete accuracy of facts or in-depth knowledge of the technology.

**Mexia Interactive takes privacy of consumers seriously**. So seriously that we have set new industry standards when it comes to data encryption, data collection procedures, access and more. We have taken these steps because we want consumers to be certain that although the technology is not in place to track individuals or gather personal information, the perception is such that it might be, and we want to provide additional levels of encryption and data handling to provide the industries leading privacy protocols. We also want to make certain that Mexia clients are assured that they are working with the leading company in the industry not only with our technology platform, but in overly protecting their customers privacy concerns.

At the core of the Mexia Analytics Platform, is our proprietary software that collects only non-personal information. There is nothing collected that could be used to determine who an individual is or access any type of personal information on a mobile device such as a phone number, email, passwords, name, address, etc. Our highly developed platform only collects an anonymous set of numbers that only relate to essentially a serial number of a piece of hardware. Although this piece of 'hardware' in this case is a mobile device that a person carries, and this may seem personal, when this number is encrypted and added into a pot of millions of other numbers to be reported as a group or 'aggregated', it becomes completely irrelevant to a 'person' or the movements of a specific device at all.

All personal information related to a device is stored directly on a SIM card or hard drive, and there is technologically no way for the Mexia Analytics Platform to access this information. There is absolutely no connection between a MAC address and a SIM card, so there is not a way that even if a company wanted to, they could access, view, collect or see any personal information. At the same time, there is never any communication between a MAC address and a SIM card on a mobile device. This adds in a level of assurance and security that at no time is there a possibility of an error being made and some personal data being seen or collected “by mistake”.

Mexia Interactive has a comprehensive Privacy Policy and set of Protocols that we and our clients follow in order to ensure that as consumers, your privacy is protected, your private information, individual shopping patterns and habits are not used, collected or analyzed and no data collected or links created through any data collection are used to identify you as an individual in any way. Essentially, we view individuals as anonymous dots. It is these dots that help us create reports for our clients to create better layouts, more pleasing designs and help consumers get through queue lines faster, move throughout stores, malls and airports better or have an better viewing experience at an outdoor concert or event. Although as a consumer, you may initially feel queasy about how this might work, but when you go to a store or mall and see new products you have before, see areas where there are promotions that you may be interested in and get through the checkout faster- the benefits are apparent. If you are at an outdoor event and notice that lines move faster or viewing screens are in areas they were not before, you will benefit from knowing that organizers used our anonymous and aggregated data to create this better experience. And if you just don’t want to be part of any of it, you can opt out with a simple scan of a QR code or log in to a mobile site, register your MAC address and we will ensure that when you enter a location that our sensors are placed, your ‘dot’ is not included in the array of dots and any data related to such dot movements are gone from our records permanently.

**Data Collection/Algorithm Process**

This document outlines the detail as to the collection, handling, storage and use of data within the Mexia Business Intelligence Platform.

1) Mobile devices enter a location where Mexia Pinpoint Pro (MPP) sensors are located.
2) The MPP passively and in the background listens for a signal coming from mobile devices’ Bluetooth  or WiFI ‘ping or callout’ in proximity to our Sensor. Mobile devices with Bluetooth or WiFi turned on are searching for Bluetooth or WiFi devices or items to connect to. At no time do our Sensors attempt to connect back or create any type of ‘handshake’ with a mobile device.
3) The MPP detects the ‘ping or callout’ from the device, at which time the MPP registers the Bluetooth, WiFI or MAC address as well as the date, time, signal strength and device manufacturer/category (Samsung, Nokia, Apple, Blackberry, etc). There is no information related to a person included in any of these items.
4) This MAC address is immediately hashed (SHA-2) and sent to our off-site data server via a secure connection and additionally encrypted with a HEX Code to the highest standards in the industry. The encryption consists of assigning a unique non-sequential identification number to the MAC address. The raw MAC address

is then deleted from the Mexia server. The unique identifier is the only reference to the mobile device that now exists. It is important to also note that this process cannot in any way be reverse engineered.

5) The new ID code is then added to the other ID codes, essentially into a bucket where it is combined with all other ID's, and aggregated or grouped patterns are determined and reported on.
6) The data warehouse server, with only aggregated data, hosts the aggregated and encrypted data. Mexia houses all data with a third-party hosting company that is a leader in data security.
7) When visualization of the data is required by clients, the data warehouse is queried in order to report on the specific business objectives of clients such as number of visitors during specific hours of the day, how long customers stayed in a store, and what departments were the most popular on specific day.

## The Mexia Data Encryption standard

Mexia hashes all data to a SHA-2 level in order to be up to date, and in most cases well ahead, of the overall data encryption systems implemented within our industry.

Below is a description from Wikipedia that explains SHA-2:

**SHA-2** is a set of cryptographic hash functions (**SHA-224, SHA-256, SHA-384, SHA-512**) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. A hash function is an algorithm that transforms (hashes) an arbitrary set of data elements, such as a text file, into a single fixed length value (the hash). The computed hash value may then be used to verify the integrity of copies of the original data without providing any means to derive said original data. This irreversibility means that a hash value may be freely distributed or stored, as it is used for comparative purposes only. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.

The security provided by a hashing algorithm is entirely dependent upon its ability to produce a unique value for any specific set of data. When a hash function produces the same hash value for two different sets of data then a collision is said to occur. Collision raises the possibility that an attacker may be able to computationally craft sets of data which provide access to information secured by the hashed values of pass codes or to alter computer data files in a fashion that would not change the resulting hash value and would thereby escape detection. A strong hash function is one that is resistant to such computational attacks. A weak hash function is one where a computational approach to producing collisions is believed to be possible. A broken hash function is one where a computational method for producing collisions is known to exist.

In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable.[2] Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2.

The NIST hash function competition selected a new hash function, SHA-3, in 2012.[3] The SHA-3 algorithm is not derived from SHA-2.

Below is an explanation of a MAC address from Wikipedia, which helps to explain that although a mobile device may have a MAC address, it does not, and can not, contain any personally identifiable information. In combination with the SHA-2 hash that Mexia undertakes, we go to great lengths to ensure consumers information is private, and our clients can get the data and analytics that help them manage their business.

A **media access control address** (**MAC address**) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmwaremechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the **burned-in address**. It may also be known as an **Ethernet hardware address** (**EHA**), **hardware address** or **physical address**. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is a SOHO router, for which the ISP grants access to only one MAC address (used previously to inserting the router) so the router must use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.

A network node may have multiple NICs and each must have one unique MAC address per NIC.

MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64. The IEEE claims trademarks on the names EUI-48 and EUI-64, in which EUI is an abbreviation for *Extended Unique Identifier*.

**Important Notes:**

1) No information that Mexia collects is shared with anyone other than our direct clients who also, through our contracts, agree that the data or reports cannot be shared outside of their organization.
2) Mexia will not sell the results of specific client data or a combination of client data to outside third parties.
3) Mexia does not combine data or reporting from multiple clients to create any type of profile of consumers outside of specific client locations.

4) Mexia uses Rackspace, who is the best in class for data managing, security, etc for the collection, aggregation, storage and report generation for our clients and Mexia's data. At no time is any data from one client combined with data from another client on our servers.
5) All data collected is stored only on servers within the USA. No outside agencies of any kind have access to any data Mexia collects, stores or reports on. No data is removed from these servers and stored on an outside server outside of our private cloud network at Rackspace.
6) At no time is any data stored on a Mexia sensor device. As soon as the data is registered, it is securely transmitted to the servers at Rackspace where it is encrypted and then stored on the Mexia servers. No raw data is stored on a sensor or server.

Mexia understands that consumers have the right to privacy when they are shopping, travelling, etc. Our technology was not designed to 'spy' on consumers, it was developed because brick-and-mortar retailers, airports, municipalities and others want to create a great consumer experience to attract more customers and provide great customer service. Our technology is the leading platform for clients to do this, which is why they choose Mexia. We ensure that we provide extra assurances to consumers to protect your rights of privacy, and a platform that our clients can use to provide great experiences.

For further information about Mexia and/or our Privacy Protocols, please contact Glenn Tinley, President at glenn@mexia.ca

## *Why doesn't Mexia capture cellular signals?*

1) What is an IMSI/TIMSI and why doesn't Mexia use these signals as part of its platform?
   a. A TIMSI (Temporary International Mobile Subscriber Indentity is a pseudo-random number generated from the IMSI number of a mobile device.
   b. An IMSI as defined by Wikipedia is: *The **International mobile Subscriber Identity** or **IMSI** /ˈɪmziː/ is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the home location register* (HLR) *or as locally copied in the visitor location register. To prevent eavesdroppers identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly generated TMSI is sent instead.*

The reason that Mexia does not develop our platform to collect information from the TIMSI/IMSI is due to:

a) Privacy concerns: because the original IMSI is generated as part of the cellular system, therefore attached to the SIM card, there is potentially a way to hack a TIMSI while being transmitted and potentially gather private or personal information. This goes completely against what the FTC and multiple privacy concerned US Senators have been working with Mexia and others on in terms of a Code of Conduct and other items related to consumer privacy. Additionally, here is a link that describes an IMSI-catcher and the concerns behind it in terms of privacy, security and other issues. It is our belief that companies using this technology will have difficulty receiving any endorsement form the FTC due to the multiple privacy concerns related to it. As mentioned in this link, the use of IMSI catchers in many countries is illegal.
*http://en.wikipedia.org/wiki/IMSI-catcher*

b) The generation of an IMSI/TIMSI is random, unpredictable and 'rarely sent'. This translates into inaccuracy in terms of determining location. It also does not provide for the consistency that a high level system would require to provide reliable and repeatable reporting.