

Privacy Preferences Information Model

Introduction

This is a specification of personal privacy preferences, based on the "[Privacy Needs and Preferences](#)" document. The information model defines the names and values and groups of name/value pairs that encode users' privacy preferences with respect to aspects of their personal information. These name/value pairs will be created, transmitted, and stored using a JSON data structure. Examples are provided of each preference encoded in JSON.

Terminology

Some of the terms used in this document are based on the "[Personal Information Protection and Electronic Documents Act](#)" (PIPEDA). They are defined here.

Personal information

Information about an identifiable individual. Examples include name, address, and credit card information.

Organization

Includes an association, a partnership, a person and a trade union.

Collection of personal information

An organization or service gathers personal information from a user and may store it internally. For example, a site may request a user enter their name, address, and credit card, and then store them on an internal server.

Use of personal information

An organization or service uses collected personal information for the purposes for which it was collected. Use is internal, within the organization. Continuing with the above collection example, a service uses credit card information when an individual purchases an item, and then the service uses the individual's address to ship the item.

Disclose personal information

An organization or service shares information it has collected with external third parties.

Information Model

privacyPreferences

The container for all of the user's privacy preferences. In JSON:

```
"privacyPreferences" : { ... }
```

An empty `privacyPreferences` implies using the default settings for all of the user's privacy preferences. Default settings are indicated using **bold text**.

privacyPreferences.thirdPartyTracking

Defines a set of Boolean preferences with respect to third parties tracking of a user's behaviour, and whether to alert the user of any tracking. If the user preference is to block all tracking, and that preference is actually enforced, then the `alert` preference is superfluous. The default preference is to prohibit all tracking by third parties.

- `doNotTrack`:
 - Value: **true (default)**, `false`, `onLeavePage`, `onLeaveSite`
 - `true`: user does not want to be tracked by any third party.
 - `false`: user allows tracking by all third parties.
 - `onLeavePage`: temporarily allow tracking until the user navigates away from the page, including ending the session with the page
 - `onLeaveSite`: temporarily allow tracking while the user is browsing pages on a site, but terminate tracking when the user navigates away from the site, including ending the session with the site
- `alerts`
 - Value: `true` or `false`
 - `true`: show a dialog alerting the user that a third party is requesting location or tracking information about the user. No limitation is assumed regarding the complexity of the dialog. The dialog can be as simple as an alert dialog with an OK button, or it could contain in context options that allow the user to block tracking.
 - `false`: do not show a dialog that alerts the user of third party tracking.
 - The `alerts` preference is superfluous if `doNotTrack` is `true`, and the system actually blocks all tracking.

Example:

```
"privacyPreferences": {  
  "thirdPartyTracking": {  
    "doNotTrack": "onLeaveSite",
```

```

        "alerts": true
    }
}

```

privacyPreferences.thirdPartyScripts

Provides preferences for restriction of third party scripts on a web page or site. There is no default setting in this case, since the preference is specified in the context of the page or site. Since there can be numerous sites and pages that these settings apply to, the `thirdPartyScripts` preference is an array of restrictions on a per site or per page basis. Each site or page is defined by a URI.

- `site or page:`
 - Value: URI of the site or the page to which to apply the user's preferred restrictions
- `allow:`
 - Value: one of `true`, `false`, or `temporarily`.
 - `true`: allow all scripts
 - `false`: block all scripts
 - `temporarily`: allow all scripts to run for the current session. That is, when the user leaves the site or page, the preference switches to `false`.

Example:

```

"privacyPreferences": {
  "thirdPartyScripts": [{
    "site": "www.somewhere.com",
    "allow": "temporarily"
  }, {
    "page": "www.elsewhere.com/login",
    "allow": true
  }, {
    "site": "www.nefarious.org",
    "allow": false
  }]
}

```

privacyPreferences.locationTracking

Provides a set of values and a whitelist of services that track the location of the user. The default is to not allow any service to track the user's location. A service is specified using a URI, designated as a *serviceURI*.

User's can allow all services to track them, or allow no services to track them, or allow only a set of trusted services to track. If the latter, the preferences allow the user to specify a list of trusted services.

- `locationTracking`:
 - Value: **none (default)**, `all`, or a whitelist of trusted services
 - `none`: indicates no location tracking is permitted by any service
 - `all`: indicates that all services are allowed to track the user's location
 - array of `serviceURIs`: a list of trusted services that are allowed to track the user's location.

Examples:

The first two examples show all that is necessary to specify no tracking or, in contrast, tracking by any service. The third example shows how to state preferences for only trusted services.

Example 1 -- no service can track:

```
"privacyPreferences": {
  "locationTracking": "none"
}
```

Example 2 -- all services can track:

```
"privacyPreferences": {
  "locationTracking": "all"
}
```

Example 3 -- trusted services can track:

```
"privacyPreferences": {
  "locationTracking": [ // whitelist of trusted services
    "serviceURI",
    "serviceURI",
    "serviceURI",
    ...
  ]
}
```

`privacyPreferences.sharingContacts`

A set of values and a whitelist of services with respect to sharing the user's contacts (e.g., address book). The default is to disallow any contact sharing.

User's can share their contacts with all services, or allow no services to track them, or share with only a set of trusted services. If the latter, the preferences allow the user to specify a list of trusted services, and whether to ask the user before sharing.

- `sharingContacts`:
 - Value: **off (default)**, `on`, an optional `askMeFirst`, or a whitelist of trusted services.
 - `off`: indicates that the user does not want to share their contacts with any service
 - `on`: indicates that the user is willing to share their contacts with all services
 - A structure that contains a Boolean value followed by a whitelist:
 - `askMeFirst`:
 - Value: `true` or `false`
 - `true`: indicates the system needs to alert the user that they are about to share their contacts with services in their whitelist, and confirm that the user wants to share.
 - `false`: indicates that the system does not alert the user about sharing their contacts with the services in their whitelist.
 - `whiteList`:
 - Value: a list of trusted services. If a service is not listed, then contacts are not shared with that service. Each service is specified using a string.

Examples:

The first two examples show all that is necessary to specify no sharing or, in contrast, sharing with any service. The third and fourth examples show how to state preferences for only trusted services, with and without confirmation.

Example 1 -- do not share contacts with any service:

```
"privacyPreferences": {
  "sharingContacts": "off"
}
```

Example 2 -- share contacts with all services:

```
"privacyPreferences": {
  "sharingContacts": "on"
}
```

Example 3 -- share contacts only with trusted services, but only with user's confirmation:

```
"privacyPreferences": {
  "sharingContacts": {
    "askMeFirst": true,
    "whiteList": [ // whitelist of trusted services
      "serviceURI",
      "serviceURI",
      "serviceURI",
    ]
  }
}
```

```

        "serviceURI",
        "serviceURI",
        "...",
    ]
}
}

```

Example 4 -- share contacts only with trusted services, but without user's confirmation:

```

"privacyPreferences": {
  "sharingContacts": {
    "askMeFirst": false,
    "whiteList": [ // whitelist of trusted services
      "serviceURI",
      "serviceURI",
      "serviceURI",
      "serviceURI",
      "serviceURI",
      "...",
    ]
  }
}

```

privacyPreferences.clearHistory

Defines which of a user's browser history features are to be forgotten, and when. The browser features are history, downloads, passwords, autofill form data, and the cache. A special case is where users do not want these features recorded in the first place. This is represented as the special time period "neverRemember", meaning do not record or store historical information.

- `clearHistory`:
 - Value: a set of browser features with an associated frequency for periodically clearing that feature. All browser features **MUST** be listed. The features to clear are:
 - history
 - downloads
 - passwords
 - autofillFormData
 - cache
 - The associated time periods are:
 - neverRemember,
 - hourly,
 - **daily (default),**
 - weekly,
 - monthly,

- neverDelete,
- onQuit

Example:

This example shows a list of all the different browser features and how frequently they should be cleared.

```
"privacyPreferences": {
  "clearHistory": {
    "history": "neverDelete",
    "downloads": "weekly",
    "passwords": "hourly",
    "autoFillData": "onQuit",
    "cache": "daily"
  }
}
```

privacyPreferences.eraseAfterUsing

Defines whether specific personal information, which has been provided, needs to be erased and forgotten immediately after its use. An example is providing one's credit card information for making a purchase. When the purchase is complete, and the information is no longer needed, this preference indicates that the user expects their credit card information will be erased.

- eraseAfterUsing:
 - Value: **true (default)** or false.
 - true: indicates that personal information is erased immediately after use.
 - false: indicates that personal information is retained.

Example:

This example indicates that personal information should be erased immediately after it is no longer needed.

```
"privacyPreferences": {
  "eraseAfterUsing": true
}
```

privacyPreferences.allowAdvertising

Defines a set of values and a whitelist of advertisements. The default is to not allow any advertisements.

Users can allow all advertisements to be shown, allow no advertisements, or allow only a targeted list. The targeted list allows the user to specify trusted services.

- `allowAdvertising`:
 - Value: **off (default)**, `on`, or a whitelist of targeted advertisements.
 - `off`: indicates no advertising is allowed
 - `on`: indicates that all advertising is allowed
 - array: a list of allowed advertisements. Each advertisement is identified as a *serviceURI*

Examples:

The first two examples show all that is necessary to prohibit any advertisements or, in contrast, allow all advertisements by any service. The third example shows how to state preferences for only targeted advertisements.

Example 1 -- no advertisements:

```
"privacyPreferences": {
  "allowAdvertising": "on"
}
```

Example 2 -- all advertisements:

```
"privacyPreferences": {
  "allowAdvertising": "off"
}
```

Example 3 -- trusted services can track:

```
"privacyPreferences": {
  "allowAdvertising": [ // whitelist of advertisements
    "serviceURI",      // URI of allowed advertisement
    "serviceURI",
    "serviceURI",
    ...
  ]
}
```

`privacyPreferences.cookies`

The “cookies” preference is a container for a number of privacy settings with respect to the creation of cookies, the sharing of cookie data, and when to force the expiration of a cookie.

- `allowCreation`:
 - Value: `never`, `always`, **fromOriginalService (default)**, `askFirst`, or a whitelist of trusted services.

- never: indicates that cookie creation of any kind is not allowed. Note that this may mean that a given page or site might not work as expected, especially if it cookies are required for normal functionality
- always: indicates that there are no restrictions on cookie creation
- fromOriginalService: indicates that cookie creation is allowed if the site currently visited is creating the cookie. Third party cookie creation from the same page is not allowed.
- askFirst: requires the system to present a confirmation dialog to the user to confirm if a cookie or cookies can be created when a service attempt is to do so.
- A whitelist of trusted services: an array of *serviceURIs* representing trusted services that are allowed to create cookies
- allowSharing:
 - Value: **never (default)**, always, askFirst, or a whitelist of trusted services.
 - never: indicates that cookie sharing of any kind is not allowed.
 - always: indicates that there are no restrictions on cookie creation
 - askFirst: requires the system to to present a confirmation dialog to the user asking if a cookie or cookies can be shared.
 - A whitelist of trustedServices: an array of *serviceURIs* representing trusted services with which sharing cookies are allowed
- expiration:
 - Value: endOfSession, **whenLeavingSite (default)**, daily, weekly
 - endOfSession: indicates that cookie data is to be erased at the end of the session
 - onLeaveSite: indicates that cookies are erased when the user leaves the site.
 - daily: indicates that cookies are deleted at the end of the day
 - weekly: indicates that cookies are deleted at the end of the week

Examples:

```
"privacyPreferences": {
  "cookies": {
    "allowCreation": [    // whitelist of trusted services
      "serviceURI",
      "serviceURI",
      "serviceURI",
      ...
    ],
    "allowSharing": "askFirst",
    "expiration": "daily"
  }
}
```

```

"privacyPreferences": {
  "cookies": {
    "allowCreation": "always",
    "allowSharing": [      // whitelist of trusted services
      "serviceURI",
      "serviceURI",
      "serviceURI",
      ...
    ],
    "expiration": "endOfSession"
  }
}

```

privacyPreferences.dataControl

This group of preferences allows users to view, update, delete, set expiration dates, and ask for details about how their information is being used or disclosed. The preferences represent user requests about their personal information as managed by some organization. The preferences or requests is on a per-organization basis. Organizations are specified by a *serviceURI*. Since a user can supply information to multiple organizations, the `dataControl` preferences are a list of requests for each organization.

With the exception of the `expiration` request, the values of each preference are `true` or `false`, meaning the user either is inquiring about that aspect of their personal information (a value of `true`), or they are not (`false`). A missing preference is equivalent to `false` for that request.

- `viewAll`: user wants to view all data held by the organization
- `editUpdateAll`: user wants to update the accuracy of their data, and submit changes back to the organization
- `howUsed`: user requests an explanation as to how their data is being used by the organization
- `howDisclosed`: user requests which third parties the organization has disclosed their personal information to, and for what purposes.
- `deleteAll`: user wants to delete all the personal information held by the organization
- `expiration`: user specifies when their personal information is to be deleted
 - Value: ISO-8601 specification of date/time

Example:

```

"privacyPreferences": {
  "dataControl": [{
    "organization": "www.somewhere.com",
    "editUpdateAll": "true",
    "howUsed": "true",

```

```

        "howDisclosed": "true"
    }, {
        "organization": "www.elsewhere.com",
        "expiration": "2017-04-05T14:30Z"
    }]
}

```

Full Preference Set Example

```

"privacyPreferences": {
    "thirdPartyTracking": {
        "doNotTrack": "onLeaveSite",
        "alerts": true
    },
    "thirdPartyScripts": [
        { "site": "www.somewhere.com", "allow": "temporarily" },
        { "page": "www.elsewhere.com/login", "allow": true },
        { "site": "www.nefarious.org", "allow": false }
    ],
    "locationTracking": [ // whitelist of trusted services
        "serviceURI",
        "serviceURI",
        "serviceURI"
    ],
    "sharingContacts": {
        "askMeFirst": true,
        "whiteList": [ // whitelist of trusted services
            "serviceURI",
            "serviceURI",
            "serviceURI",
            "serviceURI"
        ]
    },
    "clearHistory": {
        "history": "neverDelete",
        "downloads": "weekly",
        "passwords": "hourly",
        "autoFillData": "daily",
        "cache": "onQuit"
    },
    "eraseAfterUsing": true,
    "blockAdvertising": [ // whitelist of targeted advertisements
        "serviceURI",

```

```

        "serviceURI",
        "serviceURI",
        ...
    ],
    "cookies": {
        "allowCreation": "always",
        "allowSharing": [ // whitelist of trusted services
            "serviceURI",
            "serviceURI",
            "serviceURI",
            ...
        ],
        "expiration": "endOfSession"
    }
    "dataControl": [{
        "organization": "www.somewhere.com",
        "editUpdateAll": "true",
        "howUsed": "true",
        "howDisclosed": "true"
    }, {
        "organization": "www.elsewhere.com",
        "expiration": "2017-04-05T14:30Z"
    }]
}

```