W3C DAP APIs and the EU Working Party 29 opinion on Consent

Frederick Hirsch, Nokia
31 October 2011

Executive Summary

The W3C Device APIs working group [W3C-DAP-WG] has taken the approach of using user interaction as a mechanism to obtain active consent in context. To improve usability consent dialogs are avoided and action is taken to mean giving permission. Examples include selecting the contact fields to share, electing to create a picture by clicking on the camera shutter, and so on. This approach is intended to be clear and less disruptive to the user.

The EU/Working Party 29 opinion on consent [WP29-Press, WP29-187] provides criteria for informed consent. Such consent may include active steps by the user, but also requires that consent to be informed, with adequate information provided to the user at the time of the consent action.

The APIs defined in DAP suggest a means to enable informed consent, but only if the service provider provides adequate information and notice in conjunction with those actions. In addition, user interaction is not always required by the DAP API specifications and it is not clear how consent is obtained in the case that the APIs are used in a web application that does not require a traditional browser user agent.

The DAP APIs are only a portion of a larger system, thus they can enable privacy but not constrain other aspects of the system [W3C-Hirsch-5Nov]. To capture aspects relevant to web application developers the DAP working group has drafted privacy best practices for Web Applications [W3C-DAP-WebApp-Privacy-BestPractices].

The remainder of this paper outlines points from the EU Working Party 29 opinion, followed by a brief review of implications for DAP.

Working Party 29 Opinion

The Working Party 29 Opinion highlights that consent must have certain properties. The core principle is that a data subject should be in control of their data.

Consent is one legal ground for processing data; there can be others such as contracts. Consent is not necessarily the only means to justify processing; it must be used in the right context (See II.4 re complexity). Lack of refusal is not the same as consent, thus not

filling in a checkbox indicating refusal does not constitute consent. The right to object is distinct from consent and serves a different purpose.

Consent should be:

1. Freely given,
    a. Transparency, a condition of being in control and for rendering consent valid
    b. Consent can be considered to be deficient if no effective withdrawal permitted
    c. Periodic confirmation of consent (people change)
    d. Obtain unambiguous consent, leaving no doubt as to user's intent. Seek clear express consent or use procedures to obtain clear inferred consent

2. Specific,
    a. Indication of consent must be unambiguous and explicit regarding sensitive data
    b. Consent must be intelligible, specific in scope, limited in context
    c. Additional consent required if purpose/context of processing changes

3. Informed
    a. All necessary information must be given at the time of consent
    b. Clear, accurate, complete information
    c. Awareness of implications of not consenting
    d. Information should be clear to average user
    e. Information must be given directly to users - it is not good enough for it to be available "somewhere"

Consent should be an "indication" and must meet “reasonable” expectations. The ability to withdraw previously given consent is important. So is the ability to be sufficiently certain the person giving consent is the data subject. Consent should be verifiable, enabling proof that consent was given.

Consent does not negate need for other aspects in addition to consent:

4. Fairness
    a. Transparency also a condition of fairness
5. Necessity
6. Proportionality
7. Data quality

Certain approaches are explicitly called out as *not* serving as consent:

1. Inaction, such as pre-ticked boxes, does not constitute consent. Likewise browser cookies do not serve as consent. It is essential that the user take action to give consent. Consent cannot be implicitly inferred from a lack of action.
    a. Action is necessary but different actions are possible, assessed in context

Other approaches are explicitly called out in the opinion as examples of giving consent:

- Consent *can* be a Behavior from which consent can be concluded (see III.A.1 p4, page 11)
- Ticking a checkbox, clicking a button for example may constitute explicit consent.
- Prior consent - consent before any data processing is also acceptable
- Flexible, 2h, any indication is suitable, so detailed technology not spelled out

An example of consent through action given in the opinion is a Bluetooth ad board. Another is the action of employee to send picture for posting (p14).

Special categories of data require “Explicit consent”, the same as “Express consent”.

The definition of consent in current use is: "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*". (See page 5 of section II.I, “Brief History”)

Implications and Interpretation for Device APIs

The W3C Device APIs working group is defining JavaScript APIs for device functionality such as access to user contacts, calendar, camera, and device information (among others). This information should not be shared arbitrarily with web applications, as it is information that should be under user control.

Experience with web security has shown that in general security dialogs are not meaningful to users and that they will generally click through to obtain desired results. In addition, policy is hard to provision and administer in the wide web, as there is no appropriate essential authority. In the interest of both usability and meaningful interactions the DAP WG has realized that privacy interactions should directly relate to the context of the action the user is attempting to perform. As a result the DAP WG has taken the approach of enabling user consent through the explicit action of the user selecting information to share [W3C-DAP-Contacts].

This approach has the following properties:

The data is *freely given*: the user can terminate the sharing by cancelling the selection operation. In addition, the selection is periodic, performed each time information is to be shared. The explicit action of selecting data to share is unambiguous.

The data selected is *specific*, however knowledge of the use will not be unless shared with the user in conjunction with the selection operation. This requires the browser to share this information, however that depends on adequate information being shared by the web service. A simple example statement of use is "Obtain your address to enable shipping the product."

It is necessary that consent be *informed*, meaning it is clear which information is being shared, and for what purpose. This depends on the Web Application providing this information – the DAP API does not mandate this information. Thus informed consent depends on the web application using the DAP APIs appropriately while providing adequate context, including notice about intended use.

The DAP approach of using a selection action to provide consent is consistent with examples in the Working Party opinion where it states that consent should be an action and that it can be a behavior from which consent may be concluded (See III.A.1. Article 2(h), p 11 for examples of placing business card in bowl, or sending address to an organization). However the consent needs to be a clear indication, for example having Bluetooth on near a billboard does not constitute consent for receiving ads (same section, p 12). This is also consistent with other examples that are given in the opinion; including a user sending a photo with that act constituting consent (same section, p 14).

Limitations of the DAP Approach

As noted above, the DAP mechanisms cannot provide informed consent without the web application providing adequate information about the information use, and this being shared in conjunction with the user action. The mechanisms defined by DAP do not define whether and how notice is to be shared by the web application.

In addition, the DAP APIs do not preclude web applications from asking for more information than they need. Although the concept of data minimization has informed the design of the DAP APIs, there is nothing to prevent an application from invoking APIs that provide more information than is needed for the user task.

There are other privacy issues that are not so obvious, such as the generic issue of obtaining consent to share metadata. An example is the information recorded by cameras in conjunction with recording an image, such as camera settings (aperture, model of camera and other information), timestamp, location (if such a setting has been enabled), tags, and other information [Exif]. The current DAP Camera API does not provide programmatic access to metadata and relies on the user pressing the camera shutter, but this action provides the user no information on metadata and

thus no associated informed consent to sharing the metadata with the web application.

Summary

The approach taken by the Device API working group toward using active consent through the action of selecting information to share is consistent with the Working Party opinion, but may not be enough unless web applications and the web browser provide enough information about the intended use of the information in conjunction with the selection operation.

Full compliance with the Working Party opinion will require more than the DAP standard as it will depend on both browser and web application provider implementation details. To help web application developers the DAP working has produced a note outlining best practices for web application providers [W3C-DAP-WebApp-Privacy-BestPractices] however approaches other than technical standards may be also required to obtain full privacy support.

Notes

[Exif] Wikipedia: Exchangeable image file format, http://en.wikipedia.org/wiki/Exchangeable_image_file_format

[W3C-DAP-Contacts] for example, http://dev.w3.org/2009/dap/contacts/#security-and-privacy-considerations and http://dev.w3.org/2009/dap/contacts/#user-interaction-guidelines

[W3C-DAP-WebApp-Privacy-BestPractices] W3C DAP note: Web Application Privacy Best Practices, http://www.w3.org/TR/2011/WD-app-privacy-bp-20110804/

[W3C-DAP-WG] http://www.w3.org/2009/dap/

[W3C-Hirsch-5Nov] Internet Privacy Workshop Position Paper: Privacy and Device APIs, http://www.iab.org/wp-content/IAB-uploads/2011/03/frederick_hirsch-revised.pdf

[WP29-Press] http://ec.europa.eu/justice/policies/privacy/news/docs/press_release%20opinion_on_consent_14072011.pdf

[WP29-187] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf