Abstract
This document is intended to define a process to conduct an assessment of the privacy impact of a W3C specification.

Status of this Document
This document is an initial draft of the Specification Privacy Assessment for discussion within the W3C Privacy Interest Group (PING). The document does not represent any current consensus within the PING, as discussion on the topic is ongoing.

If you wish to make comments regarding this document, kindly email them to public-privacy@w3.org.

Publication as a Working Draft does not imply endorsement by the W3C Membership. This is a draft document and may be updated, replaced or obsoleted by other documents at any time. It is inappropriate to cite this document as other than work-in-progress.

Introduction
The W3C Privacy Interest Group is chartered to improve the support of privacy in Web standards by, among other things, providing guidelines and advice for addressing privacy in standards development.

The W3C defines standards for the World Wide Web that forms part of the backbone for an emerging online digital marketplace. The standards will need to be developed with the intentions of protecting the personal information of the consumers who trust in this technology. The Standards Privacy Assessment (SPA) document provides W3C specification Editors with guidance on:

- Why a Privacy Considerations section is needed in a W3C specification,
- When a SPA process should be used for a W3C specification,
- How to conduct a SPA analysis on a W3C specification, and
- What findings should be included in the Privacy Considerations section of a W3C specification?

The SPA is a methodology for analyzing a specification for possible privacy impact. It takes into account applicable privacy principles and associated privacy safeguarding requirements in order to assess the potential threats arising from the specification that require mitigation by introducing privacy safeguards or controls. In addition, the SPA process is intended to be helpful in creating analysis information that will be useful in conducting a privacy risk assessment of deploying the specification that analyzes the harm towards an individual that could be caused by the technology being defined by the specification.

Guidance to Editors on when to apply SPA
The work of W3C covers the development and maintenance of specifications and guidelines defining the World Wide Web. This work will require the Editors of W3C specifications to take into account the privacy impact of their specification.

While the scope of these specifications will vary, it is important for the Editors to be mindful of when their work has a privacy impact.

In addition, when W3C participants liaise and collaborate with other organizations and committees dealing with work similar to that of W3C, the participants need to be mindful when their collaboration topics have privacy impact.

The privacy impact of a specification is directly related to whether the specification creates or processes personal information and/or whether the specification deals with technical mechanisms for identifying personal information with the individual associated with that personal information.

The following logic diagram may be useful to an Editor or W3C participant to determine the privacy impact of the work they are involved in.

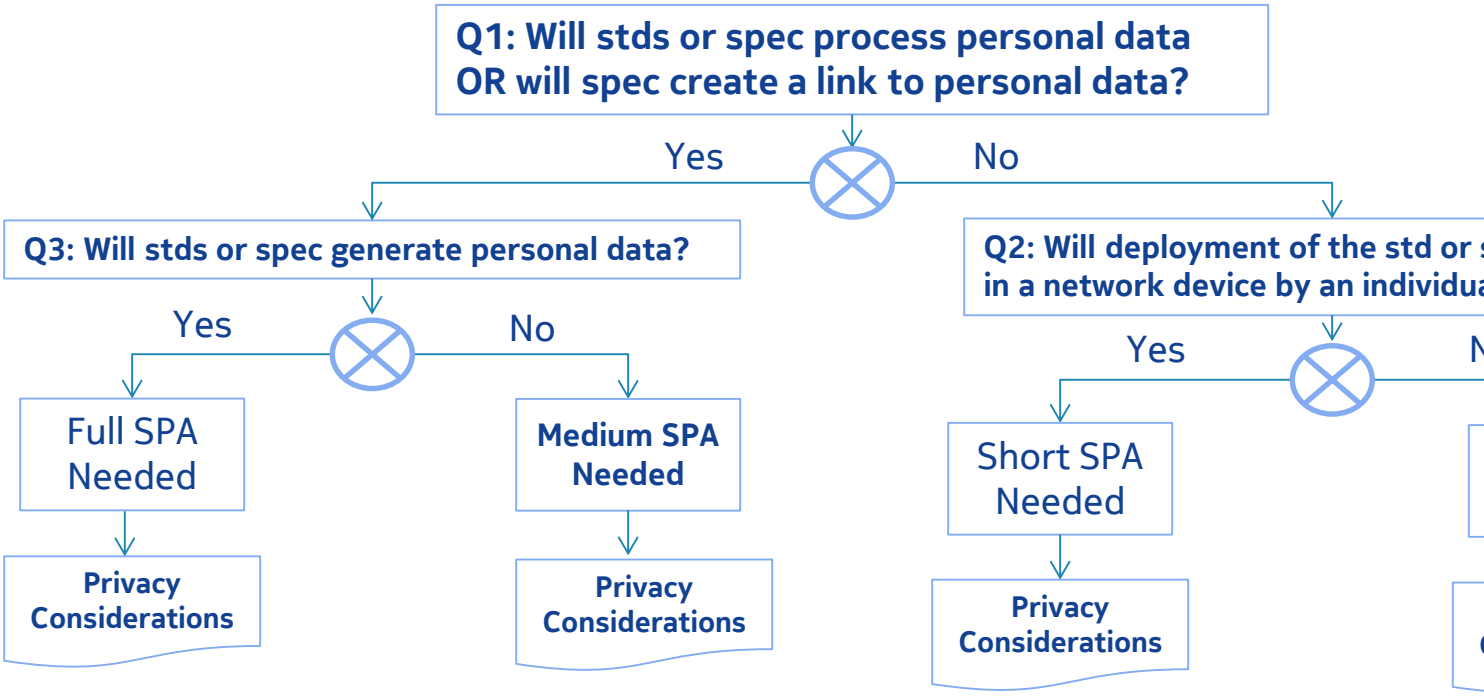

Figure 1: Determining when to apply SPA

In Figure 1, "spec" refers to either a W3C specification. In order to determine whether to apply the SPA process, the specification under review (SUR) should be evaluated to determine if it will involve technology that will process personal information, or if it will involve technology that could link to personal information. If the evaluation determines that the SUR will not process personal information or involve technology that could like to personal information or an individual, then a further evaluation should be undertaken to determine if the SUR will involve technology that will be used in a network device by a data principal, or individual. If these evaluations result in a negative conclusion, then a SPA process probably need not be applied to the specification. Otherwise, application of the SPA to the specification is warranted. If the answers to questions Q1 and Q3 are affirmative, then a more involved analysis of the SUR using the SPA process is warranted, resulting in a more detailed Privacy Considerations section in the "spec". If the answer to Q1 is negative but the answer to Q2 is affirmative, then a less involved analysis of the SUR is necessary and the resulting Privacy Considerations section in the "spec will be specific to how the network device may present conditions where the user of the device can be identified and its usage tracked, for example. The case where Q1 is answered affirmative but Q3 is answered in the negative presents a use case where the "spec" will need an analysis with efforts somewhere between the previous two cases.

In the event that a SPA process is not considered warranted, then the Privacy Considerations section should clearly articulate this using text such as the following:

"This specification does not define technology that will process personal information, nor will it create any link to personal information. Furthermore, the specification does not define technology that will be deployed in a network device and used by an individual."

Application of SPA to the W3C Technical Report Development Process

The W3C technical report development process is defined in section 7 of the W3C Process Document [1].

Figure 2: W3C TR Development Process

The application of the SPA process should not wait until the final milestones but instead should be applied from the first milestone, when a Recommendation is being drafted with its first working draft. The various activities that apply to each milestone include:

Working Draft (WD)

- Best time to start is when a Working Draft for a Recommendation has been created, and
- Work can be introduced, privacy fundamentals explained, privacy goals explained, SPA approach explained, Privacy Champ identified.

The Privacy Champ being a member of the project team whom is the champion for privacy considerations within the project.

Candidate Recommendation (CR)

- Specification takes shape through contributions and reaches control mode, and
- As the Recommendation team creates specification functionality, data flows are analyzed and categorized, areas for Privacy Engineering are identified, privacy requirements are identified, threats are identified, safeguards are defined, and findings documented in SPA report for follow-up action.

Proposed Recommendation (PR)

- Privacy Considerations section reflects mitigation steps to address SPA findings.

Recommendation (REC)

- Publication staff and Specification Editor verify Privacy Considerations compliance against SPA findings and update accordingly.

Maintenance of Technical Recommendation

- Deployment of specification can lead to issue reporting that need address in timely manager with technical opinions and possible change requests for spec update.

SPA process

The SPA process involves the following analytical steps:

1. Create a clear understanding of the description of the technical functioning of the SUR,
2. Identify the data flow between internal components (interactors) of the SUR and external components (interactors),
3. Classify the data identified in Step 2 to understand the data processed (I.E., the Privacy Data Lifecycle defined by IAPP knowledge base) and whether the SUR features can identify, link to, or through observation otherwise determine the person associated with the personal information,
4. Identify applicable privacy principles and associated privacy safeguarding requirements, such as those from [2] that apply to the primary use cases for the SUR,
5. Outline the threats created by analyzing the data flows from Step 2, along with the data classification from Step 3 and the applicable privacy requirements from Step 4,
6. Identify appropriate privacy control mechanisms that can be introduced to safeguard data protection, and
7. Consider approaches, beyond the privacy controls in Step 6, that will enhance privacy, such as limits on collection, limits for retention, rules for secure transfer, rules for limiting identification or obfuscation, for those deploying the specification or standard.

Step 1: ***Description*** - The SPA process is based on having a detailed understanding of the features and functions of the SUR. The description of the SUR generally includes an understanding of:

- Primary use cases for the features of the SUR,
- Internal interactors of the SUR. These include the internal processes and data stores, as well as interfaces to external interactors,
- External interactors that the primary use cases of the SUR may either be dependent on or that the SUR maybe a dependent resource for. These include external processes and data stores.
- Identification of the data that flows between the internal interactors and external interactors, and
- Borders between the internal and external interactors that form a trust boundary.

Step 2: ***Data Flow*** - The old adage that "privacy impact comes with data" is true. Privacy impact is related to processing of personal information and the linkability of that personal information to a data principal or individual (I.E., the individual's identifiability). Detailing the data flow involved in a SUR is a key element to systematically applying the SPA. Ad hoc application of the SPA will result in spot application of safeguards and possibly lead to missing key vulnerabilities in the SUR. A primer on data flow diagram technique can be found in [2].

Step 3: ***Data Classification*** – Understanding the scope of the data that is associated with the SUR is important in determining where unneeded data is being processed by the SUR or through the SUR by external interactors. One way to minimize the privacy impact of the SUR is to minimize the collection of personal information in the first place and to limit the retention of that data for further processing. To assess this, the data flowing through the SUR needs to be identified and classified. If the team creating the W3C specification utilizes design principles, then having considerations for data management within the design principles should be considered.

The Privacy Data Lifecycle (sometimes called the Consumer Data Lifecycle) defines the actions related to personal data and is a fundamental component of the privacy knowledge base. When analyzing the data

flow in a W3C specification, the complete data lifecycle for the associated personal information should be considered because each stage may introduce nuances to the overall privacy consideration of the specification.

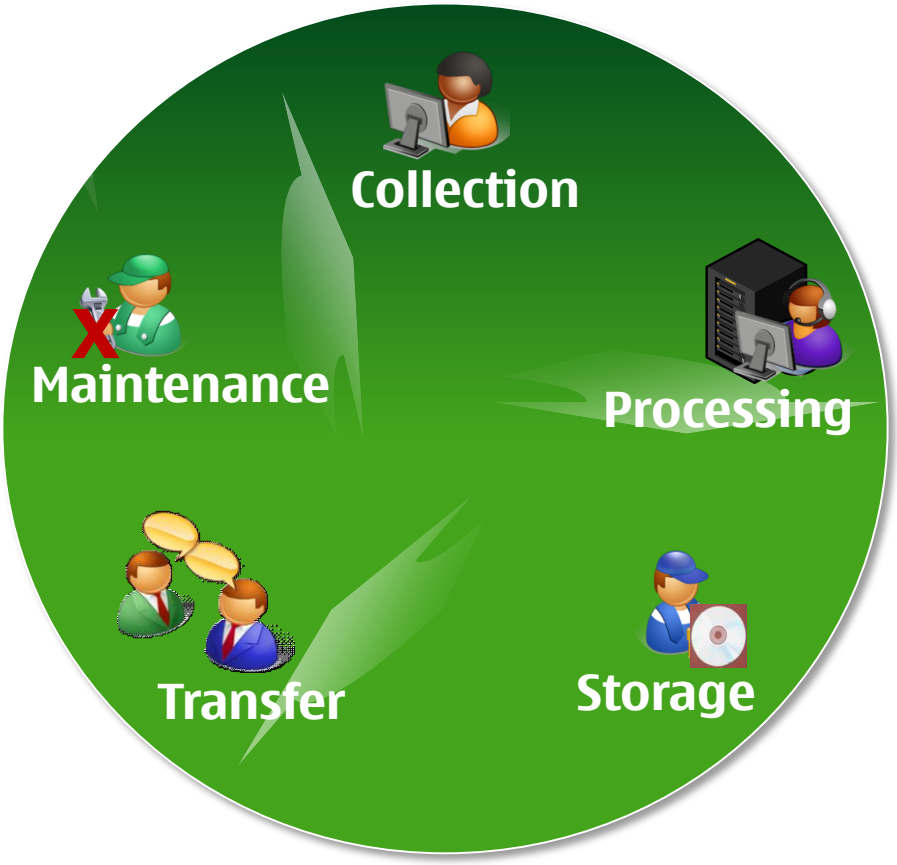

Figure 3: Privacy Data Lifecycle

It should be noted that within the EU, collection, itself is considered to be an act of data processing.

There are a number of classification schemes that can be used to achieve this process step, but in general the analysis step should determine ***why*** the data is collected, ***what*** primary purpose there is for the processing of it, ***where*** it is being transferred or stored and ***how long*** it is being retained. In addition, the "nymity" characteristic or the degree that the individual associated with the personal data can identified, linked to, or named through observing the network traffic containing the data, needs to be classified (IE, is the personal data, in fact, personally identifiable information or PII). A PII classification approach can be found in [3]. There, personal data is classified as "identified", "identifiable" and "non-identifiable". In addition, a classification of "sensitive identifiable" should be considered.

Step 4: ***Privacy Safeguarding Requirements*** – At this point in the SPA process, there is sufficient information to evaluate the SUR to determine which privacy safeguarding requirements apply. This involves first understanding which privacy principles are applicable. One such set of privacy principles is defined by the ISO 29100/Privacy Framework [4] standard. The standard defines the privacy principles as:

1. Consent and choice
2. Purpose legitimacy and specification

3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

The SUR should be reviewed to determine which of these principles are applicable and ISO 29100 provides some guidance on applicable privacy safeguarding principles, under the description for each. Other sets of acceptable privacy principles can be found in [5], [6] and [7].

Step 5: Threat Analysis – Threat Analysis is a step where the privacy safeguarding requirements identified in Step 4 are analyzed to identify inherent vulnerabilities that a threat agent could utilize to create an incident with the technology being defined by the SUR.

Step 6: Threat Mitigation – Mitigation of threats identified in Step 5 is necessary to create a robust privacy enhanced specification. Threat mitigation involves application of one or more privacy safeguards or controls to thwart an identified threat scenario.

Step 7: Deployment Considerations – Steps 1-7 when applied at an early stage in the creation of the specification will assist in introducing more privacy enhancing design choices for the SUR. However, even when these steps are followed from New Work Item Proposal through Publication of the specification, there are still considerations to take for the deployment of a published standard. In some cases, the organization deploying the SUR will be in the best position most to take into account privacy safeguards. This last step in the SPA process challenges the Editor or W3C participants to consider what can be done during the implementation and deployment of the SUR to enhance the privacy of individuals who will be using ICT systems with the SUR embedded inside them.

Privacy Considerations outline

The results of applying the SPA process is the creation of text within the specification that outlines the privacy considerations that have been taken into account in the development of the specification, as well as those that should be considered when deploying the specification. This means that there should be a Privacy Considerations section in every W3C specification. In the case where it has been determined that the application of the SPA process is not warranted then this section would contain text such as:

> "**This specification does not define technology that will process personal information, nor will it create any link to personal information. Furthermore, the specification does not define technology that will be deployed in a network device and used by an individual."**

However, in those cases where a SPA process has been determined to be warranted then this section needs to include text that:

- Catalogs the personally identifiable information (PII) collected, its classification, instances of data storage, type of processing, instances of data transfer (against the privacy data lifecycle) from SPA Step 3;
- Identifies and list privacy threats from SPA Step 5;

- Identifies appropriate privacy safeguards/controls and context for mitigating identified threats from Step 6, and
- Identifies recommendations such as uses of privacy controls, by organization deploying the specification, that would additionally thwart the associated threats from Step 7.

References

[1] "W3C Technical Report Development Process", W3C, http://www.w3.org/2005/10/Process-20051014/tr.html#Reports.

[2] "A 10 Minute Data Flow Diagrams (DFD) Quick Start", Mike Prestwood, http://www.prestwood.com/ASPSuite/KB/document_view.asp?qid=100887.

[3] "PII 2.0", P. Schwartz and D. Solove, http://docs.law.gwu.edu/facweb/dsolove/files/BNA-PII-FINAL.pdf.

[4] "ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy framework", http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45123.

[5] "OECD Privacy Principles", OECD, http://oecdprivacy.org.

[6] "Fair Information Practice Principles", US Federal Trade Commission, http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[7] "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data", European Parliament and Council, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.