SOASTA

mPulse – What's in a Beacon?

mPulse and Data Privacy

Table of Contents

Background

Since the invention of the term ‘Big Data’, we have been inundated with new technologies and information sources in our day-to-day lives that have given way to uncertainty around data privacy. This has led to paranoia (oftentimes with good reason) and regulation by way of ‘Cookie Law’ and ‘Do Not Track’.

We believe data should be used for good, especially when it comes to improving the user experience. The purpose of this paper is to clearly explain what data we collect, our stance on adherence to the imposed policies, and how we keep your data safe.

Data Collected From the User

For our web offering, the list below includes everything that is collected by default from the end user.

HTTP Headers

The following is an example of the headers that are collected from the end user:

```
Accept:*/*
Accept-Charset:ISO-8859-1,utf-8;q=0.7,*;q=0.3
Accept-Encoding:gzip,deflate,sdch
Accept-Language:en-US,en;q=0.8
Connection:keep-alive
Host:mpstat.us
User-Agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2)
AppleWebKit/537.28 (KHTML, like Gecko) Chrome/26.0.1397.2
Safari/537.28
```

The User Agent along with the user’s IP address (used for geo-lookup in order to segment traffic by Country/Region) are the only pieces of information collected outside of the beacon parameters covered below.

Beacon Parameters

The full list of query parameters that are passed via the request object (beacon) for mPulse can be found here:

http://cloudlink.soasta.com/t5/Knowledge-Base/mPulse-Beacon-Parameters/ba-p/26676

In general, data passed through the beacon falls into one of three categories:

Performance timers: Timing information related to the perceived user experience measured from their browser. Examples: Page Load time, Back-end time, Front-end time, DNS, TCP, or response time for a page component or specific resource/asset (custom timers). See the following articles for a more detailed explanation of timers:

http://cloudlink.soasta.com/t5/Knowledge-Base/mPulse-Custom-and-Navigation-Timers/ba-p/17071

http://cloudlink.soasta.com/t5/Knowledge-Base/mPulse-Estimated-Back-End-Time-for-Safari-and-Legacy-Browsers/ba-p/31998

Metrics: Measurement information used to capture the user's behavior or actions during their session. Examples: Conversion flags, Order Value, Facebook "Likes", or blog comments. Further information on custom metrics can be found here:

http://cloudlink.soasta.com/t5/Knowledge-Base/mPulse-Custom-Metrics/ba-p/17067

Administrative and Dimension data: Other required values for correctly aggregating and classifying the data in the beacon. Examples: Page Group, A/B Test and Domain.

Cookies and Tracking

Third Party Cookies

mPulse does not set third party cookies. All cookies are set on the primary domain for the site. Third party tracking cookies are used to track the identity and previous activity of an end user across multiple domains. This is typically used for targeting content for a user (advertisements, product placement, etc.). mPulse sets no such tracking cookie and stores no data in local storage that is used in tracking a user's activity or behavior beyond their single session or across other sites that use mPulse.

Do Not Track

Do Not Track is a proposal which will enable users to opt out of tracking by third parties such as ad networks and marketing analytics services. While still a proposal, browsers such as Internet Explorer, Firefox and Safari have all enabled support for opt out.

At its core, the proposal is designed to allow users to opt out of tracking outside of their existing session or across domains. mPulse is in adherence with Do Not Track, as we do not track users beyond their session, and all cookies are set on the primary domain.

Cookie Law

In May of 2011, the EU modified the existing EU Privacy and Communications Directive of November 2009 to include policy intended to safeguard online privacy and protect users from unwanted solicitation and marketing.

The simple interpretation of the law is that site owners are required to gain consent prior to setting any non-essential cookies used to collect information from the user. Non-essential cookies refer to any cookies that are not required for the function of the site (such as a session cookie used to track a user through the checkout process or a cookie used for security during a banking session).

What this means for site owners doing business in the EU is that users must 'opt-in' for cookies that mPulse will set on the primary domain. Opt-in typically includes language around tracking page views, visits, etc. captured from typical analytics offerings. In most cases cookies set by mPulse have been covered in the existing opt-in language for site owners in Europe.

Option for Exclusion of Cookies

mPulse offers domain administrators the ability to disable cookies for session tracking, if desired. This is NOT recommended, as you will not have visibility into session data (completed sessions, active sessions) and user behavior metrics (defined custom metrics, bounce rate).

Data Security

WHO Has Access to Your Data

All data stored in raw or aggregate format is only available outside of the customer's tenant to key SOASTA personnel. Domain specific data is NOT shared between tenants. Access to raw beacon logs can be provided to customers through a feature in the product. In order to obtain access to your data, you must provide your own Amazon account information which will be used to copy data for your tenant and specified domain into your own privately held Amazon S3 storage. Documentation for this feature can be found here:
http://cloudlink.soasta.com/t5/Knowledge-Base/mPulse-Administration-Beacon-Settings/ba-p/15483

Customers have the option to further limit access to their data at the domain level by using our access permissions feature – once enabled, access needs to be granted to each mPulse username that should have the ability to view or modify the domain data. This could be useful when multiple business units are sharing an mPulse tenant, and access to some data needs to be restricted. See here for documentation of this feature, using a sister product (CloudTest) for the examples: http://cloudlink.soasta.com/t5/CloudTest-Technical-Articles/Permission-Feature/ba-p/19633

WHAT Data is Stored (PII Compliance)

There is a high level of sensitivity for site owners around the collection and storage of personally identifiable information (PII). PII is a legal definition used in US privacy law to describe any piece or set of information that can be used to identify an individual. By default, mPulse does not collect PII data.

Customers should be cautious when defining metrics or A/B tests, or adding additional variables to the beacon such as credit card information, user names, account numbers or anything else that would be considered PII.

In some cases, PII may be extended to include the user's IP Address. mPulse provides the option of excluding this from data storage through the configuration option. Additionally, we have added the ability to exclude query strings from the URLs stored, which in rare cases have contained data considered to be PII.
See documentation of these features here: http://cloudlink.soasta.com/t5/Knowledge-Base/mPulse-Administration-Beacon-Settings/ba-p/15483

WHERE Data is Stored

SOASTA mPulse leverages Amazon Web Services' infrastructure (EC2, S3) for collection, storage, and display of collected data. AWS is compliant with the following certifications and third-party attestations as of this writing:

- SAS70 Type II
- PCI DSS Level 1
- ISO 27001
- FISMA
- HIPPA compliancy to Security and Privacy Rules

More information on AWS security can be found here: http://aws.amazon.com/security/

About SOASTA, Inc.

SOASTA is the leader in cloud testing. Its web and mobile test automation and monitoring solutions, CloudTest, TouchTest and mPulse, enable developers, QA professionals and IT operations teams to test and monitor users with unprecedented speed, scale, precision and visibility. The innovative product set streamlines test creation, automates provisioning and execution, and analyzes real user behavior in real-time to deliver actionable intelligence, faster. With SOASTA, companies have confidence that their applications will perform as designed, delivering quality user experiences every time. SOASTA's customers are many of today's most successful brands including Avaya, American Girl, Bonobos, Backcountry.com, Chegg, Experian, Gilt Groupe, Hallmark, Intuit, Microsoft and Netflix. SOASTA is privately held and headquartered in Mountain View, Calif. For more information about SOASTA, please visit www.soasta.com.