Tracking to Consensus: Coordination of Policy and Technical Standardization in Web Privacy Efforts

W3C Workshop on Web Tracking and User Privacy
28/29 April 2011, Princeton, NJ, USA

Sue Glueck, Senior Attorney, Microsoft Corporation and Craig Shank, General Manager, Interoperability Group, Microsoft Corporation

At Microsoft, consumer trust is vital to our business, and privacy is a critical component of earning and maintaining that trust. In all of our service offerings, we strive to be transparent about our privacy practices, offer meaningful privacy choices, and protect the security of the data we store.

The explosive growth of the Internet, cloud computing, the proliferation of computers and handheld mobile devices, and the expansion of e-commerce, e-government, e-health, and other web-based services have brought tremendous social and economic benefits. At the same time, however, technology has fundamentally redefined how, where, and by whom data is collected, used, and shared. The challenge that industry, government, academics, and advocates must address together is how to best protect consumers' privacy while enabling businesses to develop a wide range of innovative products and services.

The multiple contexts in which Microsoft engages with consumers give us a unique perspective on the privacy discussion. For example, as a website operator, an ad network, and a browser developer, we have a deep understanding of the roles that different participants in the digital ecosystem play in safeguarding consumer privacy. Also, based on our longstanding involvement in the privacy debate, we recognize that the combined efforts of industry and government are required to effectively balance the need to protect consumers' privacy interests and promote innovation.

When Justice Louis Brandeis famously defined privacy as "the right to be let alone" in 1890,[†] he could not have foreseen how technology would revolutionize our world. In the digital era, privacy is no longer about being "let alone." Privacy is about knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure. These three principles—transparency, control, and security—underpin Microsoft's approach to privacy. We believe

[†] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). Accessed at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

that the principles of transparency, control, and security should inform technological, self-regulatory, legislative, and educational initiatives to safeguard consumer privacy.

In a separate paper from Adrian Bateman entitled "Web Tracking Protection" we have written about the browser features in IE9 and Microsoft's Member Submission to the W3C. Here we would like to identify some of the key questions we believe need to be addressed across the stakeholder communities in order to make any of these approaches effective.

In light of our experience, we continue to advocate a multi-pronged approach that includes technology tools – such as the Tracking Protection and "Do Not Track" user preference described in our W3C submission – as well as industry self-regulation, legislation, and consumer education. We have written in more detail about each of these in connection with the recent Senate Commerce Committee hearings here.

For the purpose of this workshop and discussions of the role of W3C and other organizations in Web privacy and tracking protection, one of our key focus areas is effective coordination of different elements of these approaches, different stakeholder views, and the alignment of technical standards with policy interests.

Over the past ten years, there have been a number of thoughtful papers on the connection between technical standards and policy interests.[§] Fundamental to that discussion is a recognition that the work on technical standards designed to implement policy or "values" will need to integrate views that reach beyond the discussions that may take place in a strictly technical standardization effort. We believe that it is important for the discussions at the Workshop to move the conversation toward consensus on how some of the underlying "values," "social protocols" or "policy and business rules" can be identified and developed in tandem with the technical means to achieve them.

[§] We appreciate the pointer from Deirdre Mulligan at the UC Berkeley School of Information to several of these, including:

- Nick Doty, Dierdre K. Mulligan and Erik Wilde, *Privacy Issues of the W3C Geolocation API,* UC BERKELEY SCHOOL OF INFORMATION REPORT 2010-038 (February 2010). Accessed at http://escholarship.org/uc/item/0rp834wf#page-2
- Lorrie Faith Cranor and Joseph Reagle Jr., *Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences,* PROCEEDINGS OF THE TELECOMMUNICATIONS POLICY RESEARCH CONFERENCE (September 27-29, 1997). Accessed at http://www.w3.org/TR/NOTE-TPRC-970930/
- John Morris and Alan Davidson, *Policy Impact Assessments: Considering the Public Interest in Internet Standards Development,* TPRC 2003 – THE 31ST RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY (August 2003). Accessed at http://www.cdt.org/publications/pia.pdf

Accordingly, we believe that some of the key questions that should be discussed in this Workshop include:

- What is the appropriate process – including policy and broad stakeholder input – to develop the definition of "track" and web site behaviors in response to the "Do Not Track" signal from a browser?
- Who are the appropriate stakeholders to be engaged in developing that definition and behaviors?
- What will be the most effective way to convene those stakeholders in that development?
- What objectives, considerations, constraints and other factors should stakeholders have in mind as they look at potential approaches to web privacy – for example to determine what actions web sites should take in response to a "Do Not Track" signal?
- How will that process best take into account the global nature of the web – for example if a consumer in Brazil accesses a French web site running on servers hosted in Germany using an ad provider from Australia and an analytics firm in the United States, how do all of the participants in the system know what definition of tracking applies and how to interpret the consumer's expression of intent?

We believe that a robust discussion of these questions will help move the overall efforts on the technology and the related policy topics forward. We also believe that a broad set of stakeholders is required to achieve effective outcomes on these issues for industry, government, and most importantly, consumers.