Internet Privacy Workshop Position Paper: Privacy and Device APIs
Frederick Hirsch, W3C DAP Co-Chair, Nokia
5 November 2010

Introduction

As outlined in previous position papers and W3C workshops, important privacy challenges are related to the use of Device APIs such as calendar, contacts, camera, geolocation, system information etc [1], [2].

There is no silver bullet for privacy, nor is there a simplistic approach for privacy design. A systemic view of privacy is necessary, since the appropriate visibility to and use of information is applicable to the entire information lifecycle. Access control and confidentiality can be helpful to keep information from those who should not see it, but cannot address the misuse by those who should have access for legitimate purposes. Thus privacy is not only a technological concern, but also a social and legal issue.

Establishing privacy requires engineering responsibility in the user sphere, for example to enable user consent, as well as responsibilities at the recipient sphere such as those related to redistribution and retention [3]. Privacy concerns cannot be addressed solely at the user sphere or at the recipient sphere, but requires consideration at both. Privacy requires consideration of the entire information lifecycle, including information collection and creation, usage, transport, storage and destruction. APIs at the device will enable much new information collection and creation (such as creating a new photograph) and possibly storage. Issues of usage, storage and destruction are important at the recipient sphere.

There are important high-level privacy choices that can be made in creating systems, for example choosing to create privacy preserving systems through the architectural design itself [3] or by providing user notice and asking for consent. What is chosen may depend on business models that use personal information as well as technical capabilities. Additional factors include identity management and anonymization (and prevention of de-anonymization).

W3C Device API Privacy Considerations

The W3C Device APIs and Policy Working Group (DAP) [4] is creating APIs to enable web applications to access information from the device, including contacts, camera and other capabilities. The working group is aware of the importance of privacy by design as well as limitations inherent in specifications that are part of a larger existing system such as the web. Simplification of API definitions and features creates a simpler system that is easier to secure and demonstrate privacy.

DAP User Sphere Privacy Considerations

The working group is using a privacy by architecture where possible. An example is designing APIs with minimization of data provided to that which is essential, such as requiring users to request the contact fields they need from specific contacts rather than always returning more information by default.

User consent is difficult as users often do not understand privacy or security related dialogs and will simply choose "yes" so they can continue what they were doing. Thus the WG is designing APIs to enable user consent as part of a user work-flow, such as a user selection for a subsequent step. This makes for natural and meaningful interactions that imply consent, at the risk that the user will not realize the privacy implications of the operation. There may be cases where explicit user consent *is* appropriate such as knowing that a possible use of data could happen *now*, such as sharing location data. This is something that may require careful review of the DAP specifications as they progress.

DAP Recipient Sphere Privacy Considerations

Some of the more difficult privacy concerns are related to data retention and secondary use. These are concerns related to the data recipient sphere use of device API information. Although important, maintaining privacy is dependent on the involvement and cooperation of the data recipient, such as a server side web application, and this cannot be required by a DAP specification.

The device API WG is exploring one approach to communicate user privacy intent to data recipients, the Rulesets approach [5]. It is not clear that this work will be adopted, as there are issues raised by implementers related both the role of the browser in privacy and the technologies.

Next Steps and Additional Questions

Applying privacy by architecture to the design of device APIs is complicated by the fact that the APIs are only one part of an overall solution, dealing only with client sphere collection of data but not able to mandate recipient sphere privacy data lifecycle (use, storage, transfer, etc) aspects. This is a social and business issue as well as a technology issue.

Approaches to share user intent with services are possible, or even negotiation, but this raises costs of implementation, questions about who should be responsible, and concerns about adoption and implementation. It is hard obtain agreement among the many parties in a system to obtain a systematic solution to the problem until the impact of the problem has been clearly demonstrated and accepted.

On the client sphere, the approach of using existing workflow interactions to enable consent offers the hope of enabling privacy decisions in a seamless and non-intrusive manner, enhancing usability. There is the risk however that this becomes indistinguishable from "business as usual" without any significant privacy impact, in fact establishing "no privacy" as the norm. There may be cases where explicit privacy notifications are appropriate and necessary. This may also relate to the need to consider context in privacy which indicates a need to understand context, probably an application issue that cannot be solved at the DAP API level alone.

The device API working group is addressing privacy by architecture through data minimization.

One of the lessons so far is that privacy by design is hard when standardizing a component of an existing architecture that includes many players with different objectives and concerns.

Acknowledgements

Thanks to Art Barstow, Frank Dawson, and Mikko Niva and Tony Spires for their comments on earlier drafts of this paper.

Notes

[1] Privacy Workshop Position Paper - The DAP Perspective,
W3C Privacy Workshop, July 13-14, 2010; Robin Berjon, Frederick Hirsch, http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-11.html
[2] Position Paper: Privacy And Policy In The Dap WG a DAP Perspective
W3C Workshop on Privacy and data usage control, 4-5 October 2010; Frederick Hirsch,

Robin Berjon, http://www.w3.org/2010/policy-ws/papers/14-Hirsch-Berjon-DAP.html

[3] Engineering Privacy
January/February, 2009 Sarah Spiekermann, Lorrie Faith Cranor, IEEE Transactions on Software Engineering, pp. 67-82

[4] DAP Home Page
http://www.w3.org/2009/dap/

[5] Privacy Rulesets: A User-Empowering Approach to Privacy on the Web.
W3C Privacy Workshop July 13-14, 2010 Alissa Cooper, John Morris, and Erica Newland Center for Democracy & Technology http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html