Voici ci-dessous notre réponse officielle, attribuable à Rachel Whetstone, Senior Vice President of Communications and Policy).

Et ici un très bon panorama/résumé de la question.

Microsoft omitted important information from its blog post today.

Microsoft uses a "self-declaration" protocol (known as "P3P") dating from 2002 under which Microsoft asks websites to represent their privacy practices in machine-readable form. It is well known - including by Microsoft - that it is impractical to comply with Microsoft's request while providing modern web functionality. We have been open about our approach, as have many other websites.

Today the Microsoft policy is widely non-operational. A 2010 research report indicated that over 11,000 websites were not issuing valid P3P policies as requested by Microsoft.

Here is some more information.

Issue has been around since 2002

For many years, Microsoft's browser has requested every website to "self-declare" its cookies and privacy policies in machine readable form, using particular "P3P" three-letter policies.

Essentially, Microsoft's Internet Explorer browser requests of websites, "*Tell us what sort of functionality your cookies provide, and we'll decide whether to allow them*." This didn't have a huge impact in 2002 when P3P was introduced (in fact the Wall Street Journal today states that our DoubleClick ad cookies comply with Microsoft's request), but newer cookie-based features are broken by the Microsoft implementation in IE. These include things like Facebook "Like" buttons, the ability to sign-in to websites using your Google account, and hundreds more modern web services. It is well known that it is impractical to comply with Microsoft's request while providing this web functionality.

Today the Microsoft policy is widely non-operational.

In 2010 it was reported:

> *Browsers like Chrome, Firefox and Safari have simpler security settings. Instead of checking a site's compact policy, these browsers simply let people choose to block all cookies, block only third-party cookies or allow all cookies.....*

Thousands of sites don't use valid P3P policies....

A firm that helps companies implement privacy standards, TRUSTe, confirmed in 2010 that most of the websites it certifies were not using valid P3P policies as requested by Microsoft:
> *Despite having been around for over a decade, P3P adoption has not taken off. It's worth noting again that less than 12 percent of the more than 3,000 websites TRUSTe certifies have a P3P compact policy. The reality is that consumers don't, by and large, use the P3P framework to make decisions about personal information disclosure.*

A 2010 research paper by Carnegie Mellon found that 11,176 of 33,139 websites were not issuing valid P3P policies as requested by Microsoft.

In the research paper, among the websites that were most frequently providing different code to that requested by Microsoft: Microsoft's own live.com and msn.com websites.

Microsoft support website

The 2010 research paper "*discovered that Microsoft's support website recommends the use of invalid CPs (codes) as a work-around for a problem in IE*." This recommendation was a major reason that many of the 11,176 websites provided different code to the one requested by Microsoft.

Google's provided a link that explained our practice.

Microsoft could change this today

As others are noting today, this has been well known for years.

- Privacy researcher Lauren Weinstein states: "*In any case, Microsoft's posting today, given what was already long known about IE and P3P deficiences in these regards, seems disingenuous at best, and certainly is not helping to move the ball usefully forward regarding these complex issues.*"

- Chris Soghoian, a privacy researcher, *points out*: "*Instead of fixing P3P loophole in IE that FB & Amazon exploited ..…MS did nothing. Now they complain after Google uses it.*"

- Even the Wall Street Journal says: "It involves a problem that has been known about for some time by Microsoft and privacy researchers...."