Glimpse

Glimpse Audience Analysis Platform

Privacy & Security Information – *as of January 2021*

Glimpse is registered with the DOP Network of the Data Protection Commission with Shane O'Sullivan as the Data Protection Officer.

Glimpse does not share client data with any third parties. Glimpse relies on Private Amazon Web Services Servers for processing and storage. Glimpse relies on a secure data carrier connection and authentication tokens for the transfer of data. Glimpse retains the right to use pseudonymised data collected from clients for the maintenance, software improvements and for the creation, improvement, and sale of new products.

GDPR & Privacy

Consumer privacy and anonymisation is a core concept of Glimpse in all of our technology. Our software has been designed as a visitor analyses tool by means of completely anonymous meta-data measurements. Glimpse's software uses advanced facial detection algorithms, **not facial recognition**. Meaning that no individual can ever be identified by our software. Audience data is generated from accumulated measurements of passers-by. Glimpse software never collects any information that is uniquely associated to an individual. Demographic and engagement information is purely assessed from visual cues. All image processing is performed in real-time, meaning no image is ever stored.

No individual can be identified, either in absolute terms (full identity) or in terms of repeated exposures (e.g. recognising that someone was at a sequence of different locations or visited the same location twice). Glimpse software can only determine an anonymous visitor's demographic characteristics, their movement and if they are engaging with a given interest point.

Glimpse does not store any personal data; it only stores anonymous meta-data that describes the size and demographics of an audience. Under the new GDPR

framework, Glimpse is actively GDPR compliant by operating through its privacy-by-design approach.

Stored Information

Glimpse sensors detect:

- Hashed MAC device address
- Estimated age range
- Estimated gender
- Accessories Present (glasses, etc.)
- Facial hair present
- Facial poses (roll, yaw, pitch)
- Head/eye positioning
- Dwell time
- Shopper Movement
- Shopper Engagement

Glimpse Security Implementations

General Security Protocol

Using Glimpse Security Protocol authentication method, no product keys or organisation identifiers exist on the device, that is all coordinated by an administrator on the client server where the display and organisation details are kept.

Security Breach Planning

The most plausible security breach would be a physical theft of a Glimpse device. A breach in this way could see an unauthorised individual do the following:

- Run their own images through Glimpse and get the results.
    - An alarm is automatically raised when obscure requests are made from any device or if a connected display is in a strange state causing us to identify that something is not working correctly. This ranges from:
        - Too many requests to the Glimpse server
        - Too few requests
        - An unexpected change in lighting or image quality
        - If the display is offline for several minutes at a time
        - If the display is turned on and off more than would be expected

- Potentially view the last few minutes of Glimpse demographic anonymised data (if the underlying network is unreliable – we use the Three Mobile Business Network which has guaranteed levels of security).
- Potentially view the device debug logs (for the past few days depending on activity).

Using these security methods, Glimpse should receive a rapid alert if any device is in a compromised/broken state. Each Glimpse unit has no access to its own data that has been stored on the server (or any similar server inside or outside its own organisation), this is only available to real users that interact with the data via the servers/webpages.

The only information that is used by a Glimpse device is:

- The anonymous demographic and movement information related to the last few images or signals detected.

Machine Access Code (MAC) Collection Protocol

Glimpse sensors can detect the MAC addresses being publicly broadcast from the mobile devices of people as they pass in the vicinity of the sensor. A hash is applied to these codes by the sensor before they are processed. This hash irreversibly scrambles the MAC address so that it can not be used in any way to identify an individual. The same hash is applied by all Glimpse sensors, meaning that we can identify the same encrypted code appearing again. This means we can relay crowd movement and loyalty over time to our customers while respecting shopper privacy.

Image Specific Security Protocol

Images taken from a Glimpse device are processed in real-time and not stored on the Glimpse server and are only stored in temporary memory, one image at a time, and each image is permanently deleted as the next one is assessed. Hence, no more than one image can be stored in temporary memory at any given time. Glimpse does store one image per hour, referred to as a status image, to ensure all sensor components are functioning correctly. This image is stored for maintenance purposes and is not processed for any other purpose. Glimpse has been created with privacy in mind. As such, any image files are automatically deleted after a few milliseconds (depending on network speed). If a device is unplugged, the image in temporary storage is automatically deleted. All images are analysed via highly encrypted communication with Amazon Web Services (AWS) and all information is stored on Irish servers on the AWS Platform.

These images are temporary and exist exclusively, meaning not even administrators can view previous images taken while in production mode.

Amazon Web Services Dependencies

Amazon Web Services (AWS) is a subsidiary of Amazon.com that provides on-demand cloud computing platforms to individuals, companies, and governments, on a paid subscription basis. The technology allows subscribers to have a virtual cluster of computers available all the time through the Internet. Glimpse hosts its servers using AWS, which has been proved as the industry leading standard in data security.

- Glimpse servers and database access is controlled by AWS. If passwords or keys are compromised, they can be changed rapidly and easily.
- All database instances are run in the Amazon Virtual Private cloud for the greatest possible network access control.
- AWS Identity and Access Management is utilised fully to assigned permissions that determine who is allowed to manage data resources.
- Security Socket Layer (SSL) connections are used with all Glimpse database connections.
- The location of all data being stored physically on AWS is in Ireland.
- Glimpse utilises encryption in transit with TLS encryption protocol across all cloud services.

DDoS (Distributed Denial of Service) Attack Mitigation

Glimpse utilises AWS technology that is built from the ground up to provide resilience in the face of DDoS attacks. A combination of services may be used to implement a defensive strategy and thwart DDoS attacks. Glimpse AWS services are designed with an automatic response to DDoS to help minimise time to mitigate and reduce the impact.

Data Encryption:

All data is encrypted at rest and in transit using a minimum RSA 1024-bit encryption and in some cases up to RSA 2048-bit encryption.

Security Audits:

Internal security audits of the entire Glimpse system are done on a regular monthly basis, with specific systems being audited on a more frequent basis along with automated alarm monitoring 24/7.

All security audits are performed by a qualified cloud architect with a minimum AWS Solutions Architect – Associate certification as of 1st January 2018.