Customer Experience Digital Data Community Privacy Recommendations

Privacy Subgroup

Mark Prince

5/31/13

ensighten

Privacy Metadata Recommendations

The Subgroup for Privacy recommends the following metadata additions to the data standard. The four completely optional additions that represent **separate** and equally important parts of privacy enforcement:

- Technology Consent Categories

  e.g.s

  default: sitename.com, ajax.googleapis.com, ensighten.com

  analytics: google-analytics.com, omniture.com

  personalisation: baynote.com, criteo.com

  recommendations: doubleclick.net

- Privacy Type

  Private: This data is Information that alone identifies a site visitor. (e.g. Personally Identifiable Information, or PII)

  Identifiable: This data, when combined with other data, may identify a site visitor.

  Sensitive: This data, although not identifying, should not be shared, due to potential embarrassment or social ramifications.

Technology Consent Categories

The consent categories serve two purposes:

1. Facilitates communication about technologies for a non-technical site visitor to understand what technologies are used on the site.
2. Allows site owner to determine what data can be shared with each technology.

Each of these purposes is intended as an optional privacy feature of the data standard.

The following maps need to exist within the data standard to provide the structures necessary for consent:

- Consent Categories: a map between the technologies and categories
- Consent Mapping: A map between the categories and the data

The consent categories' only relationship outside of the digital data standard is to a site's Privacy Policy. The Privacy Policy forms the basis for gathering the site visitor's legal consent to share visitor data and interactions with the site's trusted technology vendors.

This could not provide a basis for any vendor lock-in, as the same categories could be enforced by any potential solution.

Privacy Type

The Privacy Type metadata serves the following purposes:

1. Allows developers and technology companies to build capabilities to restrict access, as appropriate, to data within the data layer.

2. If transmitted to trusted technology vendors, this will allow the vendors to enforce proper handling within their service.

Each of these purposes is intended as an optional privacy feature of the data standard.

The following map needs to exist within the data standard to provide the structures necessary for typing:

- A map between the privacy type and the data

The Privacy Types' definitions were chosen to present very specific notions that could be enforced using technology for proper handling. Extending these types would create a basis for vendor lock-in.

The proper handling may include any/all of the following:

- De-identification of Data
- Anonymizing Data
- Deletion of Data

The enforcement, however, is out of scope of the Digital Data Community Group's charter for this project.

Metadata Location

Metadata can be located in one of two places:

1. In *digitalData.privacy*, or a similar section of the data standard.
2. Nestled within the data structure itself

e.g.

digitalData.cart.item[3].privacy.accessor

The decision on where to include the data within the standard should be based on ease of use and performance based on the best possible syntaxes for the location (and not based on the examples in this document).

Building for the Masses, not the Few

It is a laudable goal to push for a dynamic data standard from the beginning. While it is true that the cutting edge of digital data is dynamic content, the majority of site owners will not be at the point of using a dynamic data stream versus a flat data structure for their content.

Whether or not to write directly to the data standard is still a point of contention within the Digital Data Community Group. Regardless of intent, simply by creating a Data Standard, the smaller/simpler of the site owners will seek to use it as a flat structure, until such time as the technologies around it mature.

To only designing for getters and setters ignores the likelihood of small site developers seeking simpler implementations. For such developers, accessing data where it will be used (within the data standard) is so simple that it does not require ANY helper functions.

Privacy Capabilities Are Options

Absence of Privacy data from data standard disables the privacy capabilities. Because the EU Cookie Directive-based legislation is very new, site owners will gradually adopt Privacy capabilities. As such, absence of appropriate metadata must be interpreted as disabling functionality.

Inheritance Adds Complication

Privacy Mapping of data is expected to be sparse, thereby reducing the concerns of muddying up the data layer with metadata. Sparseness implies that inheritance of Privacy metadata to subtrees overcomplicate an otherwise simple processes.

Metadata Syntaxes

Consent Categories

There is no logical fit for the technology to category map within the current data structure. So, consensus is to create the digitalData.privacy designation within the digitalData object. This data is already functionally useful to companies providing Privacy solutions to EU Cookie Directive-related concerns.

digitalData.privacy.consent

A structure that contains the technologies to be allowed for every level of consent.

```
digitalData.privacy.consent = {
        "default" : ["sitename.com", "ajax.googleapis.com", "ensighten.com"],
        "analytics" : ["google-analytics.com", "omniture.com"],
        "personalisation" : [ "baynote.com, criteo.com " ],
        "recommendations" : ["doubleclick.net"] };
```

There must be a "default", to contain the list of technologies to be interpreted as 1st party.

Consent Category to Data Map and Privacy Data Type Map

1) digitalData.privacy.mapping

A single structure that contains the mapping of consent categories and data types to the data standard

```
digitalData.privacy.mapping = [
        "cart" : "identifiable",
        "cart.item[3]" : "sensitive, identifiable",
        "transaction.total" : "private @analytics", // defined as private, but we make an exception for our analytics tools
        "privacy.mapping" : "@default", // in this example, we decide we only want to expose the exact policy mapping to 1st party technologies
        "user" : "identifiable" ];
```

2) digitalData.*.privacy

Metadata only tagged on fields of data layer where Privacy is required.

```
digitalData.cart.privacy = [ "types" : "identifiable" ];
digitalData.cart.item[3].privacy = [ "types" : "sensitive, identifiable" ];
digitalData.transaction.total.privacy = [ "types" : "private", "consent" : "analytics" ];
digitalData.privacy.consent.privacy = ["consent" : "default" ];
digitalData.user = ["types" : "identifiable" ];
```