Capturing User Consent

Addendum for Distributed Content Tagging

document version: 1.2.0; released on November 11, 2019

Introduction

Applicable privacy and data protection laws and regulations may require companies to capture and/or document a user's consent for measurement. For example, the European Union's General Data Protection Regulation ("GDPR") and the Privacy and Electronic Communication Directive 2002/58/EC require capturing user consent. The California Consumer Privacy Act ("CCPA") requires companies to provide users with the ability to "opt-out of the sale of personal information." Please note that the implications of applicable privacy and data protection laws and regulations may vary and are best evaluated by each individual business.

This document explains the steps to communicate user consent (e.g., did a user opt in or out of measurement) for publishers using Comscore distributed content tagging. Comscore collects data through the use of name/value pairs, typically called 'labels' in Comscore tagging implementation documents. For distributed tagging, typically a Comscore-provided piece of HTML and JavaScript code is implemented. In this HTML and JavaScript code the collected data data is represented in a JavaScript object with properties and/or in the URL of an `<img>` HTML tag, using URL query string parameters.

Although the distributed content tagging might contain additional collected data, in most cases the overall structure of the HTML and JavaScript code will look like this:

```
1.   <!-- Begin Comscore Tag -->
2.   <script>
3.       var _comscore = _comscore || [];
4.       _comscore.push({ c1: "7", c2: "1234567", c3: "7394751" });
5.       (function() {
6.           var s = document.createElement("script"), el = document.getElementsByTagName("script")[0]; s.async = true;
7.           s.src = "https://sb.scorecardresearch.com/beacon.js";
8.           el.parentNode.insertBefore(s, el);
9.       })();
10.  </script>
11.  <noscript>
12.      <img src="https://sb.scorecardresearch.com/p?c1=7&c2=1234567&c3=7394751&cv=2.0&cj=1">
13.  </noscript>
14.  <!-- End Comscore Tag -->
```

The highlighted parts indicate where the collected data is provided in the HTML and JavaScript code:

- `c1: "7"`, `c2: "1234567"` and `c3: "7394751"` in the JavaScript object
- `c1=7&c2=1234567&c3=7394751` in the URL query string parameters of the `src` attribute in the `<img>` HTML tag

Depending on individual data collection needs other labels might be included. Regardless of exactly what labels appear, **for the purpose of collecting user consent opt-in an additional label needs to be included in these parts** which is explained in the following section.

> **About the instructions in this document…**
>
> Please make sure to follow the instructions in this document to ensure user consent opt-in is collected for each transmission of distributed content tagging. Any questions about the instructions, code changes, the impact on the collected data or differences between the examples in this documentation and the tagged distributed content can be addressed to Comscore TagSupport and/or a Comscore client account representative.

Using the user consent label

To collect user consent opt-in, label `cs_ucfr` needs to be added to the collected data. The required values for the user consent label are:

Label `cs_ucfr` values for communicating user consent

Value	Interpretation	Usage
0	User has not given consent or has opted out	Use this value to indicate the user 1. has been asked for consent where the user did not give consent, or 2. enabled the option to opt out (e.g., opt out of the sale of personal information)
1	User has given consent	Use this value to indicate the user has been asked for consent where the user has given consent to collect data for measurement
	User has not taken an action	Use an empty string value (i.e., blank) to indicate the user has not taken an action

> **About including label `cs_ucfr` when not collecting user consent opt-in…**
>
> If you do not communicate consent for a user, then **do not populate** label `cs_ucfr`.

Label `cs_ucfr` must be added with an appropriate value to the distributed content tagging in the HTML and JavaScript code. With this change of the HTML and JavaScript code **any other collected data values should not be changed**. For example, assuming the user has given consent, the aforementioned code would be changed into:

```
1.  <!-- Begin Comscore Tag -->
2.  <script>
3.      var _comscore = _comscore || [];
4.      _comscore.push({ c1: "7", c2: "1234567", c3: "7394751", cs_ucfr: "1" });
5.      (function() {
6.          var s = document.createElement("script"), el = document.getElementsByTagName("script")[0]; s.async = true;
7.          s.src = "https://sb.scorecardresearch.com/beacon.js";
8.          el.parentNode.insertBefore(s, el);
9.      })();
10. </script>
11. <noscript>
12.     <img src="https://sb.scorecardresearch.com/p?c1=7&c2=1234567&c3=7394751&cs_ucfr=1&cv=2.0&cj=1">
13. </noscript>
14. <!-- End Comscore Tag -->
```

Confirm user consent is communicated

After changing web page impression tagging as instructed in this document the collected data should contain label `cs_ucfr` with its assigned value **for each** distributed content impression. The collected data is transmitted as HTTP requests, which can be inspected with a modern web browser's 'Developer Tools' or by using an HTTP proxy such as Fiddler or Charles Proxy.

The collected data will be transmitted to the host `b.scorecardresearch.com`[1] where the URL query string parameters of the HTTP request should contain label `cs_ucfr` with its assigned value.

> **About confirming expected behavior…**
>
> As a good practice, it is advised to confirm this expected behavior across all web pages where Comscore distributed content tagging is used.

---

(1) For secure transmissions using HTTPS the hostname will be `sb.scorecardresearch.com`.